Міністерство внутрішніх справ України

Луганський державний університет
внутрішніх справ імені Е.О. Дідоренка

М.В. Карчевський

Кримінально-правова охорона інформаційної безпеки України

Монографія

Луганськ
РВВ ЛДУВС
ім. Е.О. Дідоренка
2012

Автор: М.В. КАРЧЕВСЬКИЙ, доцент кафедри кримінального права Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, кандидат юридичних наук, доцент

Рецензенти: М.І. ХАВРОНЮК, доктор юридичних наук, професор, заслужений юрист України, заступник керівника апарату Верховного Суду України; О.О. ДУДОРОВ, доктор юридичних наук, професор, професор кафедри кримінального права Луганського державного університету внутрішніх справ імені Е.О. Дідоренка

Рекомендовано до друку вченою радою Луганського державного університету внутрішніх справ імені Е.О. Дідоренка (протокол № 7 від 8 грудня 2011 року)

УДК 343.3/.7

Кримінально-правова охорона інформаційної безпеки України : монограф. / М.В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. – 528 с. – Бібліогр. : С. 394 – 439.

ISBN 978-617-616-006-9

Монографію присвячено комплексному дослідженню кримінально-правової охорони інформаційної безпеки України. Питання вдосконалення чинного законодавства про кримінальну відповідальність розглядаються в контексті соціальних тенденцій інформатизації.

Книга розрахована на студентів, викладачів вищих навчальних закладів юридичного профілю, працівників правоохоронних органів, а також усіх, хто цікавиться проблемами кримінального права.

© Карчевський М.В., 2012

Присвячую батькам,
їх віра і любов дуже важливі

Вступ

Сучасне суспільство дедалі частіше називають інформаційним. Загально визнано, що його головною ознакою є принципова зміна ролі інформації: на неї головним чином спирається економіка; вона є основним ресурсом, який за показником економічної ефективності відіграє домінуючу роль, відтіснивши на другий план сировину й енергію.

Такі зміни в суспільстві вимагають певного нормативно-правового відображення. Адже саме право є тим соціальним регулятором, який забезпечує стабільність суспільства та формує напрямки його розвитку.

Головною метою правового регулювання в умовах формування інформаційного суспільства є побудова ефективного механізму реалізації інформаційних прав і свобод людини; забезпечення такого рівня регуляції та охорони інформаційних відносин, який би максимально забезпечував їх якісне функціонування та вдосконалення. Безсумнівно, що однією з найважливіших складових такого механізму є кримінально-правова охорона інформаційної безпеки, адже від захисту суспільних відносин, у межах яких забезпечується реалізація інформаційних прав і свобод, залежить їх ефективність, напрямок та інтенсивність розвитку.

Слід зауважити, що на теперішній час законодавство про кримінальну відповідальність уже містить низку норм, що забезпечують захист інформаційних відносин: окремий розділ КК присвячено злочинам у сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку (ст.ст. 361 – 3631 КК України); передбачено кримінальну відповідальність за незаконні дії з інформацією з обмеженим доступом (ст.ст. 111,

114, 145, 168, 231, 232, 328 КК) та подання неправдивої інформації або неповідомлення певної інформації (ст.ст. 218, 383, 384 КК) тощо.

Водночас, на жаль, не можна сказати, що всі або хоча б більшість кримінально-правових норм з питань інформаційної безпеки охоплюються єдиним розумінням проблеми, мають єдину ідеологію. Вони являють собою фрагментарні рішення окремих проблем інформаційної безпеки, що з необхідністю порушує питання про недостатню ефективність захисту українського інформаційного ресурсу засобами чинного законодавства про кримінальну відповідальність.

Окремі питання кримінально-правової охорони інформаційних суспільних відносин розглядали в своїх роботах Д.С. Азаров, П.П. Андрушко, П.С. Берзін, В.М. Бутузов, В.Б. Вєхов, А.Г. Волєводз, В.Д. Гавловський, В.А. Голубєв, О.П. Горпинюк, В.Д. Гулкевич, М.В. Гуцалюк, Ю.І. Дем'яненко, С.В. Дрьомов, Д.А. Калмиков, В.В. Крилов, О.В. Красненкова, С.Я. Лихова, Т.В. Міхайліна, А.А. Музика, А.С. Нерсесян, Ю.Ю. Орлов, С.О. Орлов, М.І. Панов, М.В. Плугатир, О.Е. Радутний, М.В. Рудик, Н.А. Савінова, К.С. Скоромніков, С.О. Харламова, В.Б. Харченко, А.В. Черних Суміжні проблеми правового регулювання відносин інформаційної безпеки досліджували: Ю.М. Батурін, В.В. Балдіцин, А.В. Бєгун, М.М. Биченок, П.Д. Біленчук, О.В. Бойченко, А.Б. Венгеров, О.А. Гаврилов, В.П. Горбулін, Р.А. Калюжний, В.О. Козубський, А.В. Колодюк, В.К. Конах, Б.А. Кормич, В.А. Ліпкан, В.М. Лопатін, А.І. Марущак, Н.С. Полєвой, А.І. Ракітов, Г.М. Сащук, О.А. Скляренко, О.В. Соснін, С.Г. Спіріна, Л.К. Терещенко, Б.С. Українцев, В.С. Цимбалюк, М.М. Швець.

Водночас комплексного, системного дослідження питань кримінально-правового захисту інформаційної безпеки ще не було здійснено. Дотепер у науці кримінального права невирішеними є питання щодо визначення поняття "інформаційна безпека", формулювання критеріїв суспільної небезпечності посягань на неї, меж застосування та змісту кримінально-правових засобів її захисту. Дискусійними залишаються пи-

тання про ознаки й сутність інформації як предмета злочину, зміст інших ознак складів так званих "комп'ютерних" злочинів (ст.ст. 361 – 363-1 КК України), напрями вдосконалення відповідних законів про кримінальну відповідальність. Україна ратифікувала Конвенцію про кіберзлочинність, що вимагає відповідної роботи щодо гармонізації українського та міжнародного законодавства. Недостатньо дієвим є механізм захисту прав інтелектуальної власності. Виникають принципово нові проблеми, пов'язані з глобалізацією інформаційних процесів: захист прав осіб під час автоматизованої обробки персональних даних, інформаційний суверенітет держави, надмірна комерціалізація інформаційного простору, небезпеки маніпулювання свідомістю та ін.

Необхідно зауважити, що розв'язання цих завдань, забезпечення належного кримінально-правового захисту інформаційної безпеки є необхідною умовою позитивного розвитку українського суспільства, його включення до світових процесів інформатизації. У свою чергу, відсутність науково обґрунтованої системи правових засобів забезпечення інформаційної безпеки може призвести до вельми серйозних наслідків для України та її громадян: від обмеженості можливостей реалізації інформаційної потреби до принципової неконкурентоспроможності національного виробництва, освіти, охорони здоров'я тощо.

* * *

Висловлюю щиру подяку докторові юридичних наук, професорові Борису Григоровичу Розовському, його підтримка та зауваження, безсумнівно, зробили роботу кращою.

Глава 1

Концептуальні засади дослідження кримінально-правових засобів охорони інформаційної безпеки України

1.1. Інформаційна безпека як об'єкт кримінально-правової охорони

Інформаційні суспільні відносини стрімко розвиваються, постійно зростають їх кількісні характеристики, змінюються якісні. Інформатизація та комп'ютеризація привели до збільшення кількості цінної інформації, яка оброблюється в автоматизованих системах, від якості, достовірності й оперативності одержання якої залежить більшість важливих рішень, що приймаються на різних рівнях – від глави держави до громадянина [387, с. 3]. Крім позитивних соціальних наслідків широке впровадження інформаційних технологій спричинило також появу нових видів посягань. При цьому їх небезпечність визначається важливістю суспільних процесів в інформаційній сфері, яке постійно зростає. Тому можна стверджувати, що очевидною є необхідність правового регулювання й охорони означеної сфери.

У комплексі наукових проблем, пов'язаних із забезпеченням правової охорони даних відносин, ключове місце займає категорія "інформаційна безпека". У цій підглаві ми спробуємо сформулювати основні підходи до її визначення. Зазначимо, що категорія "інформаційна безпека" є значущою для ба-

гатьох як гуманітарних, так і технічних наук, і в межах кожної з них існує власне визначення інформаційної безпеки, яке відповідає предмету тієї чи іншої науки. Зрозуміло, що сформулювати універсальне визначення неможливо, тому в цій підглаві буде здійснено спробу визначення інформаційної безпеки як об'єкта кримінально-правової охорони, тобто певної сукупності суспільних відносин, які охороняються законом про кримінальну відповідальність.

Починаючи розгляд наявних у законодавстві та висловлених у науці визначень досліджуваної категорії, зазначимо, що в аналітичній доповіді Українського центру економічних і політичних досліджень імені Олександра Разумкова, оприлюдненій у 2001 році, було сказано: "Проведений аналіз засвідчує, що рівень інформаційної безпеки в Україні, за окремими ознаками, наближається до критичної межі, за якою – втрата демократичних принципів і засад діяльності держави, повернення до авторитаризму, ізоляція України на міжнародній арені" [7]. У Постанові Верховної Ради України "Про підсумки парламентських слухань "Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України" від 7 червня 2001 року фіксується невтішний висновок: "Визнати незадовільним стан національної безпеки України в інформаційній сфері, що виявляється передусім у втраті контролю за використанням радіочастотного ресурсу України, уповільненні розвитку новітніх інформаційних технологій, протекціонізмі зарубіжними суб'єктами інформаційних відносин на національному рівні інформаційних послуг, ігноруванні посадовими особами органів державної влади, керівниками засобів масової інформації норм законодавства України в інформаційній сфері" [276]. Отже, питання визначення інформаційної безпеки як концептуальної передумови побудови ефективної системи її захисту має не тільки наукове, але й велике практичне значення.

Не можна не відзначити, що на сьогодні в кримінально-правовому науковому дискурсі поняття "інформаційна безпека" переважно використовується в надто вузькому значенні: як

захищеність від витоку відомостей, що містять державну таємницю. Насамперед це пов'язано з тим, що у КК воно використовується тільки в диспозиції ч.1 ст. 111, яка передбачає відповідальність за державну зраду. Так, М.І. Хавронюк обґрунтовано зазначає, що безпосереднім об'єктом державної зради є національна безпека переважно у сфері державної безпеки, інформаційній, економічній, науково-технологічній і військовій сферах, при цьому робить уточнююче зауваження про те, що в контексті ст. 111 інформаційна безпека перш за все означає захищеність України від витоку інформації, що складає державну таємницю [251, с. 257 – 258]. Е.М. Кісілюк та В.І. Павліковський у ході аналізу складу злочину державної зради зазначають, що під загрозами національній (у тому числі державній) безпеці України в інформаційній сфері слід розуміти витік інформації, яка становить державну таємницю [189, с. 31]. Подібні позиції висловлюються і в роботах інших авторів [348, с. 256; 349, с. 244; 194, с. 327; 192, с. 10; 192, с. 26].

Очевидно, що таке становище не відповідає соціальним тенденціям інформатизації та зумовленим ними потребам у правовому регулюванні й охороні суспільних відносин. Як правильно зазначає Л. Шуберт: "Науковість пізнання певного суспільного явища, узагальненого в понятті, полягає в тому, що наука намагається таким чином уточнити поняття, щоб його зміст відповідав даній історичній обстановці" [386, с. 11]. В умовах, коли можливі загрози у сфері інформаційної безпеки далеко не вичерпуються витоком відомостей, що складають державну таємницю, кримінальне право, як нормативна база охорони суспільних відносин від злочинних посягань, не повинне розглядати інформаційну безпеку настільки вузько. Отже, необхідно запропонувати таке визначення інформаційної безпеки, яке б урахувало сучасні соціальні тенденції та зумовлені ними потреби в кримінально-правовій охороні.

Окремо зазначимо, що в межах суміжних юридичних наук, зокрема в адміністративному та інформаційному праві, здійснено достатньо значну кількість досліджень з питань інформаційної безпеки, отримано вагомі наукові результати [28,

133, 142, 210, 227]. І хоча можливості їх використання в межах цієї роботи обмежені відомою специфікою предмета й методу кримінально-правового регулювання, аналіз висловлених пропозицій щодо сутності інформаційної безпеки та загальних засад її правового забезпечення є необхідним. Таким чином, для формулювання науково обґрунтованого визначення інформаційної безпеки як об'єкта кримінально-правової охорони потрібно: по-перше, провести аналіз ґенези нормативно-правового відображення досліджуваного поняття; по-друге, установити його сутнісні характеристики шляхом дослідження підходів до визначення цього поняття, запропонованих у суміжних юридичних науках; по-третє, ураховуючи специфіку інформаційної безпеки саме як об'єкта кримінально-правової охорони, сформулювати необхідне визначення.

Включення цієї категорії в науковий та нормативно-правовий обіг зумовлене перш за все статтею 17 Конституції України, у якій зазначено: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та *інформаційної безпеки* (курсив наш. – *М.К.*) є найважливішими функціями держави, справою всього Українського народу".

Достатньо цікавим видається дослідження того, як розуміється поняття "інформаційна безпека" в інших нормативно-правових актах. Так, Закон України "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 року констатує, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. До об'єктів інформаційної безпеки цей закон відносить: інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Отже, під інформаційною безпекою в цьому нормативно-правовому акті розуміється комплекс заходів, спрямованих на забезпечення захисту інформації від неправомірного витоку, перекручення, знищення тощо.

Приблизно такий самий зміст досліджуване поняття має й у Рішенні Ради голів урядів СНД про Концепцію інформаційної безпеки держав-учасниць Співдружності Незалежних Держав у військовій галузі. Інформаційна безпека хоча й визначається в цьому документі як "стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави", але використовується як близьке за змістом до поняття "захист інформації". Про це насамперед свідчить визначення системи забезпечення інформаційної безпеки, під якою розуміється сукупність правових, організаційних та технічних заходів, органів, сил, засобів та норм, спрямованих на попередження або істотне ускладнення заподіяння шкоди власнику інформації, а також перелік методів забезпечення інформаційної безпеки, який фактично являє собою перелік методів забезпечення захисту інформації.

В Указі Президента України "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні" від 31 липня 2000 року поняття інформаційної безпеки вже не обмежується тільки захистом інформаційного ресурсу. Так, до завдань щодо ґарантування інформаційної безпеки держави відноситься недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства. Отже, під забезпеченням інформаційної безпеки розуміється не тільки захищеність інформаційного ресурсу, але й захищеність суспільства від розповсюдження "неґативної" інформації (порнографія, пропаганда культу насильства та жорстокості тощо).

Закон України "Про основи національної безпеки України" від 19 червня 2003 року використовує поняття "інформаційна безпека" у ще ширшому значенні. Про це свідчить зміст визначених у ньому загроз та напрямків державної політики в інформаційній сфері. Так до загроз національній безпеці в інформаційній сфері закон відносить:

1) прояви обмеження свободи слова та доступу громадян до інформації;

2) поширення засобами масової інформації культу насильства, жорстокості, порнографії;

3) комп'ютерну злочинність та комп'ютерний тероризм;

4) розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

5) намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основними ж напрямками державної політики з питань національної безпеки закон визначає:

1) забезпечення інформаційного суверенітету України;

2) вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

3) активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, ін.-шими явищами, які загрожують національній безпеці України;

4) забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

5) вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Логічним продовженням такого підходу законодавця є визначення інформаційної безпеки, яке наводиться в Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 9 січня 2007 року – це "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації". Таке визначення достатньо чітко фіксує відхід законодавця від вузького розуміння інформаційної безпеки як технічного захисту інформації, її визначення сформульоване як стан захищеності від загроз інформаційного та технологічного характеру.

Указом Президента України № 514/2009 від 8 липня 2009 року було затверджено Доктрину інформаційної безпеки України. Як правильно зазначає О.Г. Братель, цей документ являє собою "сукупність офіційних поглядів на мету, функції, принципи та методи забезпечення національної безпеки України у інформаційній сфері" [32, с. 37]. Розглянемо ретельно його положення. По-перше, підкреслюється подвійне значення інформаційної безпеки: 1) як невід'ємної складової кожної зі сфер національної безпеки; 2) як самостійної сфери національної безпеки. По-друге, класифікація життєво важливих інтересів в інформаційній сфері здійснюється за суб'єктом, тобто доктриною виокремлюються інтереси особи, суспільства та держави. До інтересів особи в доктрині віднесено: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та розповсюдження інформації; недопущення несанкціонованого втручання в зміст, процеси обробки, передачі та використання персональних даних; захищеність від не-

ґативного інформаційно-психологічного впливу. Інтереси суспільства полягають у збереженні та примноженні духовних, культурних і моральних цінностей Українського народу; забезпеченні суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формуванні й розвитку демократичних інститутів громадянського суспільства. Державні інтереси сформульовано таким чином: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; інтеґрація України у світовий інформаційний простір. По-третє, доктрина формулює основні реальні та потенційні загрози інформаційній безпеці в певних сферах і визначає основні напрямки протидії їм. Систематизуємо ці дані в таблиці (додаток 1).

Таким чином, аналіз національного законодавства дає підстави стверджувати, що наявною є тенденція розширення змісту законодавчого визначення поняття "інформаційна безпека". З розвитком інформатизації суспільства та вдосконаленням нормативно-правового забезпечення цих процесів розуміння інформаційної безпеки на законодавчому рівні пройшло шлях від вузького, найпростішого її визначення як технічного захисту інформації до складної розгалуженої системи характеристик, викладених у проаналізованій доктрині.

Про складність та багатовимірність категорії "інформаційна безпека" свідчить і активний науковий дискурс вітчизняних та зарубіжних дослідників з приводу формулювання її ключових ознак, структури, видів тощо. Так, Г. Бруснічкін визначає інформаційну безпеку як стан або міру технічної захищеності інформації від різних загроз (викрадання, знищення, перекручення), що досягається шляхом реалізації тих чи інших заходів щодо захисту інформації [33, с. 9]. А.А. Тер-Ако-

пов під інформаційною безпекою пропонує розуміти стан захищеності інформації, що забезпечує життєво важливі інтереси людини (вітальні, фізичні, психологічні, генетичні, репродуктивні, інтелектуальні та духовні) [331, с. 168]. В.К. Конах уважає, що інформаційна безпека являє собою захищеність інформації та забезпечення цілісності та надійності критичної інформаційної інфраструктури держави від випадкових впливів природного чи штучного характеру, навмисних вторгнень або нападів, які можуть спричинити руйнування, перериванння, перекручування інформації, що може призвести до широкомасштабних небажаних наслідків політичного, релігійного чи ідеологічного характеру, а також – забезпечення формування та подальшого розвитку інформаційних ресурсів з урахуванням інтересів особистості, суспільства та держави [138]. У цих визначеннях інформаційна безпека фактично зводиться до технічного захисту інформації та технічних засобів, що забезпечують роботу з нею.

Слід зазначити, що більшість науковців розуміють інформаційну безпеку значно ширше. В.О. Козубський зазначає, що інформаційна складова національної безпеки держави – це не тільки захист комп'ютерних систем і телекомунікаційних мереж країни, але й цілий комплекс проблем, які пов'язані з гуманітарною складовою національної безпеки, управлінням суспільною свідомістю нації [131].

Істотну частину визначень інформаційної безпеки, представлених у науковій літературі, сконструйовано за принципом розуміння досліджуваної категорії *як стану захищеності від певних небажаних наслідків*. Так, під час роботи круглого столу "Інформаційна безпека України: сутність та проблеми", який проводила в червні 1998 року Комісія з питань інформаційної безпеки спільно з Національним інститутом стратегічних досліджень, висловлювалися такі думки. В.Я. Рубан пропонував визначати інформаційну безпеку людини, суспільства, держави як "такий стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні

викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів" [229], подібної точки зору дотримується й Г.М. Сащук [313]. О.А. Баранов визначав досліджувану категорію як "стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації" [229].

О.В. Бойченко в ході дослідження організаційно-правових засад інформаційної безпеки органів внутрішніх справ обґрунтував, що вона є "станом захищеності інформаційного середовища, відповідного інтересам органів внутрішніх справ, за якого забезпечуються їх формування, використання та можливості розвитку незалежно від дії внутрішніх і зовнішніх інформаційних погроз" [28, с. 232]. Російський дослідник В.М. Лопатін визначає інформаційну безпеку як "стан захищеності національних інтересів країни (життєво важливих інтересів особи, суспільства та держави на збалансованій основі) в інформаційній сфері від внутрішніх та зовнішніх загроз" [215, с. 91]. Це визначення отримало закріплення в Доктрині інформаційної безпеки Російської Федерації, затвердженій Указом Президента РФ від 9 вересня 2000 року № пр-1895. Аналізуючи його, інший російський учений Д.О. Калмиков відзначає, що принцип балансу інтересів особи, суспільства та держави в інформаційній сфері слід розуміти як вимогу неухильного дотримання прав та свобод особи, суспільства та держави в інформаційній сфері з закритим переліком підстав для їх тимчасового обмеження. Таке обмеження можливе лише на підставі судового рішення або відповідного закону [116, с. 9]. О.В. Красненкова також солідаризується з наведеним визначенням та зазначає, що інформаційна безпека передбачає: 1) повне забезпечення заінтересованих суб'єктів необхідною життєво важливою інформацією; 2) їх захист від впливу негативної інформації; 3) можливість захисту конфіденційної ін-

формації та відомостей, що відносяться до комерційної таємниці [146, с. 33, 34].

Для О.А. Скляренка інформаційна безпека являє собою "стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави" [318, с. 125]. Близькі погляди викладаються також у роботах російських науковців. Так, В.Д. Курушин та В.А. Мінаєв визначають досліджувану категорію як "стан інформаційної сфери суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій та держави" [199, с. 141]. На думку І.М. Панаріна, під інформаційною безпекою слід розуміти "стан інформаційного середовища суспільства і політичної еліти, що забезпечує його формування і розвиток в інтересах керівництва держави, громадян і суспільства" [260, с. 128].

Отже, прибічників визначення інформаційної безпеки як певного стану захищеності можна поділити на дві групи: перші визначають досліджувану категорію як стан захищеності інтересів в інформаційній сфері, другі – як стан захищеності інформаційного середовища. При чому перша група може бути поділена ще й за критерієм захищеності, який вони визначають. Так, О.А. Баранов розуміє під ним стійкість до загроз, пов'язаних з інформаційними впливами, доступом до інформації та використанням технологій. Критерієм захищеності у визначенні В.М. Лопатіна також є стійкість до внутрішніх та зовнішніх загроз, однак прибічники такої точки зору особливу увагу звертають на спосіб досягнення цієї стійкості – баланс інтересів особи, суспільства та держави, що ґрунтується на неухильному дотриманні "інформаційних" прав та свобод.

Зазначимо, що висловлені в науці підходи до визначення поняття "інформаційна безпека" не обмежуються її розумінням як певного "стану захищеності". Так, один із провідних українських дослідників у цій сфері Б.А. Кормич визначає інформаційну безпеку як "захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані конституцією умови існу-

вання і розвитку людини, всього суспільства і держави" [141, с. 92]. У контексті подібного розуміння інформаційну безпеку пропонує розглядати й А.І. Марущак. Він визначає поняття інформаційної безпеки через комплекс прав людини: по-перше, це комплекс прав людини вільно, безперешкодно, на власний розсуд бути суб'єктом інформаційних процесів: шукати, одержувати та поширювати інформацію, причому це право не пов'язане з територіальною юрисдикцією держави й не обмежується територіальними кордонами; по-друге, це комплекс прав людини на захист від неправомірного інформаційного втручання, що охоплюється англійським терміном privacy, тобто правом на конфіденційність інформації щодо особистого життя та правом на захист від розповсюдження вигаданої та перекрученої інформації, що завдає шкоди її честі й репутації [227, с. 82]. Наведені визначення цілком справедливо акцентують увагу на значенні правого регулювання інформаційної сфери. Доречно зазначити, що, на думку В.М. Лопатіна, державна політика з забезпечення інформаційної безпеки реалізується через правотворчість, правозастосування та участь держави в розвитку правової свідомості та культури громадян. При цьому на сучасному етапі визначальною є правотворчість – розвиток законодавства [216, с. 13]. У питанні мети правового регулювання інформаційних відносин погляди В.Б. Кормича та А.І. Марущака близькі до позицій В.М. Лопатіна. Формулюючи її, дослідники чітко фіксують діалектичність сучасних суспільних потреб, що, з одного боку, полягають у розширенні вільного доступу до інформації, а з іншого – вимагають збереження окремих регламентованих обмежень на її поширення. На цю специфіку інформаційної безпеки звертає увагу й І.М. Колодій [132, с. 304].

В.А. Ліпкан, автор ґрунтовного дослідження з питань адміністративно-правового забезпечення національної безпеки України [210] дає таке визначення інформаційної безпеки: "складова національної безпеки, свідомий цілеспрямований вплив суб'єкта управління на загрози та небезпеки, за якого державними та недержавними інституціями створюються не-

обхідні і достатні умови для: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активного залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України, неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України" [211, с. 253 – 254]. Отже, В.А. Ліпкан звертає увагу ще на одне проблемне поле інформаційної безпеки – включення її до системи національної безпеки.

Як видається, найбільш вдалий висновок щодо співвідношення категорій "інформаційна безпека" та "національна безпека" запропонував Б.А. Кормич. Він зазначає: " … діяльність по підтриманню національної безпеки охоплює певну частину інших напрямів діяльності держави, зокрема інформаційної. Саме на перетині цих напрямів формується сфера державної діяльності, яка пов'язана із підтриманням стану інформаційної безпеки держави, суспільства та людини" [142, с. 109 – 110].

А.В. Бєгун уважає, що проблему інформаційної безпеки слід розглядати в трьох аспектах: 1) захист інформації; 2) контроль за національним інформаційним простором; 3) достатнє інформаційне забезпечення державних і недержавних органів, громадських і приватних організацій. При цьому до захисту інформації він відносить питання, пов'язані з побудовою системи захисту від несанкціонованих дій з інформацією. Контроль за національним інформаційним простором передбачає мінімізацію збитків від "здійснення як іноземними державами,

так і внутрішніми організаціями підривних психологічних операцій". Рівень достатності інформаційного забезпечення державних і недержавних органів, громадських і приватних організацій пропонується визначати виходячи з їхніх потреб в інформації для прийняття рішення в кожному конкретному випадку [24, с. 9 – 10]. Близькі погляди висловлює й М.М. Потрубач, який визначає інформаційну безпеку як здатність держави, суспільства, соціальної групи, особи забезпечити з певною вірогідністю достатні та захищені інформаційні ресурси й інформаційні потоки для підтримання життєдіяльності та життєздатності, стійкого функціонування та розвитку; протистояти інформаційним небезпекам і загрозам, негативним інформаційним впливам на індивідуальну й суспільну свідомість та психіку людей, а також на комп'ютерні мережі та інші технічні джерела інформації [289, с. 265]. Певний розвиток таке бачення інформаційної безпеки отримало в дослідженні О.О. Тихомирова, який зазначає, що на основі діяльнісного підходу філософсько-соціологічна інтерпретація інформаційної безпеки має бути такою: "сукупність умов функціонування суб'єктів в інформаційній сфері та суб'єктивних можливостей їх усвідомлення й контролю" [335, с. 9]. Наведені підходи наочно демонструють складність внутрішньої структури інформаційної безпеки, той факт, що її межами охоплюються суспільні відносини, пов'язані з використанням технологій, формуванням правових ґарантій доступу до інформації та унеможливленням негативних інформаційних впливів на свідомість.

На окрему увагу заслуговують результати дослідження В.П. Горбуліна та М.М. Биченка [71]. Вони виходять з того, що якісні та кількісні характеристики інформаційних процесів у будь-якій сфері життєдіяльності вимірюються за двома складовими: інформаційно-психологічною та інформаційно-комунікаційною. Перша складова являє процеси в індивідуальній, колективній і масовій свідомості. Друга – процеси, що реалізують інформаційні взаємозв'язки та взаємовпливи між людиною, суспільством і державою. Ці взаємозв'язки та взаємовпли-

ви породжуються різноманітними особистими, суспільними та державними інтересами, які постійно змінюються і потребують динамічного узгодження та коригування. Відсутність чи викривлення інформації щодо цих інтересів може порушити їхній баланс і призвести до конструктивних (творчих) або деструктивних (руйнівних) конфліктів. Негативні інформаційні впливи, як правило, породжуються деструктивними конфліктами й можуть мати до вкрай небезпечні соціальні, економічні, політичні й інші наслідки. Керуючись таким підходом, автори класифікують об'єкти ураження в інформаційній сфері на інформаційно-психологічні та інформаційно-комунікаційні. До перших відноситься індивідуальна, колективна та масова свідомість, до других – складові інформаційно-комунікаційної інфраструктури.

Отже, "забезпечення інформаційної безпеки, – на думку В.П. Горбуліна та М.М. Биченка, – потребує динамічного узгодження й коригування особистих, суспільних і державних інтересів з метою недопущення виникнення між ними деструктивних конфліктів або локалізації та нейтралізації їхніх негативних наслідків у разі неможливості досягнення балансу інтересів з об'єктивних чи суб'єктивних причин" [71, с. 10]. Для нашого дослідження ця концепція важлива включенням у науковий дискурс такої властивості інформаційної сфери, як змінність. У свою чергу це означає, що інформаційна безпека являє собою динамічний процес.

Аналіз наведених визначень дозволяє стверджувати, що в сучасній юридичній науці під інформаційною безпекою розуміється далеко не тільки забезпечення цілісності інформаційного ресурсу, режиму обмеженого доступу до нього. Таке становище є абсолютно адекватним відображенням того значення, якого сьогодні набувають інформаційні процеси, усвідомленням державного рівня небезпеки негативних інформаційних впливів та обмеження доступу до інформації. Виявлене нами різноманіття підходів до визначення інформаційної безпеки дозволяє сформулювати основні характеристики інфор-

маційної безпеки. Найбільш вдало специфіку інформаційної безпеки як *об'єкта правового регулювання* розкриває Б.А. Кормич:

"1. Зона інформаційної безпеки знаходиться на перехресті функції національної безпеки та інформаційної функції держави.

2. Питання інформаційної безпеки держави має екстериторіальний характер.

3. Суспільні відносини, що входять до інформаційної безпеки є неоднорідними та різноплановими.

4. Компетенція держави у сфері інформаційної безпеки зумовлюється конкуренцією між інформаційними правами особи та функціями держави її органів із регулювання інформаційних процесів.

5. У демократичному суспільстві державне регулювання інформаційної сфери можливе лише шляхом встановлення правових норм.

6. Політика інформаційної безпеки має багатовекторний характер. ЇЇ головними складовими (векторами) є: регулювання інформаційних відносин з метою забезпечення національної безпеки, територіальної цілісності та громадського порядку, підтримання законності; регулювання інформаційних відносин з метою забезпечення прав і свобод громадян, здоров'я та моральності; регулювання інформаційних відносин у сфері комерційної інформації" [143, с. 108].

Починаючи розгляд інформаційної безпеки як *об'єкта кримінально-правової охорони,* по-перше, зазначимо, що за суттю вона є не певним станом або захищеністю, а системою суспільних відносин. Будь-який інший підхід входив би в очевидну суперечність з аксіоматичними положеннями юридичної науки. Крім цього, дуже важливою сутнісною ознакою інформаційної безпеки є її динамічність, оскільки, як ми встановили, вона, у найширшому розумінні, являє собою забезпечення стабільності та розвитку інформаційної сфери, яка постійно змінюється через різноманіття потреб учасників інформаційних відносин. У зв'язку з останнім зауважимо, що більшість із наведених визначень хоча й фіксують важливі, конститутивні

ознаки інформаційної безпеки, однак розглядають її як стабільне, незмінне явище: "стан захищеності", "здатність захищати", "захищеність" тощо. Російський дослідник Н.І. Зінченко зазначає, що розуміння безпеки держави як певного стану чи можливості протистояти супротивнику або захищеності його основ є обмеженим і не може бути сприйняте безперечно, оскільки всі ці точки зору передбачають розгляд безпеки, по-перше, ізольовано від процесів, що викликають необхідність "захисту", "протистояння"; по-друге, однобічно та в статичному стані, без урахування особливостей соціального розвитку [110, с. 187]. Висловлені положення також підтверджують обґрунтованість розгляду інформаційної безпеки саме як певної системи суспільних відносин.

По-друге, інформаційна безпека має специфічне подвійне значення. Як ми вже зазначали, відповідно до Доктрини інформаційної безпеки України вона розглядається як: 1) невід'ємна складова кожної зі сфер національної безпеки; 2) самостійна сфера національної безпеки. У контексті розв'язання завдань правового регулювання та охорони це означає, що нормативно-правовий вплив на відносини інформаційної безпеки здійснюється як у межах інформаційного права, так і за допомогою різноманітних інших конструктивних галузей права: конституційного, цивільного, банківського, комерційного тощо. Відповідно, і кримінально-правова охорона предмета нашого дослідження забезпечується за допомогою норм, що передбачають посягання на різноманітні родові об'єкти.

По-третє, суспільні відносини, що складають інформаційну безпеку як об'єкт кримінально-правової охорони, слід визначати так, щоб висновок щодо необхідності застосування кримінально-правових засобів для охорони саме цих відносин був чітким і послідовним. У найбільш загальному розумінні особу слід уважати такою, що перебуває в стані інформаційної безпеки, тоді, коли її потреба в інформації забезпечена належним чином. Тобто тоді, коли особа має можливість одержувати достовірну та достатню для здійснення ефективної діяльності інформацію. А суспільно небезпечними слід визнавати такі

посягання у сфері інформаційної безпеки, які виключають або значно ускладнюють реалізацію інформаційної потреби.

Отже, зміст системи суспільних відносин інформаційної безпеки як об'єкта кримінально-правової охорони пов'язаний із поняттями "інформаційна потреба", "інформаційний ресурс", "інформаційні суспільні відносини", "соціальна інформаційна взаємодія" та "інформаційні технології".

Інформаційна потреба виникає тоді, коли певний суб'єкт не може виконати завдання, що стоїть перед ним, без отримання додаткової інформації. Інформаційний ресурс – уся сукупність одержуваних відомостей і таких, які накопичуються в процесі розвитку науки та практичної діяльності людей для їх багатоцільового використання в суспільному виробництві й управлінні; відноситься до найважливіших видів ресурсів, що визначають економічну, політичну та (або) військову міць їх власника [60 с. 3 – 8]. До інформаційних ресурсів нашої країни згідно зі ст. 53 Закону України "Про інформацію" входить вся належна їй інформація незалежно від змісту, форм, часу і місця створення. Як уважає О.В. Соснін, інформація, створена чи виявлена, систематизована, зареєстрована й накопичена у перетвореній формі, є інформаційним ресурсом. Інформаційні ресурси, на його думку, є безліччю різноманітних об'єктів, що беруть участь у ряді процесів, які відрізняються за своєю природою. У загальному розумінні інформаційним ресурсом є організована за єдиною технологією сукупність інформаційних продуктів. До основних сучасних форм організації інформаційного ресурсу О.В. Соснін відносить: файл, базу даних, банк даних, базу знань, бібліотеку тощо. Важливим результатом його дослідження є й формулювання важливих ознак інформаційного ресурсу, до яких він відносить можливість бути системоутворюючим чинником діяльності, позитивно впливати на соціально-економічний розвиток суспільства і держави та забезпечення національної безпеки, а також здатність завдавати шкоди суспільству в разі низької якості або негативної інформаційної експансії з боку інших країн [319]. Ураховуючи наведені законодавчі положення та поділяючи

наукові, у межах нашого дослідження інформаційним ресурсом будемо вважати всю сукупність об'єктивованої інформації, тобто інформації, яка знаходиться на певному носієві й може слугувати задоволенню інформаційної потреби людини, держави або суспільства.

Інформаційні відносини – відносини, що виникають у всіх сферах життя та діяльності суспільства й держави при збиранні, одержанні, використанні, поширенні та зберіганні інформації [53, с. 152].

Соціальна інформаційна взаємодія, у найзагальнішому розумінні, являє собою динамічний процес використання та формування соціального інформаційного ресурсу. Необхідною складовою будь-якої діяльності держави, суспільства, фізичних або юридичних осіб є інформаційне забезпечення: для того щоб діяти, їм необхідна інформація, яку вони отримують у межах інформаційних суспільних відносин (використання). Водночас результатом будь-якої діяльності є певна зміна соціальних відносин, предметів, статусу учасників та ін., ця зміна породжує нову інформацію, якою, у свою чергу, поповнюється інформаційний ресурс (формування). Отже, у процесі соціальної інформаційної взаємодії, з одного боку, відбувається забезпечення учасників суспільних відносин інформацією, необхідною для їх діяльності, а з іншого – здійснюється поповнення інформаційного ресурсу новою інформацією.

Одержуючи інформацію, суб'єкт узгоджує свої дії з діями інших суб'єктів, чим забезпечує їх результативність та ефективність. Інформація як необхідна умова людської діяльності робить поведінку людини усвідомленою, оскільки опосередковує зв'язки людини з людиною, людини з природою і технікою. Слід погодитися з Д.В. Дюжевим, який зазначає, що ніяке соціальне життя неможливе без інформації, без спілкування та комунікацій [92]. Досить чітко соціальну значущість інформаційної взаємодії сформулював засновник кібернетики Норберт Вінер: "... будь-який організм скріплюється наявністю засобів придбання, використання, зберігання та передавання інформації" [55, с. 234]. О.Г. Старіш, розглядаючи суспільство

як систему, зазначає, що існування будь-якого соціуму припускає узгодження дій його членів (як елементної бази системи) в напрямку забезпечення збереження самого соціуму в цілому й у напрямку забезпечення існування окремих його членів. Узгодження дій досягається процесами інформаційного обміну всередині соціуму [324, с. 67]. Робить він і такий висновок: "Без інформаційної взаємодії членів соціуму організація їхньої спільної діяльності – існування соціуму як системи – була б просто неможлива" [324, с. 85]. Отже, інформаційна взаємодія як основа результативної, ефективної діяльності людини врешті-решт є необхідною умовою розвитку та стабільності суспільства. Значущість інформаційної взаємодії для суспільства можна умовно порівняти зі значущістю нервової системи для організму людини. Подібно до того, як через нервову систему скеровуються імпульси до органів, що зумовлює їхню діяльність, а також фіксуються зміни в стані організму, навколишньому середовищі, чим забезпечується можливість пристосування та розвитку організму, процеси соціальної інформаційної взаємодії зумовлюють діяльність членів суспільства, фіксують зміни забезпечують його сталий розвиток.

Поняття "інформаційна технологія" визначається в Законі України "Про Національну програму інформатизації" так: "цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування". Інформаційні технології являють собою організаційно-технічну базу процесів інформаційної суспільної взаємодії.

Таким чином, інформаційна безпека розуміється як система суспільних відносин, що забезпечує можливість реалізації інформаційної потреби громадян, суспільства, держави. Реалізація інформаційної потреби здійснюється шляхом отримання доступу до необхідної інформації, базується на використанні інформаційних технологій та забезпечується формуванням інформаційного ресурсу. Означеного достатньо для того, щоб

сформулювати таке визначення: *інформаційна безпека – система суспільних відносин щодо забезпечення реалізації інформаційних потреб громадян, суспільства, держави, яка включає: 1) відносини щодо забезпечення доступу до інформаційних ресурсів; 2) відносини щодо формування інформаційного ресурсу; 3) відносини щодо забезпечення функціонування інформаційних технологій як засобів доступу до інформаційного ресурсу та його формування.*

Отже, суб'єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією. Такий стан досягається соціальною активністю в трьох взаємопов'язаних групах суспільних відносин, що представляють собою структурні елементи інформаційної безпеки: суспільні відносини у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного ресурсу. У межах першої групи забезпечується функціонування ефективних засобів інформаційної діяльності, у межах другої – забезпечується можливість суб'єктів отримувати доступ до необхідних інформаційних ресурсів, у межах третьої – формується інформаційний ресурс, що відповідає потребам суб'єктів. Серед означених суспільних відносин ті, які охороняються законом про кримінальну відповідальність, і складають зміст інформаційної безпеки як об'єкта кримінально-правової охорони.

Наведена теза вимагає відповідні на ще одне важливе питання: наскільки обґрунтовано вважати інформаційну безпеку самостійним об'єктом кримінально-правової охорони? Означена проблема актуалізується насамперед тим, що відповідно до чинного законодавства суспільні відносини інформаційної безпеки відносяться до значної кількості різноманітних родових об'єктів. Так, до посягань на відносини у сфері забезпечення доступу до інформаційних ресурсів слід відносити злочини, передбачені ст.ст. 111, 114, 132, 145, 159, 163, 168, 182, 231, 232, 328, 330, 381, 387, 422 КК України. Досить великою є й група злочинів, які можна віднести до посягань на суспільні відносини у сфері формування інформаційного ресурсу: чч. 2, 3

ст. 109, ст.ст. 110, 161, 171, 258-2, 295, 300, 301; ч. 2 ст. 442. У свою чергу, групу посягань на відносини у сфері використання інформаційних технологій складають злочини, передбачені ч. 11, 12 ст. 158, ст.ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1. Таке положення є цілком очевидним. Настільки широке коло відносин інформаційної безпеки зумовлюється тим, що інформація є необхідною передумовою будь-якої діяльності людини, тому наслідки посягання в інформаційній сфері можуть наставати в достатньо великій кількості інших різноманітних соціальних сфер. Означена специфіка інформаційної безпеки зумовлює й більш радикальні висновки науковців. Так, російський дослідник Д.О. Калмиков зауважує: "… інформація в найзагальнішому випадку є необхідним компонентом будь-якого суспільного відношення, являючи собою не що інше, як універсальний засіб комунікації… інформація тим самим автоматично входить і до складу поняття загального об'єкта злочину" [116, с. 39]. Ґрунтуючись на такому висновку, автор формулює твердження, що випливають із нього: "1) злочинне посягання на будь-який об'єкт кримінально-правової охорони з точки зору формальної логіки (у найзагальнішому розумінні) означає в тому числі й порушення інформаційного компонента відповідного об'єкта; 2) більшість злочинних посягань порушують суспільні відносини в галузі забезпечення інформаційної безпеки…" [116, с. 39]. Висновки доволі спірні, але вони, як видається, мають розглядатись як додаткові аргументи на користь необхідності наукового аналізу питання щодо самостійності інформаційної безпеки як об'єкта кримінально-правової охорони.

Думаємо, що головними підставами для розгляду інформаційної безпеки як самостійного об'єкта кримінально-правової охорони слід уважати: 1) системні властивості визначеної сукупності суспільних відносин; 2) специфіку змісту шкоди, що заподіюється під час посягань на інформаційну безпеку.

По-перше, інформаційна безпека є не простою сукупністю, а системою суспільних відносин. Її структурні елементи

(відносини щодо забезпечення доступу, відносини щодо формування інформаційного ресурсу, відносини щодо використання інформаційних технологій) підпорядковані єдиній спільній соціальній меті – реалізації інформаційної потреби громадян, держави, суспільства. Функціонування та ефективність кожного з елементів системи взаємозумовлені іншими елементами. Так, надання доступу до інформації не має сенсу без формування інформаційного ресурсу та є неефективним без використання інформаційних технологій. Значення формування інформаційного ресурсу визначається можливістю подальшого доступу до нього та забезпечується шляхом використання інформаційних технологій. Функціонування інформаційних технологій набуває соціального значення саме як засіб доступу та формування інформаційних ресурсів. При цьому соціальна значущість як формування інформаційного ресурсу, так і надання доступу до інформації та використання інформаційних технологій є похідною від значення тих суспільних відносин, у межах яких виникає інформаційна потреба. Наприклад, суспільне значення доступу до інформації не є самостійним, а визначається важливістю тієї діяльності, для здійснення якої потрібен доступ; наслідки незаконного отримання доступу до інформації визначаються змістом тих відносин, у межах яких виникла потреба його обмеження; небезпечність порушення функціонування певної комп'ютерної мережі визначається важливістю завдань, для яких вона використовується, тощо.

По-друге, особливості соціальної значущості кожної з названих груп суспільних відносин інформаційної безпеки дозволяють установити специфіку змісту шкоди, яка може бути їм заподіяна. Для всіх визначених відносин інформаційної безпеки спільним є те, що шкода від посягань на них полягає в позбавленні або обмеженні можливості реалізації інформаційної потреби.

Так, зміст шкоди, заподіяної порушеннями інформаційної безпеки, пов'язаними з втручанням у роботу інформаційних технологій, полягає в тому, що незаконні дії з даними в

комп'ютерній системі призводять до неможливості або значного ускладнення використання певних технічних засобів інформаційної діяльності, а це у свою чергу зменшує або виключає можливість реалізації інформаційної потреби певного суб'єкта.

Сутність порушень інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу полягає в тому, що ускладнення чи унеможливлення реалізації інформаційної потреби зумовлюється або порушенням установленого режиму доступу до певного ресурсу, або неправомірним обмеженням доступу до певної інформації.

У свою чергу функціонування суспільних відносин формування інформаційного ресурсу забезпечує саму можливість реалізації інформаційної потреби. Тому специфіка посягань на інформаційну безпеку в означеній сфері полягає в тому, що обмеження можливості реалізації інформаційної потреби зумовлене отриманням суб'єктом інформаційного ресурсу, який не дозволяє ефективно розв'язувати завдання, що стоять перед ним.

Окремим аргументом на користь запропонованого підходу до розгляду інформаційної безпеки як самостійного об'єкта кримінально-правової охорони є й те, що він забезпечує системний підхід до роботи щодо вдосконалення національного законодавства. Так, до питань удосконалення правового регулювання відносин щодо забезпечення доступу до інформаційного ресурсу слід відносити: забезпечення реалізації прав громадян на інформацію та визначення їх меж; забезпечення конфіденційності інформації з обмеженим доступом. Удосконалення правового регулювання відносин щодо забезпечення захищеності формування інформаційного ресурсу, як видається, пов'язане з вирішенням таких проблем: забезпечення діяльності ЗМІ; протидія "зловживанням" свободою слова; захист від маніпулювання масовою свідомістю; забезпечення захищеності прав громадян під час автоматизованої обробки персональних даних. Нарешті, удосконалення кримінально-правового забезпечення використання інформаційних технологій

пов'язане передусім з удосконаленням законодавчої бази протидії так званій кіберзлочинності.

Зазначимо, що на сьогодні проведено низку наукових досліджень з означеної проблематики. Однак комплексного дослідження дотепер здійснено не було. Питання відповідальності за злочини у сфері використання комп'ютерної техніки, за порушення обмеженого доступу до інформації або формування інформаційного ресурсу розглядались окремо, не як складові певної системи кримінально-правових засобів. Тому сьогодні не можна сказати, що всі або хоча б більшість кримінально-правових норм з питань інформаційної безпеки охоплюються єдиним розумінням проблеми, мають єдину ідеологію. Вони являють собою фрагментарні рішення окремих проблем, що з необхідністю порушує питання про недостатню ефективність захисту інформаційної безпеки засобами чинного законодавства про кримінальну відповідальність.

Так, здійснено низку досліджень з питань кримінальної відповідальності за злочини у сфері використання інформаційних технологій (ст.ст. 361 – 363-1 КК). Вагомий внесок у вивчення проблеми зробили М.І. Панов [193], П.П. Андрушко [13], В.М. Бутузов [36], Д.С. Азаров [3], В.О. Голубєв [70], С.В. Дрьомов [86], Т.В. Міхайліна [235], М.В. Плугатир [270], С.О. Орлов [254], Н.А. Розенфельд [301], М.В. Рудик [305]. Більш докладний аналіз цих досліджень буде здійснено в третій і четвертій главах, проте зазначимо, що дискусійними залишаються питання про ознаки й сутність інформації як предмета злочину, зміст інших ознак складів так званих "комп'ютерних" злочинів (ст.ст. 361-363-1 КК України), напрями вдосконалення відповідних законів про кримінальну відповідальність. Актуалізує означені питання очевидна неефективність засобів кримінальної юстиції в цій сфері, про що свідчить аналіз відповідної судової практики (підглава 4.3). Розв'язання поставлених проблемних питань можливе шляхом включення до наукового дискурсу аргументів, пов'язаних із розглядом "комп'ютерних" злочинів саме як одного з видів посягань на інформаційну безпеку. Як зазначалося раніше, таким посяганням властива певна специ-

фіка змісту заподіяної шкоди, і саме врахування цієї специфіки дає певні можливості у розв'язанні питання підвищення ефективності кримінально-правової протидії злочинам у сфері використання комп'ютерної техніки (більш докладно в підглаві 4.3).

Проблеми кримінальної відповідальності за злочини у сфері обмеженого доступу до інформації розглядалися переважно як складові кримінально-правового забезпечення конституційних прав і свобод (С.Я. Лихова [209], Ю.І. Дем'яненко [82], О.П. Горпинюк [72]) або в контексті злочинів у сфері господарської діяльності (О.Е. Радутний [297], С.О. Харламова [375], П.С. Берзін [23]). Автори зазначених досліджень отримали важливі результати для правозастосовної та законотворчої роботи. Однак, можливо, саме через те, що означені проблеми досліджувалися та розглядалися законодавцем як самостійні, здійснений аналіз (підглава 5.1) всієї сукупності норм, що передбачають відповідальність за посягання у сфері обмеженого доступу до інформації , свідчить про: 1) непослідовність законодавчих рішень щодо впливу фактичних чинників суспільної небезпечності на інтенсивність санкцій за окремі види незаконного надання та отримання доступу до інформації; 2) невідповідність цих норм соціальним потребам кримінально-правової протидії, пов'язаним з формуванням тіньового ринку інформації, здобутої злочинним шляхом. Що стосується іншої складової питань кримінально-правого забезпечення доступу до інформації – охорони прав громадян на доступ до певної інформації, то їм, як видається, належної уваги не приділялося.

Таким чином, суспільні тенденції інформатизації зумовили формування та розвиток самостійної системи суспільних відносин – відносин інформаційної безпеки. Рівень суспільної значущості цих відносин вимагає застосування відповідних заходів правового регулювання та охорони. Використання запропонованого підходу до визначення інформаційної безпеки як об'єкта кримінально-правової охорони забезпечить системний підхід до аналізу та вдосконалення чинного законодав-

ства, дозволить обґрунтовано прогнозувати підвищення ефективності правової охорони інформаційної безпеки.

Зазначимо, що важливою складовою дослідження інформаційної безпеки є її класифікація. Наведений вище розподіл суспільних відносин інформаційної безпеки за змістом (використання інформаційних технологій, забезпечення доступу до інформаційного ресурсу, забезпечення формування інформаційного ресурсу) є базовим для нашого дослідження, але не єдиним можливим.

Так, у загальнотеоретичних дослідженнях питань безпеки як категорії права пропонується виділяти такі її види, як безпека особи, безпека суспільства та безпека держави. До безпеки особи відноситься здатність і готовність держави, суспільства захищати індивіда від загроз та небезпек для його життя, здоров'я, майна, цивільних прав, свобод і законних інтересів. Під безпекою суспільства розуміється певна множинність станів соціальної системи, за якої забезпечується її стабільність і розвиток. Нарешті, безпека держави відображає соціальну потребу – потребу суспільства та його громадян у забезпеченні територіальної цілісності та суверенітету держави, основ політичного, економічного та конституційного ладу як найважливішої умови економічного, національного, духовного розвитку суспільства та кожного його члена [110, с. 176 – 84]. Отже, можна говорити про такі види інформаційної безпеки за ознаками джерела інформаційних потреб: інформаційна безпека особи; інформаційна безпека суспільства; інформаційна безпека держави.

А.І. Марущак звертає увагу на те, що нормативне визначення інформаційної безпеки, яке міститься в Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 9 січня 2007 року, дає підстави стверджувати, що наявними є дві взаємопов'язані, але суттєво різні сфери суспільного життя, у яких виникають загрози інформаційній безпеці, – інформаційний простір України та сфера національних інформаційних ресурсів [225, с. 64]. До основних загроз у сфері інформаційного простору він відно-

сить "безсистемний і нескоординований характер діяльності органів державної влади щодо поширення інформації", "недостатній доступ громадян України до відкритої достовірної інформації про діяльність органів державної влади, про події суспільного життя", "здійснення окремими суб'єктами негативних зовнішніх інформаційних впливів на свідомість громадян та усього суспільства". А традиційними негативними явищами та процесами у сфері національних інформаційних ресурсів А.І. Марущак уважає занепад вітчизняних високотехнологічних розробок, недостатній рівень захисту патентоспроможної інформації та комп'ютерну злочинність [225, с. 65 – 66]. Схожі позиції викладаються також у роботах російського дослідника А.Ю. Лазарєва. Він зазначає, що інформаційна сфера, з огляду швидкість її розвитку, – це найменш захищений в організаційному, правовому та технічному плані елемент державного механізму. Відповідно, однією з найважніших складових частин безпеки держави є забезпечення інформаційних процесів та існування інформаційних ресурсів [202, с. 8, 9]. Тому обґрунтованою слід уважати пропозицію щодо класифікації інформаційної безпеки за об'єктом загроз на такі види: безпека інформаційного простору та безпека інформаційних ресурсів.

Оскільки доктрина інформаційної безпеки містить поділ загроз інформаційній безпеці за сферами суспільного життя, видається обґрунтованою відповідна класифікація інформаційної безпеки: політична інформаційна безпека, економічна інформаційна безпека, військова інформаційна безпека тощо. Так, Є.А. Макаренко зазначає, що в умовах інформаційного протиборства до найбільш уразливих сфер життєдіяльності суспільства слід відносити: політичну, суспільну, економічну, військову, науково-технологічну та духовну. До прикладів інформаційних впливів на політичну сферу дослідниця відносить зокрема ідеологічну операцію "Perestroika" (1980 – 1990 рр.). У ході цієї операції, за словами Б. Клінтона, США, вплинувши на ідеологічні основи СРСР, вивели із війни за світову гегемонію державу – основного конкурента Америки. Військова сфера

характеризується вразливістю – в умовах інформаційного протиборства – інформаційних ресурсів збройних сил, ВПК, систем управління військами тощо. У науково-технічній сфері інформаційні загрози полягають у транскордонному переміщенні інтелектуальних ресурсів, несанкціонованому доступі до державних структур накопичення науково-технічної інформації. Загрози міжнародній інформаційній безпеці в духовній сфері стосуються конфесійного протистояння, релігійного фанатизму, трансформації духовних ідеалів та морально-етичних цінностей [221]. До аспектів політичної інформаційної безпеки можуть бути віднесені також загрози, що виникають унаслідок упровадження електронного урядування. Д.В. Дубов структурує систему загроз інформаційній безпеці в цій сфері за напрямами взаємодії в системі електронного урядування. Так, для напрямку "уряд – громадянин" властиві такі загрози, як маніпулятивні технології та ігнорування громадської думки, що можуть призвести до наслідків у вигляді політичного відчуження громадян, порушення демократичних принципів і норм діяльності держави. Відсутність комунікації за напрямком "уряд – бізнес", недостатність доступу до нормативно-правової інформації, ігнорування повідомлень про факти корупції, зловживань посадових осіб тощо загрожують утратою підтримки державної політики з боку підприємницьких структур. Нарешті, відсутність зв'язків типу "уряд – уряд", відсутність інтеграції інформаційних ресурсів державних органів, недостатня розвиненість їх інфраструктури небезпечні порушенням координації управлінських відносин, зниженням ефективності державного управління в цілому [91].

На думку М.В. Гуцалюка "у випадках, коли мова йде про безпеку обробки, отримання, передачі інформації в електронному вигляді, слід говорити про електронну безпеку. Таким чином можливо відокремити загрози, пов'язані із семантичним навантаженням інформації" [79, с. 42]. У свою чергу С. Назаренко зазначає, що в структурі інформаційної безпеки слід виокремлювати інформаційно-психологічну безпеку, яка являє собою "стан захищеності індивідуальної, групової та су-

спільної психології, а відтак і суб'єктів різного рівня спільності, системно-структурної та функціональної організації від впливу таких інформаційних чинників, які спричиняють дисфункціональні соціальні процеси [244]. Погоджуючись із пропозиціями авторів та враховуючи наведені вище висновки В.П. Горбуліна та М.М. Биченка, можна класифікувати інформаційну безпеку за складовими інформаційного процесу на технологічну (електронну, інформаційно-комунікаційну) та інформаційно-психологічну.

Наступну підставу класифікації інформаційної безпеки пропонує В.М. Лопатін. Для побудови цілісної правової системи у сфері інформаційної безпеки він виділяє сім основних об'єктів захисту: захист прав особи та суспільства на доступ до інформації; захист права на недоторканність приватного життя; захист права на інформацію з обмеженим доступом; захист права на об'єкти інтелектуальної власності; захист прав людини та інтересів суспільства від впливу "шкідливої" інформації; захист права на інформаційні системи; захист прав та інтересів держави щодо збереження єдиного інформаційного простору в країні [216, с. 14]. Отже, види інформаційної безпеки можуть виділятися й залежно від змісту прав і свобод в інформаційній сфері.

Головною класифікацією інформаційної безпеки для нашого дослідження є визначення видів суспільних відносин, що її складають, за ознакою змісту структурних елементів досліджуваної категорії: інформаційна безпека у сфері формування інформаційного ресурсу; інформаційна безпека у сфері забезпечення доступу до інформаційного ресурсу; інформаційна безпека у сфері використання інформаційних технологій. Це положення потребує певного обґрунтування. Дійсно, чому серед наявних у науці класифікацій інформаційної безпеки (за джерелом інформаційних потреб, об'єктом загроз, сферами суспільного життя, складовими інформаційного процесу, змістом прав і свобод в інформаційній сфері) для дослідження її кримінально-правової охорони було обрано класифікацію за змістом структурних елементів? Як відомо, класифі-

кація є такою формою систематизації знань, коли вся ділянка об'єктів, що вивчаються, подана у вигляді системи класів або груп, за якими вони розподілені на підставі їх подібності у певних властивостях. При цьому класифікація покликана вирішувати два основні завдання: подавати в надійному та зручному для огляду й розпізнавання вигляді всю цю ділянку й містити в собі максимально повну інформацію про її об'єкти [253]. Отже, класифікація, яка використовується в цьому дослідженні, повинна бути такою, щоб чітко та рельєфно представляти види відповідних суспільних відносин інформаційної безпеки залежно від специфіки кримінально-правових засобів, які використовуються для їх охорони. Очевидно, що специфіка таких засобів визначається змістом певних суспільних відносин. Тому класифікація суспільних відносин інформаційної безпеки за змістом і визначає структуру подальшого розгляду кримінально-правових заходів охорони інформаційної безпеки. Так, у подальших главах будуть проаналізовані три групи кримінально-правових заборон, які відповідають визначеним структурним елементам інформаційної безпеки. По-перше, злочини у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку будуть розглянуті як кримінально-правові засоби охорони інформаційної безпеки у сфері використання інформаційних технологій. По-друге, злочини, що являють собою незаконні дії з інформацією з обмеженим доступом та протиправне обмеження доступу до інформації, – як кримінально-правові засоби охорони інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу. По-третє, протиправні дії пов'язані зі створенням інформаційних ресурсів, інформатизацією, включенням до суспільного дискурсу провокативної, дестабілізуючої інформації, – як кримінально-правові засоби охорони інформаційної безпеки у сфері формування інформаційного ресурсу.

1.2. Соціальні потреби в кримінально-правовій охороні інформаційної безпеки України

Необхідність у кримінально-правовій охороні суспільних відносини виникає тоді, коли вони набувають певного значення та посягання на них стають суспільно небезпечними. Для того щоб установити, чи потребують заходів кримінально-правової охорони відносини інформаційної безпеки, а якщо так, то якого змісту, необхідно дійти висновків щодо суспільної значущості процесів інформатизації, векторів змін сучасного суспільства у цій сфері, які мають істотне значення для його позитивних трансформацій у бік розвитку та стабільності, а також тих, які, навпаки, мають небезпечний потенціал. Це дозволить визначити соціальні потреби в кримінально-правовій охороні інформаційної безпеки, створити обґрунтовану систему критеріїв оцінки якості засобів кримінально-правової охорони інформаційної безпеки, оскільки кінцевою метою як правового регулювання інформаційної безпеки взагалі, так і її кримінально-правової охорони зокрема, є забезпечення розвитку суспільно значущих тенденцій інформатизації та попередження ризиків загострення негативних наслідків асоціального використання інформатизації.

Отже, необхідним елементом наукового дослідження питань кримінальної відповідальності за посягання на інформаційну безпеку є аналіз концепцій інформаційного суспільства та дослідження висновків науковців щодо соціальних наслідків інформатизації, який і буде проведено в цій підглаві.

Зазначимо, що в сучасному науковому дискурсі використовується велика кількість визначень, для того щоб більш наочно відобразити соціальні зміни, які зумовлені технологічним прогресом в інформаційній сфері та пов'язаними з ним суспільними трансформаціями. Крім терміна "інформаційне суспільство" використовуються й такі поняття, як "мережеве суспільство", "суспільство знань", "постіндустріальне суспільство", "пізній модернізм" [258, с. 82] тощо. У нашому дослідженні по-

няття "інформаційне суспільство" будемо використовувати в найширшому розумінні, як сукупний масив соціальних, економічних, політичних, культурних і технічних тенденцій розвитку сучасного суспільства, зумовлених його інформатизацією та комп'ютеризацією.

Окремо зауважимо, що в ході дослідження сутнісних ознак інформаційного суспільства ми будемо керуватися принципом різноманіття підходів. Слід погодитися з Н.П. Лукіною в тому, що складність процесів, які відбуваються в сучасному суспільстві, потребують "зміщення дослідницького ракурсу, що в першу чергу передбачає відмову від принципу методологічної одноманітності при розгляді суспільства… Принцип різноманіття підходів полягає не стільки у визнанні наявності рівнозначних стандартів раціональності, скільки у визнанні обмеженості кожного з них. Ця обмеженість долається шляхом можливості переходу від одного підходу до іншого, спираючись на методологічний принцип доповнення" [219]. Отже, шляхом аналізу комплексу наукових концепцій інформаційного суспільства, керуючись принципом різноманіття підходів та спираючись на методологічний принцип доповнення, ми встановимо систему соціально корисних та соціально небезпечних тенденцій інформатизації.

Історично перші наукові дослідження у сфері інформаційного суспільства містили так зване *технологічне* визначення. Автори, які дотримуються такої точки зору, уважають, що інформаційне суспільство має місце тоді, коли бурхливо розвиваються та широко використовуються інформаційно-комунікаційні технології. Відповідно до такого бачення саме технології виступають тим чинником, під впливом якого відбуваються зміни в суспільстві, вони забезпечують трансформацію сучасного соціуму на майбутнє більш безпечне та досконале, на думку більшості прибічників технологічного визначення, "інформаційне суспільство". З технологічним підходом пов'язується і поява в науковому обігу цього терміна. Першим, як уважається, його використав професор Токійського техноло-

гічного інституту Ю. Хайяші. На той час, наприкінці 1960-х – на початку 1970-х років, контури інформаційного суспільства були окреслені у звітах, представлених японському урядові низкою організацій, зокрема: Агентством економічного планування (англ. EPA: Economic Planning Agency) – "Японське Інформаційне суспільство: теми і підходи"; Інститутом розробки використання комп'ютерів (англ. JACUDI: Japan Computer Usage Development Institute) – "План інформаційного суспільства"; Радою з питань структури промисловості (англ. ISC: Industrial Structure Council) – "Контури політики сприяння інформатизації японського суспільства". У згаданих звітах інформаційне суспільство визначалось як суспільство, у якому процес комп'ютеризації надасть людям доступ до надійних джерел інформації, звільнить їх від рутинної роботи, забезпечить високий рівень автоматизації виробництва [383, с. 91 – 92].

Подальший розвиток концепції інформаційного суспільства, що ґрунтується на технологічному поясненні трансформації соціальних процесів, пов'язаний з іменами таких всесвітньо відомих соціологів і футурологів, як Йонедзі Масуда та Елвін Тофлер. До прибічників технологічного визначення інформаційного суспільства належить і відомий американський політолог Збігнев Бжезинський. "Постіндустріальне суспільство, – стверджує він, – стає технотронним суспільством – суспільством, що в культурному, психологічному, соціальному й економічному відношенні формується під впливом техніки й електроніки, особливо розвинених у галузі комп'ютерів і комунікацій" [395, с. 9].

Незважаючи на зовнішню послідовність і відповідність технологічних визначень дійсності, не можна не погодитися з критичними зауваженнями щодо такого бачення інформаційного суспільства, які висловив професор City University of London Френк Уебстер. По-перше, доволі складно визначити "точку на технологічній шкалі, досягши якої суспільство можна вважати інформаційним". По-друге, неправильно вважати позасоціальний феномен (технологію) чинником, що визначає розвиток суспільства. Технологія сама є результатом розв'язан-

ня певних соціальних потреб, і вважати її самодостатнім чинником соціальних трансформацій непослідовно [361, с. 17]. Досить різка критика подібних підходів міститься й у відомій роботі Девіда Лайона "Інформаційне суспільство: проблеми та ілюзії". Він зауважує: "…там, де ідея інформаційного суспільства залежить від версій технологічного детермінізму, вона повинна зустріти опір. Такий детермінізм є демонстративно фальшивим. Технологічний розвиток не має заздалегідь встановлених соціальних ефектів, відносно яких можна передбачити, чи є вони благотворними універсально, чи лише для даного випадку. Його можна представити як похідний від самого соціального утворення, включаючи деякі навмисні політичні, економічні й культурні уподобання" [203].

Головним висновком із технологічних підходів, корисним для цілей нашого дослідження, є фіксація того, наскільки велике значення в сучасному суспільстві мають інформаційно-комунікаційні технології. Очевидним є той факт, що соціальне значення відносин у сфері використання інформаційних технологій дозволяє використовувати кримінально-правові засоби для їх охорони. При цьому зауважимо, що значення це є не самостійним, технології важливі не самі по собі, а лише у зв'язку з тим видом соціальної активності, для автоматизації чи інтенсифікації якої вони використовуються.

Подальший розвиток теорій інформаційного суспільства відбувається в контексті дослідження специфічних тенденцій розвитку економічних і політичних відносин, змін у структурі зайнятості населення, особливостей організації діяльності людини в ході розвитку глобальних інформаційних мереж, трансформацій культурної складової суспільства тощо.

Достатньо знаковою віхою в розвитку теорій інформаційного суспільства стала поява в 1973 році роботи професора Гарвардського університету Деніела Белла "Прихід постіндустріального суспільства. Досвід соціального прогнозування" (The Coming of Post-Industrial Society: A Venture in Social Forecasting). З цим дослідженням, як правило, асоціюється визначен-

ня інформаційного суспільства за *критерієм зайнятості населення* [394]. Зауважимо, що Д. Белл використовує терміни "інформаційне суспільство" та "постіндустріальне суспільство" майже як синонімічні: інформаційне століття він розглядає як відображення постіндустріального суспільства, а постіндустріалізм – як інформаційне суспільство [361, с. 43].

У типології суспільного устрою, яку запропонував Д. Белл, роль критерію відіграє домінуючий на певній стадії вид найманої праці, саме він є визначальною рисою того чи іншого суспільства. Так, якщо в доіндустріальних суспільствах переважав сільськогосподарський труд, а в індустріальних найбільш поширеною була праця на виробництвах, то в постіндустріальному суспільстві більшість зайнятих працює у сфері послуг. Ці зміни Д. Белл пояснює зростанням продуктивності праці. Перехід від доіндустріального до індустріального суспільства був забезпечений зростанням результативності сільськогосподарського виробництва, що дозволило звільнити частину зайнятих в аграрному секторі та задіяти їх у промисловому виробництві. Подальша трансформація зумовлена розвитком механізації та автоматизації, завдяки яким стає можливо виробляти дедалі більший обсяг продукції за участю все меншої кількості працівників. Отже, більшість зайнятих переходить до сфери послуг, яка швидко розвивається завдяки зростанню продуктивності сільського господарства та промисловості. При цьому робота у сфері послуг є, по суті, інформаційною, оскільки послуги являють собою взаємодію з людьми, яка здійснюється на основі інформації. Саме це якісно відрізняє постіндустріальне (інформаційне) суспільство від індустріального, що характеризується взаємодією зі зміненою природою на основі енергії, та доіндустріального, де домінувала взаємодія з природою на основі "грубої мускульної сили" [394, с. 126; наводиться за 361, с. 55]. Такі зміни в структурі зайнятості, а також те, що предметом праці більшості населення є інформація, зумовлюють такі ключові характеристики інформаційного суспільства: перехід від товаровиробничої до обслуговую-

чої економіки; перевага професійно-технічного класу; провідна суспільна роль теоретичного знання як джерела нововведень і політичних формулювань [18]. Пояснюючи провідну роль теоретичного знання, Ф. Уебстер зазначає, що в попередні епохи домінувало практичне та ситуативне знання; за словами Д. Белла, промислову революцію творили "талановиті вигадники, яким наука та фундаментальні закони, що складали основу їх винаходів, були байдужі" [394, с. 20; наводиться за 361, с. 38]. Сьогодні, навпаки, первинним є не досвід чи ситуативна потреба, а принципове знання, з найбільшою очевидністю це проявляється у сфері науки та технологій. Важко уявити собі реальність такого проекту, як, наприклад, "Геном людини", без наявності глибоких теоретичних напрацювань у його стартовій точці.

Для нашого дослідження важливими результатами роботи Д. Белла є обґрунтування суспільної значущості інформації: вона є предметом праці більшості населення, саме завдяки їй забезпечується найбільш поширений в інформаційному суспільстві вид діяльності – надання послуг. Крім того, сформульовані сучасною соціологічною наукою положення щодо підвищення значущості теоретичного знання повертають нас до важливості розв'язання проблемних питань щодо захисту авторського права та інтелектуальної власності в сучасних умовах, актуалізують дослідження доцільності та меж застосування відповідних засобів кримінальної юстиції.

Так зване *економічне* визначення інформаційного суспільства відображає тенденції зростання економічної цінності інформаційної діяльності. Дослідники, які дотримуються такої точки зору, уважають, що про інформаційне суспільство можна говорити тоді, коли в економічній сфері інформаційна активність превалює над діяльністю в галузі сільського господарства та промисловості [408, наводиться за 361]. Найбільш відомими представниками такого підходу є Фриц Махлуп [411] та Марк Порат [417]. Підхід цей має право на існування через об'єктивні характеристики сучасних економічних процесів.

Так, за даними російських дослідників, обсяг продукції інформаційної індустрії, що випускається сьогодні, сягає у вартісному вираженні одного трильйона доларів США та може перевищити обсяг ринку природних ресурсів. Уже в 1994 році близько 11% світового експорту товарів у вартісному вираженні припадало на офісне та телекомунікаційне обладнання, включаючи комп'ютери та їх комплектуючі, що перевищувало обсяг торгівлі продовольчими товарами, нафтохімічними продуктами й автомобілями [291, с. 3].

Необхідно зазначити, що такий підхід досить активно критикується. Звертається увага на принципову недосконалість запропонованих методів обчислення інформаційної діяльності. Наприклад, дуже складно встановити, до якого сектору слід відносити виконання управлінських функцій, які є невід'ємним елементом виробництва, або роботу технічного персоналу в такій типово інформаційній сфері, як освіта. Отже, головне зауваження полягає в тому, що практично неможливо виокремити інформаційну діяльність у чистому вигляді: як правило, вона виступає складовою інших видів діяльності. Ф. Уебстер зазначає, що подібні підходи мають оцінний характер, а отже, "не розвіюють скептицизму стосовно самої ідеї виникнення інформаційної економіки" [361, с. 20].

Для нашого дослідження тут важливі дві речі: 1) велика економічна значущість відносин, пов'язаних з інформацією; 2) принципова неможливість виділення інформаційного сектору, свого значення він набуває як складова інших видів діяльності. Ми стикаємося з проблемою, на яку вже звертали увагу під час розгляду технологічного критерію: як техніка не має значення сама по собі, а набуває його тільки в контексті певної соціальної активності, так і інформаційний сектор економіки навряд чи може бути виділений у "чистому вигляді", а не як сукупність складових різних видів діяльності інших секторів економіки. Отже, на рівні кримінально-правової охорони обов'язково мають ураховуватися такі специфічні характеристики суспільної небезпечності посягань на інформаційну без-

пеку, як велика економічна значущість інформації, а також її несамостійний, похідний характер.

Важливі дослідження сучасних тенденцій інформатизації суспільства в контексті економічної складової здійснили й науковці так званої школи регулювання Ален Ліпіц [410] та Мішель Альєтта [1]. Фундаментальним питанням школи регулювання є дослідження того, яким чином капіталізм забезпечує собі тривале існування. Для цього вони аналізують режим накопичення капіталу, який превалює в той чи інший період, та способи регулювання, використання яких дозволяє здійснювати соціальний контроль [361, с. 85 – 87].

На думку дослідників школи регулювання, сьогодні домінує так званий постфордистський режим накопичення капіталу. Основною причиною появи такого способу накопичення стала глобалізація та поява великих транснаціональних корпорацій. Розглядаючи концепції представників школи регулювання, Ф. Уебстер виокремлює її чотири особливо важливі складові: глобалізація ринку, виробництва, фінансів та комунікацій [361, с. 94 – 97]. Глобалізація ринку полягає в тому, що основні корпорації працюють сьогодні з урахуванням того, що їх ринком збуту стає весь світ. Глобальні виробничі стратегії, глобалізація виробництва полягають у децентралізації виробництва, широкому використанні аутсорсингових рішень тощо. Глобалізація фінансів являє собою інтегрований фінансовий ринок, що постійно зростає. Нарешті, глобалізація комунікацій означає появу та широке розповсюдження комунікаційних мереж, які об'єднують весь світ. За умов таких характеристик сучасного режиму накопичення капіталу ключового значення набуває інформаційна інфраструктура, оскільки вона: 1) є необхідною умовою керування глобальними виробничими та маркетинговими стратегіями; 2) необхідна для ведення глобальної фінансової діяльності; 3) забезпечує належний рівень контролю якості виробництва; 4) створює умови для впровадження інновацій.

Отже, представники школи регулювання порушують ще одне питання, важливе для дослідження кримінально-правової охорони інформаційної безпеки, – значення інформації та інформаційних технологій у контексті тенденцій глобалізації економіки. Вони обґрунтовано доводять, що інформація та інформаційні технології є необхідною умовою стабільності постфордистського режиму накопичення капіталу. Доречним буде приклад, який пропонує В.А. Лужецький. Акцентуючи увагу на суспільній небезпечності посягань на інформаційну безпеку в умовах глобалізації економіки, він наводить витяг з інтерв'ю з М. Дюре, директором Центру інформації та документації НАТО в Україні. Експерт з питань інформаційної безпеки зазначає, що свого часу планувалася терористична атака на Нью-Йоркську біржу, метою терористів були комп'ютерні системи, що зберігають та обробляють інформацію про торгові операції в США та Європі. Наслідки такого терористичного акту могли призвести до кризи світового масштабу [218, с. 35].

Важливі аспекти інформатизації аналізує професор Каліфорнійського університету в Сан-Дієго Герберт Шиллер. Для нього зміни, які відбуваються в суспільстві, не означають появу його нового типу. Головні імперативи ринкової економіки залишаються без змін, які б трансформації не відбувалися в технологічній та інформаційній сферах [418, наводиться за 361, с. 169].

На думку Г. Шиллера, в інформаційній сфері домінують інтереси корпоративного капіталізму. Розвиток інформаційних технологій відбувається в інтересах приватного бізнесу, а не суспільства загалом. Ураховуючи означені положення, Г. Шиллер аналізує небезпеки сучасного інформаційного простору. Так, він зазначає, що зміст повідомлень у засобах мАсової інформації визначається тим, чи забезпечить він більшу аудиторію для реклами. Це приводить до збільшення кількості інформації, але не до покращення інформованості населення. Інформаційне наповнення засобів масової інформації є таким, яке не вимагає мислення, не стосується політично спірних питань, але допомагає зібрати максимальну аудиторію, яка приваблює спонсорів та рекламодавців [361, с. 176]. Також Г. Шиллер аналізує вплив інформаційної сфери на розвиток конс'юмеризму, він зазначає, що створений "інформаційний ковпак" використовується для того, щоб упровадити ринкові категорії в усі сфери життя людини, і головна з них – споживання. Крім цього, капіталізація інформаційної сфери, зауважує дослідник, відбувається і в глобальному масштабі, що створює небезпеку втрати культурної ідентичності країнами з менш розвиненим інформаційним сектором. Він ідентифікує такі процеси як "культурний імперіалізм", використання інформації для збереження західного панування в економічній та політичній сферах [361, с. 180].

Таким чином, до особливостей сучасного інформаційного суспільства слід додати небезпеки функціонування інформаційної сфери, пов'язані з її капіталізацією. Дослідження Г. Шиллера ставлять питання про побудову ефективного механізму контролю за розвитком та функціонуванням медійного бізнесу та попередження його негативних соціальних наслідків. Тому до актуальних завдань дослідження засобів кримінально-правової охорони інформаційної безпеки треба також віднести аналіз доцільності та меж використання засобів кримінальної юстиції для мінімізації негативних проявів комерціалізації інформаційного простору.

Серед досліджень, пов'язаних із небезпеками маніпулятивного інформаційного впливу та його небезпек, варто відзначити роботи німецького філософа Юргена Габермаса. Він уважав, що поширені форми "технократичного розуму" являють собою серйозну загрозу людській свободі. Суспільна сфера комунікацій і прийняття рішень так усе перекручує, що більша частина населення перебуває в цілковитому невіданні стосовно реального розподілу влади й контролю в суспільстві. Габермас говорив, що політичні дебати систематично зводяться до суто технічного рівня і водночас технологія стає майже конкурентом політики. Зведення політичних дебатів до технічних

засобів веде до того, що люди втрачають можливість брати в них участь на рівні моралі та справедливості й, отже, можливість шляхом політичних дій впливати на їх результати [203].

Проблеми інформаційного суспільства Ю. Габермас розглядає крізь призму концепції публічної сфери. Це була сфера, яка дозволяла будь-якому бажаючому раціонально обговорити проблему, провести дискусію, учасники якої особисто не заінтересовані, а тому не підтасовують її результатів. Саме в цій сфері й формувалася суспільна думка. Інформація слугувала становим хребтом публічної сфери, передбачалося, що учасники публічних дискусій чітко викладуть свої позиції, а широка публіка ознайомиться з ними та усвідомить те, що відбувається. Формування публічної сфери Габермас розглядає на прикладі Великобританії XVIII – XIX ст., він зазначає, що до середини XIX ст. у цій країні було створено буржуазну публічну сферу з її головними рисами: відкритою дискусією, критикою дій влади, повною підзвітністю, гласністю та незалежністю дійових осіб від економічних інтересів та контролю держави [361, с. 220 – 222].

Однак із розвитком капіталізму почало відбуватися "взаємопроникнення" відносин приватної власності та публічної сфери. Прибічники капіталістичної держави стали частіше переходити від дебатів та агітації до використання держави, у якій тепер домінували, у боротьбі за свої особисті інтереси [361, с. 222]. Інформаційні технології, зокрема піар, внесли до публічної сфери маскарад, який використовується учасниками для того, щоб приховати дійсні інтереси під час міркувань про "суспільство загального добробуту" або "національні інтереси". Усе це дає Ю. Габермасу підстави називати сучасну політичну дискусію "підробкою" справжньої публічної сфери, говорити про перетворення політичного життя на шоу, яке розігрується перед обдуреними "глядачами, які тут же готові до нього приєднатися" [405, с. 195, наводиться за 361, с. 223, 225].

Для нашого дослідження суттєвим у роботах Ю. Габермаса є акцент на залежності політичного життя країни від можливих маніпуляцій, які взагалі ставлять під сумнів можливість демократичного розвитку країни. Отже, маємо ще один аспект суспільної небезпечності посягань на інформаційну безпеку. Оскільки важливою характеристикою сучасного суспільства є складна система політичної участі, яка забезпечується сучасними інформаційними технологіями, наслідки посягань у сфері інформаційної безпеки можуть мати не тільки економічний, але й політичний характер.

Важливі характеристики інформаційного суспільства розглядає відомий англійський соціолог, доктор філософії Кембриджського університету Ентоні Гідденс. Зауважимо, що для нього інформаційне суспільство не є новим типом соціального устрою. "Хоч зазвичай припускають, що ми тільки вступаємо в нову епоху інформації, насправді сучасне суспільство було "інформаційним" від самого свого початку" [403, наводиться за 361, с. 276]. Е. Гідденс уважає, що в сучасному світі відбулася "інформатизація" соціальних зв'язків, але це не означає, що ми наближаємося до нового суспільства [361, с. 276].

Вихідним положенням його теоретичної конструкції є таке: світ, у якому ми живемо, організований набагато більше, наше життя заплановане та впорядковане так, як ніколи раніше. Щоб така високоорганізована форма суспільних зв'язків могла існувати, необхідним є систематичне збирання інформації про індивідів та їх діяльність. Модернізація суспільства – це збільшення можливостей вибору для його членів. Однак модернізація потребує підвищення рефлективності на кожному рівні організації суспільства. Під зростанням рефлективності Е. Гідденс розуміє більш повне відстеження ситуації (збирання інформації), яке дозволяє накопичувати знання, необхідні для здійснення вибору. Саме необхідність здійснювати вибір в умовах суспільства, що ускладнюється, зумовлює підвищену потребу в інформації, розвиток інформаційних технологій, засобів масової інформації тощо [361, с. 277 – 280].

У своїй основі всі держави – "інформаційні суспільства", оскільки державна влада передбачає рефлексивне збирання, зберігання інформації, яка необхідна для адміністрування, та

управління нею [404, с. 178, наводиться за 361, с. 286]. Основні цілі збирання інформації державою полягають у забезпеченні національної безпеки, контролі за виконанням громадянських обов'язків та створенні можливостей для реалізації прав громадян. При цьому Е. Гідденс висловлює глибоке занепокоєння з приводу того, що накопичення державними інституціями великих обсягів інформації, яке є логічним наслідком розвитку національної держави, створює загрозу демократичному розвитку, "тоталітаризм залишається загрозою" у всіх промислово розвинених країнах через безпрецедентні масштаби збирання інформації [404, с. 310, наводиться за 361, с. 305].

Поза увагою дослідника не залишаються й питання збирання інформації великими бізнес-структурами. "При капіталістичному способі виробництва відстеження – ключовий елемент менеджменту" [403, с. 27, наводиться за 361, с. 276]. Комерційний сектор має широкі можливості збирання інформації про особу. Так, за умов сучасного рівня інформатизації не викликає складнощів з'ясування того, які товари, у якій кількості, де та з якою періодичністю придбаває особа, які інформаційні канали кабельного мовлення або ресурси Інтернет використовує для задоволення інформаційних потреб, як часто розмовляє по телефону тощо. Звичайно, що така інформація допомагає суб'єктам господарювання поліпшити стратегію продажів, зробити рекламну кампанію більш прицільною, але водночас у цьому криється небезпека системних порушень прав на повагу до приватного життя.

Таким чином, Е. Гідденс звертає увагу на становище, яке є важливим для дослідження кримінально-правової охорони інформаційної безпеки: організація сучасного суспільства обов'язковою умовою функціонування передбачає збирання інформації про особу; технології, які використовуються, дозволяють шляхом збирання та накопичення великих обсягів інформації забезпечити реальне покращення життя кожного, надаючи йому можливість широкого вибору варіантів поведінки, одночасно це створює суспільно небезпечні загрози – від порушень права на повагу до приватного життя до розвитку тоталітарного керування суспільством. Крім цього, висновки Е. Гідденса щодо надзвичайної організаційної ускладненості сучасного суспільства з необхідністю ставлять питання нових форм захисту цієї організації. Очевидно, що більш складну систему набагато легше вивести з ладу, ніж просту, отже, сучасне суспільство через власну ускладненість має більше ризиків втрати стабільності.

Серед наукових підходів до визначення основних характеристик інформаційного суспільства окреме місце займають теорії, що використовують основною ознакою суспільства нового типу так званий *просторовий* критерій. Він полягає в тому, що в суспільстві нового типу інформаційні мережі чинять глибокий вплив на організацію часу та простору. У мережевому суспільстві ускладнення, пов'язані з часом та простором, багато в чому подолані; корпорації та окремі особи мають змогу ефективно вести свої справи в глобальному масштабі, дослідникам немає необхідності вирушати у відрядження для відвідування бібліотек, оскільки є можливість доступу до мережевих інформаційних ресурсів, менеджерам корпорацій не треба перелітати через континенти, щоб з'ясувати, як працюють філії на Далекому Сході, оскільки комп'ютерна мережа надає можливість постійного дистанційного спостереження за ходом робіт [361, с. 26]. На думку багатьох дослідників, це свідчить про серйозну трансформацію соціального устрою [416, наводиться за 361].

Найбільш відомою науковою розробкою питань впливу комунікаційних технологій на суспільство є дослідження професора Каліфорнійського університету в Берклі Мануеля Кастельса, викладене в його трилогії "Інформаційна доба: економіка, суспільство, культура" [398; 397; 396]. На його думку, новий світ зародився наприкінці 1960-х – у середині 1970-х рр. унаслідок трьох незалежних процесів: 1) революції інформаційних технологій; 2) кризи як капіталізму, так і етатизму; 3) розквіту культурних суспільних рухів, таких як лібертаріа-

нізм, боротьба за права людини, фемінізм, захист навколишнього середовища. Взаємодія між цими процесами та спровоковані ними реакції створили нову домінуючу соціальну структуру – мережеве суспільство; нову економіку – інформаціональну/глобальну і нову культуру – культуру реальної віртуальності.

Ключовою трансформацією в економічний сфері є те, що "незважаючи на широке різноманіття соціальних та культурних ландшафтів, уперше в історії життя всієї планети організоване значною мірою відповідно до загальних економічних правил" [123]. Нову форму капіталізму дослідник називає інформаціональним капіталізмом. Він має специфічні особливості виробничого процесу, праці та капіталу. Виробничий процес розвивається в напрямку збільшення інновацій та гнучкості з метою забезпечення глобально орієнтованого підвищення продуктивності та конкурентоспроможності. Праця диференціюється згідно з характеристиками працівників на "родову" та "працю, що самопрограмується". Головна різниця полягає в тому, що працівники, які відносяться до останньої категорії, здатні шляхом освіти змінювати свої навички, пристосовуючи їх до завдань процесу виробництва, які постійно змінюються. Головною особливістю капіталу є наявність глобальних фінансових ринків, які М. Кастельс відносить до фундаментальних особливостей нового інформаціонального капіталізму. "Фірми всіх видів, фінансові, промислові, сільськогосподарські виробники, виробники послуг, а також уряди та громадські організації використовують глобальні фінансові мережі як депозитарії своїх доходів і як потенційні джерела більш високих прибутків. Саме в цій специфічній формі глобальні фінансові мережі є нервовим центром інформаціонального капіталізму" [123].

Через істотні зміни в економіці з'являються й принципово нові характеристики суспільного устрою. Найбільш важливою характеристикою соціальних зрушень, за М. Кастельсом, є те, що включеність до мережі розглядається як умова повноцінної участі в житті суспільства. Стверджується, що доступ до інформаційно-комунікаційних технологій визначає права громадя-

нина в інформаційній добі [361, с. 142]. Разом із цим, до чинників суспільних негараздів дослідник відносить такі "фундаментальні соціальні розломи": внутрішня фрагментація робочої сили на інформаціональних виробників та родову робочу силу; соціальне виключення значного сегменту суспільства, який складається з індивідів, чия цінність як працівників/споживачів вичерпана та чия значущість як людей ігнорується. Крім того, мережеве суспільство характеризується кризою національної держави як суверенної одиниці, оскільки з широким включенням у глобалізаційні процеси нова структура влади характеризується домінуванням "мережевої геометрії, у якій відносини влади завжди специфічні для цієї конфігурації акторів та інститутів" [123]. У контексті соціальних змін дослідник звертає увагу й на трансформацію відносин досвіду, які головним чином пов'язані з кризою патріархальності, зумовлені такими глобалізованими суспільними рухами, як фемінізм і сексуальна революція.

Основні зрушення в культурному контексті М. Кастельс пов'язує з реальною віртуальністю, що являє собою систему, у якій сама реальність (тобто матеріальне/символічне існування людей) повністю занурена в установлення віртуальних образів, у світ створюваних переконань, де символи є не просто метафорами, а містять у собі актуальний досвід. Важлива особливість культури реальної віртуальності полягає в тому, що вона формується в умовах так званого "простору потоків" та "позачасового часу". Домінантні функції та цінності суспільства організовані в просторі потоків інформації, що уникають досвіду, пов'язаного з місцем їх походження. Крім того, ці функції та цінності конструюються безвідносно до минулого та майбутнього, тобто в позачасовому часі. "Усі відображення з усіх часів та всіх просторів змішуються в одному й тому ж гіпертексті, який постійно реорганізується та є доступним у будь-який час та звідки завгодно, залежно від інтересів відправників та схильностей отримувачів. Ця віртуальність є нашою реальністю внаслідок того, що саме в цьому полі позачасових, позбавлених місця символічних систем ми конструюємо кате-

горії та викликаємо образи, які формують поведінку, запускають політичний процес, викликають сни та породжують кошмари" [123].

Виявлені особливості дозволяють М. Кастельсу стверджувати, що "наші суспільства – не впорядковані в'язниці, а безладні джунглі", та прогнозувати, що в майбутньому на нас чекає "інформована плутанина". "Існує екстраординарний розрив між нашою технологічною надрозвиненістю та нашою соціальною недорозвиненістю. Наші економіка, суспільство та культура побудовані на інтересах, цінностях, інститутах та системах уявлень, які загалом обмежують колективну креативність, конфіскують плоди інформаційної технології та відхиляють нашу енергію в бік самознищуючої конфронтації" [123].

Важливими в контексті дослідження кримінально-правових засобів охорони інформаційної безпеки є, як ми вважаємо, такі положення теорії інформаціонального капіталізму: 1) доступ до інформаційно-комунікаційних технологій набуває для сучасної людини значення, яке важко переоцінити; 2) існує великий потенціал соціальних конфліктів, який можна задіяти інформаційними засобами; 3) наявною є реальна небезпека виключення з процесів, що відбуваються у світовій економіці, через неготовність здійснювати інноваційне та гнучке виробництво; 4) історично безпрецедентна глобалізація фінансового ринку, організаційно побудованого на використанні сучасних інформаційних технологій, створює ризик посягань з надзвичайно великим ступенем небезпеки.

Розгляд концепцій інформаційного суспільства був би неповним без дослідження концепцій інформаційного суспільства, що базуються на так званому *культурному* критерії. Для науковців, які дотримуються таких поглядів, найбільш визначальною рисою сучасного суспільства є набагато більша інформативність сучасної культури, ніж будь-якої попередньої. Життя істотно символізується, воно проходить у процесах обміну повідомленнями, спостерігається вибухове зростання знаків. Однак таке зростання знаків приводить багатьох дослідників до парадоксального висновку: зі зростанням своєї кількості знаки втрачають вагу. Так, Жан Бодіяр зазначає: "Знаків стає все більше, а сенсу все менше" [393, с. 95, наводиться за 361, с. 29]. Російська дослідниця І.О. Мальковська констатує, що у величезному комунікаційному просторі, через надлишковість інформації (ексформації), загострюються проблеми втрати смислів [223, с. 77]. М.М. Павликова зазначає, що ми тонемо в інформації, але в знаннях відчуваємо голод, і наводить думку нобелевського лауреата, економіста Герберта Саймона: "... сьогоднішня інформація винищує та поїдає увагу своїх споживачів" [258, с. 83].

Найбільш ретельно ці та пов'язані з ними проблеми досліджували представники постмодерністської інтелектуальної традиції. Професор Ф. Уебстер, зауваживши, що сам не поділяє поглядів постмодерністів, до особливостей їх концепцій відносить такі: неприйняття будь-яких претензій на встановлення істини, оскільки існують тільки її версії; неприйняття намагань уточнення смислу, оскільки смислів – нескінченна множина, і це робить безнадійним сам пошук смислів; задоволення від поверхового, уявного, розмаїття, змін, пародій та стилізацій [361, с. 330 – 331]. Відповідаючи, наприклад, на побоювання Г. Шиллера та Ю. Габермаса щодо маніпуляцій свідомістю за допомогою знаків, які не відповідають дійсності, постмодерністи відзначають, що "аудиторія зовсім не складається з людей, "підсаджених на іглу" хитромудрих знаків, чого так боялися ідеологи сучасного суспільства. Насправді аудиторія взагалі нічого не бачить та не чує, вона просто насолоджується тим спектаклем, який розігрує для неї сучасне суспільство" [361, с. 341]. Оскільки щодня ЗМІ завалюють кожного величезною кількістю різних інтерпретацій фактів і абсолютно по-різному визначають коло подій, то як можна говорити про єдину для всіх реальність? [361, с. 342].

Для нашого дослідження важливим є сам факт існування постмодерністських концепцій. Він демонструє специфічні наслідки надмірного насичення соціального буття інформацією.

За втратою знаками смислу, неприйняттям теоретичного знання, поверховим ставленням до інформації через відсутність у ній смислу та сприйняття її виключно як розваги, як видається, криється небезпека тотальної втрати принципових навичок роботи з інформацією. Соціологи зазначають, що один із парадоксів сучасного інформаційного суспільства полягає в тому, що "суспільство знань" дуже стрімко продукує "суспільство нічогонезнайок" [223, с. 77]. Представники психологічної науки підтверджують ці висновки, але в більш різкій та категоричній формі. Так, Т. Росінчук указує на такі негативні наслідки ущільнення інформаційних потоків і розширення сфери застосування інформаційних технологій, як: 1) витіснення писемного мовлення (читання і письма), яке є найважливішим інструментом особистого розвитку, та, як наслідок, руйнування мовлення у дітей 5 – 10 років; 2) зниження культури мислення у молоді; 3) небезпека інволюції, процесу, зворотного еволюції [303, с. 92 – 94]. У книзі "iBrain: Як пережити технологічну зміну мозку" її автор Г. Смолл зазначає: "...оскільки Інтернет зменшує здатність концентруватися та споглядати, … мислення стає уривчастим, читання – поверховим. Користувачі лише по діагоналі проглядають заголовки та анотації. А зони мозку, що відповідають за абстрактне мислення … практично атрофуються". "Інтернет створює лише ілюзію доступності інформації та технічної оснащеності, – каже автор монографії "Походження мозку" С. Савельєв. – У так званих "цифрових аборигенів" навантаження на мозок постійно знижується... Інтелектуальна деґрадація в таких умовах ґарантована" [195].

Самостійною проблемою та визначальною ознакою інформаційного сучасного суспільства є також втрата державою своїх позицій у сфері суспільного контролю. Сучасні дослідники формулюють так званий парадокс "інтеґрації-дезінтеґрації". Л.П. Нагорна зазначає, що поширені нещодавно очікування електронної демократії, гібридної ідентичності з прозорими кордонами, космополітичної етики відповідальності не справдилися. "Навпаки, побічним ефектом глобалізації та все-

світньої комунікації стала активізація явищ гетерогенності, локалізації, фраґментації, що змусило політологів спішно уводити в обіг гібридні терміни – "глокалізація", "глоболокалізм", "фраґмеграція" тощо" [243, с. 4]. Отже, означений парадокс полягає в тому, що хоча комунікаційні мережі забезпечують певну інтеґрацію людського суспільства, власне зв'язок між людьми відсутній, існує його ілюзія, створена інформаційними технологіями. Насправді ж соціальні контакти втрачають свою інтенсивність [223, с. 79]. Втрата цих контактів, а відповідно, і зменшення ефективності механізму критичного оцінювання інформації, що надходить, призводить до того, що молоді громадяни стрімко втрачають уявлення про навколишню реальність та своє місце в ній; насичення інформаційного простору автоматично не створює організованого суспільного простору, призводить до проблеми "втрати реальності" [223, с. 78]. Крім того, за умов фраґментації суспільства значно підвищується ймовірність маніпулювання суспільною свідомістю. Усе це спричиняє ситуацію, коли віртуальний світ стає реальним за своєю значущістю для людини та суспільства, а держава, навпаки, стає для них віртуальною [214, с. 5]. За даними соціологів, на початку нашого століття 2/3 громадян у світі не ідентифікували себе з державою та не розглядали себе як народ, представлений їх урядами [258, с. 89]. У таких умовах особливого значення набуває пошук нових правил і форм взаємодії держави та суспільства в інтересах збереження своєї цілісності й безпеки розвитку всіх і кожного.

Дослідження характеристик інформаційного суспільства було б неповним без розгляду робіт вітчизняних науковців, які інтерпретують досвід світової науки з урахуванням українських особливостей інформатизації. Так, Д.В. Дюжев ґрунтовно доводить, що "формування інформаційного суспільства є сучасною домінуючою тенденцією розвитку людства в глобальний інформаційний простір на базі інформаційно-комп'ютерних технологій, Інтернету тощо" [92]. Одним із результатів дисертаційного дослідження В.М. Скалацького є констатація того, що перехід до інформаційного суспільства в Україні є об'єк-

тивною необхідністю. "Однак лише належне стратегічно-інституційне забезпечення формування інформаційного суспільства дозволить виявити реальні можливості України як держави з потужним інтелектуальним потенціалом" [317, с. 4].

В.О. Даніл'ян пропонує визначення інформаційного суспільства як сучасного стану цивілізаційного розвитку, сутність якого полягає в збільшенні масштабів створення, накопичення, передачі, обробки й використання інформації, перетворенні інформації та знання на продуктивні сили суспільства, а також у збільшенні впливу новітніх інформаційно-комунікаційних технологій на політику, економіку, соціальну структуру, право, культуру тощо. Він констатує, що процеси становлення вітчизняного інформаційного суспільства "відбуваються стихійно і неузгоджено, а рівень розвитку інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу і можливостям України" [81, с. 7, 14]. Підтвердження такої констатації ми знаходимо в Доповіді Державного комітету інформатизації України Кабінету Міністрів України у 2008 році. У цьому документі зазначається, що існує кілька рейтингів оцінювання країн на предмет розвиненості інформаційного суспільства. Результати щодо України такі: Індекс інформаційного суспільства (ISI) – на офіційному сайті наводяться значення для 53 країн, України серед них немає; Індекс цифрового доступу – розраховувався для 178 країн, які були поділені на чотири групи за рівнем доступу до інформаційно-комунікаційних технологій (найвищий, високий, середній, низький) – Україні присвоєно середній рівень; Рейтинг електронної готовності – 60 місце серед 69 країн, між Еквадором та Шрі-Ланкою [317, с. 8].

Провідне значення знання для характеристики сучасної суспільної обстановки підкреслює О.В. Пархоменко. Він використовує термін "інформаційно-знаннєве суспільство" та зазначає, що воно поступово стає основою розвитку соціальної, економічної, гуманітарної, культурної та інших сфер повсякденного життя. "Унаслідок формування інформаційно-знаннєвих суспільств створюється фундаментальна основа для реа-

лізації індивідуальних творчих можливостей кожного члена суспільства, а отже, й умови для формування потужного інтелектуального капіталу країни" [263, с. 6]. У зв'язку з цим необхідно звернути увагу на припущення О. О. Маруховського, що попри сучасне домінування концепцій інформаційного суспільства дедалі помітнішою є їх теоретико-методологічна та історична обмеженість і що світ стає свідком зміни концепцій інформаційного суспільства на концепцію суспільства знань, що веде до епохальних зрушень в усіх сферах суспільного життя, зокрема в політичній [224, с. 6]. У цьому контексті неможливо не відзначити тенденції інноваційної діяльності в Україні, про які йдеться в колективній монографії за загальною редакцією Ю.Г. Рубана "Україна в 2005 – 2009 рр.: стратегічні оцінки суспільно-політичного та соціально-економічного розвитку". Розвиток однієї з ключових позицій в економіці інформаційного суспільства – інновацій – характеризується, на думку авторів, такими положеннями: збереження низького рівня інноваційної активності промислових підприємств; поступове зниження результативності інноваційного процесу в промисловості; неефективність структури реалізованої інноваційної продукції; звуження інноваційного потенціалу інвестицій; недосконаліть структури інноваційних витрат; невідповідність структури фінансування інвестиційної діяльності пріоритетам інноваційного розвитку економіки; зниження інноваційної ефективності інвестицій в основний капітал [358, с. 323 – 328].

А.О. Сіленко констатує наявність значного потенціалу сучасних інформаційно-комунікаційних технологій у плані збирання, зберігання та поширення інформації, а отже, визнає можливість їх використання як досить ефективного засобу маніпулювання людською свідомістю. "За допомогою інформаційних технологій формується специфічне інформаційне поле, що стає потужним засобом здійснення й проведення владних стратегій. Інформаційне поле настільки ж невидиме для безпосереднього спостереження, як гравітаційне чи електро-

магнітне, але воно здатне структурувати все, що виявляється „усередині" його, за певними лініями і напрямами. Невидиме управління не викликає протесту, оскільки створюється враження, ніби людина всі рішення приймає вільно й тільки сама" [316, с. 97 – 98]. Крім цього, професор А.О. Сіленко поділяє стурбованість теоретиків інформаційного суспільства щодо тенденцій інтеґрації культурного простору, заміщення локальних просторів інформаційними потоками: "вплив місцевих традицій, які сприяють самодостатньому інерційному розвитку окремих елементів, послаблюється", наслідком інтеґрації стає "розмивання регіональних і культурно-історичних особливостей розвитку" [316, с. 98].

Значну роботу щодо встановлення сутнісних характеристик інформаційного суспільства провів вітчизняний дослідник А.В. Колодюк. У своєму дисертаційному дослідженні "Інформаційне суспільство: сучасний стан та перспективи розвитку в Україні" [133] він здійснив ретельний аналіз концепцій інформаційного суспільства, розглянув світові стратегії його розвитку, визначив особливості та основні пріоритети його становлення в Україні. Серед результатів цього дослідження нас насамперед цікавить включення в науковий дискурс категорії "цифровий розподіл". На думку А.В. Колодюка, "в сучасних умовах розвитку інформаційного суспільства на міжнародному, регіональному та національному рівнях одночасно відбувається й розвиток процесу нового виду соціального розмежування – цифрового розподілу, в результаті чого переважна більшість людей не знає або ж не бажає знати про можливості життєдіяльності у новітньому типі суспільного устрою" [134]. Автор констатує, що ця проблема актуальна і для нашої держави, її розв'язання вимагає збалансованого загальнодержавного системного підходу та впровадження строкових, цільових ініціатив для залучення широких верств населення до використання переваг інформаційно-комунікаційних технологій у різноманітних сферах життєдіяльності. "У вирішенні цих завдань слід також усвідомити, що завдяки використанню інформа-

ційно-комунікаційних технологій можна і, наголошуємо, потрібно вирішувати увесь комплекс сьогоденних соціально-економічних проблем" [133, с. 59]. Зауважимо, що проблема "цифрової нерівності" має й внутрішньодержавний вимір. Так, згідно з даними спеціальних досліджень у 2004 році, 55% українських користувачів Інтернету мешкає в м. Києві, ще третина (29%) перебуває в містах Одесі, Дніпропетровську, Донецьку, Харкові, Львові, Запоріжжі. Як правильно зазначає М.З. Згуровський, це є однією з причин глибокої соціально-економічної кризи суспільства, оскільки його переважна більшість відокремлена від актуальних світових знань та інформації і їх генерування [108, с.110]. На жаль, ситуація з територіальним розподілом національних користувачів Інтернету залишається складною. На тлі суттєвого збільшення інтернет-аудиторії України майже не відбулося змін у її регіональній структурі. Як і раніше, спостерігається суттєва диспропорція, навіть між Київським регіоном та іншими регіонами, у яких розташовані великі міста [318].

Змістовне дослідження інформаційного суспільства провів і автор роботи "Політична система України: розвиток в умовах глобалізації та інформаційної революції" М.А. Дмитренко [84]. Констатуючи багатомірність соціальних змін, що характеризують інформаційне суспільство, він пропонує класифікацію критеріїв інформаційного суспільства. Так, до технологічного критерію відноситься використання інформаційних технологій у сферах виробництва, управлінні, побуті; до соціального – значення інформації як важливого стимулятора зростання якості життя, формування й утвердження "інформаційної свідомості" за широкого доступу до інформації; під економічним критерієм розуміється отримання інформацією статусу економічного ресурсу; політичний критерій полягає в тому, що інформація стимулює політичні процеси; нарешті, культурний критерій інформаційного суспільства – "визнання культурної цінності інформації сприяє утвердженню інформаційних цінностей в інтересах розвитку окремого індивіда і су-

спільства в цілому" [84, с. 56 – 57]. Окрему увагу М.А. Дмитренко приділяє темі "інформаційного розриву", визначаючи його як "нерівномірний доступ до інформаційно-комунікаційних технологій, інформаційне домінування одних країн над іншими, що є серйозною перешкодою на шляху створення стійкого глобалізаційного інформаційного суспільства". Дослідник констатує, що "інформаційний розрив", або "цифрова нерівність", є актуальною проблемою для української держави і це створює ризики відставання у розвитку та неможливості використання сучасних методів збільшення виробництва [84, с. 55 – 56, 59]. У питанні політичних наслідків розвитку інформаційних технологій М.А. Дмитренко відзначає діалектичність процесів та прогнозів: з одного боку, розширення демократичної участі, інформатизація державного управління, а з іншого – монополізація інформаційного простору, контроль над індивідуальною свідомістю, посилення культурного імперіалізму, установлення інформаційно-фінансового тоталітаризму [84, с. 67]. Обґрунтованим видається й висновок щодо підвищення ідеологічної уразливості політичної системи та необхідності відповідної реакції держав і транснаціональних структур шляхом застосування юридичних методів посилення контролю за використанням інформаційних технологій [84, с. 87].

Нарешті, зупинимося ще на одному важливому положенні. Як можна було побачити з проведеного аналізу, далеко не всі дослідники поділяють думку про те, що інформаційне суспільство являє собою новий вид соціуму. Професор Ф. Уебстер з цього приводу зазначає, що серед науковців, які займаються проблемами інформаційного суспільства, існує фундаментальний розкол на тих, хто "проголосив виникнення суспільства нового типу", і прибічників ідеї соціальної спадкоємності, тих, які не заперечують ключової ролі інформації в сучасному світі, але стверджують, що процеси інформатизації раніше встановлених відносин ще не означають появи нового соціального устрою. Здійснивши ретельний аналіз поглядів як представників першої групи, так і другої, він зазначає: "… ті,

хто вважає, що в останній час інформаційне суспільство вже стало реальністю (або стає нею), використовують критерії, які відповідають їх технократичним переконанням. Вони намагаються показати, що інформаційне суспільство виникло, шляхом вимірювання явищ, які, як вони вважають, характерні для цього суспільства, що виглядає доволі дивно. Як кількісна міра обираються інформаційні технології, вартість створеної інформації, збільшення числа зайнятих в інформаційній сфері, насиченість суспільства інформаційними мережами або очевидне (а тому таке, що не вимагає ніяких підрахунків) вибухове зростання кількості знаків та значень. … не використовуючи ніяких інших аргументів, крім тих, що навколо нас так багато інформації та інформаційних технологій, стверджують, що ці кількісні характеристики свідчать про якісний перехід – виникнення інформаційного суспільства… Тому видається, що ті, хто пояснює явище інформатизації в термінах історичної спадковості, дозволяють нам краще зрозуміти роль інформації в сьогоднішньому світі… вони чинять супротив намаганням квантифікувати інформаційне суспільство і саму інформацію" [361, с. 372 – 373]. Відомий дослідник соціальних аспектів інформатизації Кристофер Мей також не вважає, що сьогодні відбувається становлення суспільства нового типу. Характеризуючи сучасні суспільні процеси, він зазначає, що зміст людської діяльності був і залишається сталим, змінюються лише її форми. Це положення підтверджується в тому числі скептичним аналізом технологічно детерміністських поглядів і критикою висловлених у науці положень щодо формування економіки нового (інформаційного) типу. Так, стосовно інформаційних технологій він зазначає, що вони створюються під впливом соціальних умов, а не навпаки, і продовжують обслуговувати суспільство. Сучасні тенденції в економіці він пов'язує зі стрімким поширенням законів приватної власності в інформаційній та науковій сферах, що свідчить не про появу нових, а про повернення до традиційних економічних відносин. "Інформаційне суспільство є лише логічним продовженням капіталістичного розвитку – новим капіталістичним ремейком".

[230, с. 4, 17, 18, 43]. Для нашого дослідження ці висновки корисні констатацією того, що інформаційне суспільство, у нашому розумінні – суспільство, яке характеризується змінами, викликаними інформатизацією та комп'ютеризацією, не являє собою суспільства нового типу, а отже, не вимагає встановлення нової системи цінностей, які необхідно забезпечувати правовою охороною. Інформація, як зазначалося раніше, є необхідною умовою ефективності будь-якої діяльності, і саме соціальне значення цієї діяльності визначає соціальне значення відповідних інформаційних відносин та суспільну небезпечність посягань на них. Отже, посягання на відносини у сфері використання інформаційних технологій або відносини у сфері надання доступу до інформації чи формування інформаційного ресурсу необґрунтовано розглядати як такі, що є небезпечними самі по собі. Знищення комп'ютерної інформації чи розголошення відомостей з обмеженим доступом є небезпечними рівно настільки, наскільки соціально значущою була діяльність, для здійснення якої використовувалася комп'ютерна техніка або обмежувався доступ до певної інформації. Тож, якщо інформаційна безпека є системою відносин, у межах яких забезпечується реалізація інформаційної потреби, то значущість цих відносин і, відповідно, необхідність їх кримінально-правової охорони, суспільна небезпечність посягань на відносини інформаційної безпеки визначаються значущістю тих суспільних відносин, у межах яких виникає інформаційна потреба.

Слід сказати, що у вітчизняній науці представлені й інші позиції. Так, Н.А. Савінова стверджує: "Інформаційному суспільству притаманні відмінні від попередніх стадій розвитку суспільства ресурси й цінності, у ньому детермінуються способи взаємодії та причини консолідації, змінюються суспільні і індивідуальні пріоритети розвитку та діяльності, глобалізуються соціально-економічні й політичні відносини" [308, с. 20]. Такий підхід можна вважати обґрунтованим і доцільним скоріше в межах соціологічних досліджень, предметом яких є тенденції та закономірності соціального розвитку. Однак коли

предметом дослідження виступають питання кримінальної відповідальності, одним із головних завдань роботи є формулювання висновків щодо того, які діяння з певного кола можливих посягань на суспільні відносини слід уважати суспільно небезпечними, а які ні. Якщо дотримуватися позиції, що інформаційне суспільство характеризується принципово новими цінностями, отримання чіткої та обґрунтованої відповіді на питання "Які посягання на інформаційну безпеку слід уважати суспільно небезпечними?" стає проблематичним. Водночас запропоноване раніше визначення інформаційної безпеки та сформульовані висновки щодо сутності суспільної небезпечності посягань на неї дозволяють чітко визначати коло відповідних суспільно небезпечних посягань.

Таким чином, суспільна небезпечність посягань на інформаційну безпеку, наслідків, які настають через порушення у сфері використання інформаційних технологій, доступу до інформації або формування інформаційного ресурсу, завжди характеризується однаковими чинниками. Загальною рисою суспільних відносини інформаційної безпеки, які потребують кримінально-правової охороні, є те, що їх значення є похідним від значущості тих суспільних відносин, у межах яких виникає інформаційна потреба. Саме важливість останніх визначає значення відносин інформаційної безпеки, а також доцільність та інтенсивність відповідних заходів кримінально-правової охорони. Тому й суспільна небезпечність посягань на інформаційну безпеку не є самостійною, залежить від соціальної значущості тих відносин, у межах яких використовується інформація, що є предметом посягання. Наприклад, знищення інформації, що обробляється в комп'ютерній системі, небезпечне настільки, наскільки соціально значущим є завдання, для виконання якого використовується певний комп'ютер. Так само небезпечність обмеження доступу до певної інформації визначається наслідками, що настали через неможливість реалізації відповідної інформаційної потреби.

Отже, результати наукових досліджень тенденцій інформатизації суспільства, інтерпретовані в контексті встановлення

системи соціальних потреб кримінально-правової охорони інформаційної безпеки, дозволяють зробити такі висновки. По-перше, оскільки становлення інформаційного суспільства – це домінуюча тенденція світових соціальних процесів та об'єктивна необхідність для України, то *охорона інформаційної безпеки є одним із пріоритетних завдань держави*, бо дозволяє запобігти тотальному виключенню України зі світових інтеграційних процесів як країни, що не може бути частиною прогресивного міжнародного співтовариства через принципову застарілість організації влади, недостатність технологічної бази та обмеженість, неготовність населення до існування в інформаційному просторі.

По-друге, *необхідність* саме *кримінально-правового захисту* інформаційної безпеки *обґрунтовується соціальним значенням відносин*, що входять до її складу. Так, *відносини інформаційної безпеки у сфері використання інформаційних технологій* потребують кримінально-правової охорони, оскільки відіграють значну роль в організації та здійсненні певних видів людської діяльності. При цьому значущість цих суспільних відносин, а отже, потреба в їх кримінально-правовій охороні, залежить від виду людської діяльності, для інтенсифікації якої використовується електронно-обчислювальна техніка. Це особливо актуалізується в умовах глобалізації, коли, наприклад, безпрецедентна глобалізація фінансового ринку, організаційно побудованого на використанні сучасних інформаційних технологій, створює небезпеку посягань з надзвичайно великим ступенем небезпечності. Крім того, тенденція зростання числа зайнятих у інформаційному секторі дозволяє прогнозувати підвищення суспільної небезпечності посягань на відносини у сфері використання інформаційних технологій. *Відносини інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу* потребують кримінально-правової охорони з огляду на наявну актуальну суспільну потребу, що, з одного боку, полягає в необхідності забезпечення вільного доступу до інформаційних ресурсів якомога більшій кількості членів суспільства, а з іншого – актуалізує проблему гарантування встановлених обмежень стосовно доступу до певних видів інформації. Необхідність кримінально-правової охорони цих відносин загострюється, крім того, істотним зростанням соціального, політичного та економічного значення інформації. Нарешті, *відносини інформаційної безпеки у сфері формування інформаційного ресурсу* потребують кримінально-правових засобів охорони з огляду на те, що продукування та захист знання, створення потужних інформаційних ресурсів є необхідною передумовою прийняття ефективних рішень на рівні індивіда, суспільства або держави, забезпечують інноваційність і гнучкість виробництва, конкурентоспроможність продукції на глобальних ринках. Важливість кримінально-правової охороні цих відносин актуалізується наявністю таких негативних тенденцій, як: надмірна капіталізація інформаційного простору; небезпека антидемократичного розвитку через маніпуляції суспільною свідомістю в політичній сфері; небезпека системних порушень права на повагу до приватного життя та тотального контролю над особистістю через створення надпотужних баз персональних даних; зростання рівня ідеологічної вразливості політичних систем через наявність потенціалів глибоких соціальних конфліктів, які можуть бути задіяні шляхом використання інформаційних технологій; утрата навичок роботи з інформацією через надмірне насичення нею соціального буття.

При цьому, по-третє, *соціальне значення названих видів відносин інформаційної безпеки, а отже, і суспільна небезпечність посягань на них характеризуються єдиними чинниками*: соціальне значення суспільних відносин інформаційної безпеки є похідним від значущості тих суспільних відносин, у межах яких виникає інформаційна потреба. Суспільна небезпечність посягань на інформаційну безпеку не є самостійною і визначається інтенсивністю наслідків, що настали через обмеження можливості реалізації інформаційної потреби.

Таким чином, інформаційна безпека являє собою сукупність суспільних відносин, які потребують кримінально-правового захисту та характеризуються специфічним, властивим саме цій групі відносин змістом чинників суспільної небезпек-

ності посягань на них. Крім цього, як було доведено в попередній підглаві, інформаційна безпека – це не проста сукупність, а система суспільних відносин, які характеризуються єдиними особливостями змісту заподіяної шкоди. Тому обґрунтованим буде твердження, що інформаційна безпека є певним колом однорідних за своєю соціальною сутністю суспільних відносин, які у зв'язку з цим повинні охоронятися єдиним комплексом взаємопов'язаних кримінально-правових норм, тобто є родовим об'єктом за визначенням. Отже, процес інформатизації зумовив формування нової групи суспільних відносин, посягання на які характеризується таким рівнем суспільної небезпечності, який свідчить про необхідність застосування кримінально-правових засобів. У зв'язку з цим обґрунтованим, таким, що відповідає фактичним соціальним потребам у кримінально-правовій охороні, буде включення інформаційної безпеки до системи родових об'єктів злочинів, передбачених КК України.

Для реалізації висловленої пропозиції доцільною видається заміна назви розділу XVI Особливої частини КК України такою – "Злочини проти інформаційної безпеки" та об'єднання в ньому норм про відповідальність за злочини у сфері використання інформаційних технологій, забезпечення доступу до інформації та формування інформаційного ресурсу. Зміст означених кримінально-правових заборон буде досліджено в подальших главах.

Висновки до першої глави

Аналіз категорії "інформаційна безпека", соціальних потреб у кримінально-правовій охороні суспільних відносин інформаційної безпеки, а також сучасного стану наукових досліджень в цій сфері дозволяє зробити такі висновки:

1. Як самостійний об'єкт кримінально-правової охорони інформаційна безпека є системою суспільних відносин, яка забезпечує можливість реалізації однієї з ключових потреб су-

часного суспільства – інформаційної. Її реалізація здійснюється шляхом отримання доступу до необхідної інформації, базується на використанні інформаційних технологій та забезпечується формуванням інформаційного ресурсу.

2. Структуру інформаційної безпеки як об'єкта кримінально-правової охорони складають: 1) відносини щодо формування інформаційного ресурсу; 2) відносини щодо забезпечення доступу до інформаційних ресурсів; 3) відносини щодо забезпечення функціонування інформаційних технологій як засобів доступу до інформаційного ресурсу та його формування.

3. Визначена сукупність суспільних відносин являє собою систему, оскільки її елементи підпорядковані єдиній, спільній соціальній меті, взаємозумовленим є їх функціонування та ефективність. Для всіх визначених відносин інформаційної безпеки спільним є й те, що шкода від посягання на них полягає в позбавленні, або обмеженні можливості реалізації інформаційної потреби.

4. Кримінально-правова охорона інформаційної безпеки складається з трьох частин: забезпечення доступу до інформаційних ресурсів; забезпечення формування інформаційного ресурсу; забезпечення функціонування інформаційних технологій як засобів формування інформаційного ресурсу та доступу до нього.

5. Соціальні потреби в кримінально-правовій охороні інформаційної безпеки систематизовані за її структурними елементами. Так, необхідність захисту відносин у сфері використання інформаційних технологій зумовлена значенням, яке має їх використання в організації та здійсненні певних видів людської діяльності, кількість яких постійно збільшується через розширення сфери застосування комп'ютерної техніки. Відносини інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу потребують кримінально-правової охорони з огляду на наявну актуальну суспільну потребу, що, з одного боку, полягає в необхідності забезпечення вільного доступу до інформаційних ресурсів якомога більшій кількості членів суспільства, а з іншого – актуалізує проблему

ґарантування встановлених обмежень доступу до певних видів інформації. Формування інформаційного ресурсу потребує кримінально-правових засобів охорони з огляду на потенційну можливість істотних порушень соціальної стабільності шляхом зловживань у цій сфері.

6. Загальною рисою суспільних відносин інформаційної безпеки, які потребують кримінально-правової охорони, є те, що їх значення похідне від значущості тих суспільних відносин, у межах яких виникає інформаційна потреба. Саме від важливості останніх відносин залежить значення певних відносин інформаційної безпеки, а також доцільність та інтенсивність відповідних заходів кримінально-правової охорони.

7. У зв'язку з тим, що інформаційна безпека є системою суспільних відносин, які потребують кримінально-правового захисту, характеризуються специфічним, властивим саме цій групі відносин змістом чинників суспільної небезпечності посягань на них, обґрунтовано доцільність включення інформаційної безпеки до системи родових об'єктів злочинів, передбачених КК України; на цій підставі запропоновано замінити назву розділу XVI Особливої частини КК України такою – "Злочини у сфері інформаційної безпеки" та об'єднати в ньому норми про відповідальність за злочини у сфері використання інформаційних технологій, забезпечення доступу до інформації та формування інформаційного ресурсу.

Глава 2

Методологічні засади дослідження кримінально-правових засобів охорони інформаційної безпеки України

2.1. Методологія дослідження кримінально-правових засобів охорони інформаційної безпеки

Інформаційна безпека, як і будь-яка інша система суспільних відносин, є динамічною й такою, що потребує забезпечення стабільності та розвитку. Останні, як свідчать аксіоматичні положення теорії держави та права, досягаються шляхом соціальної регуляції, дією звичаїв, традицій, права тощо. Зауважимо, що такі рівні соціальної регуляції властиві й інформаційній безпеці.

Так, неправовий рівень регулювання інформаційної безпеки може виявлятись у певних механізмах самоорганізації в інформаційному суспільстві. Розглядаючи їх, російська дослідниця Е.Л. Вартанова зазначає, що в інформаційному суспільстві до традиційної сфери формування механізмів саморегуляції разом із професіоналами, бізнес-спільнотою та частково державою включається й сама аудиторія, яка через зростаючу інтерактивність і можливість зворотного зв'язку, що збільшується, починає чітко формулювати свої вимоги до медіа контенту. До найбільш успішних, позаправових форм саморегулювання, які довели свою ефективність у протидії інформаційних загроз, дослідниця відносить: гарячі лінії в Інтернеті, маркування медіаконтенту, кодекси поведінки провайдерів, контроль користувачів [51, с. 15 – 17].

На правовому рівні забезпечення інформаційної безпеки досягається нормативним регулюванням у межах різних галузей права. Головним чином регулювання інформаційної безпеки здійснюється в межах права інформаційного.

Включення кримінально-правових засобів до системи правового регулювання інформаційної безпеки відбувається в основному шляхом *криміналізації* суспільно небезпечних посягань на неї. Отже, методологією, що відповідає меті дослідження та його завданням, є аналіз засобів кримінально-правової охорони інформаційної безпеки з позицій досягнень науки кримінального права в питанні криміналізації та її критеріїв, а також визначених у попередній главі соціальних потреб кримінально-правового впливу на інформаційні суспільні відносини.

Серед наукових досліджень, присвячених питанням криміналізації, найбільш повною та обґрунтованою видається колективна робота "Підстави кримінально-правової заборони. Криміналізація та декриміналізація" за редакцією докторів юридичних наук, професорів В.П. Кудрявцева та А.М. Яковлєва [256]. Запропонована в ній методологія визначення обґрунтованості криміналізації являє собою достатньо чіткий інструментарій, який видається доцільним використати для нашого дослідження. З його допомогою ми зможемо сформулювати положення про те, якими мають бути зміст і межі кримінально-правового регулювання інформаційної безпеки. Наявність цих положень дозволить нам критично проаналізувати чинне законодавство та запропонувати, за необхідності, обґрунтовані пропозиції щодо його подальшого вдосконалення.

Доцільність криміналізації зазначені автори розглядають, установлюючи підстави та принципи криміналізації. Підставами є "дійсні передумови, соціальні причини виникнення кримінально-правової норми". Принципи, у свою чергу, утворюють систему правил і критеріїв установлення кримінальної відповідальності [256, с. 206]. Таким чином, висновок щодо доцільності криміналізації та її змісту отримується шляхом поступового аналізу фактів дійсності, що свідчать про необхід-

ність запровадження певної кримінально-правової заборони, та подальшого розгляду цих фактів у контексті кримінального-правового регулювання.

Підставами криміналізації посягань на інформаційну безпеку виступають процеси, що відбуваються в матеріальному й духовному житті суспільства, розвиток яких породжує об'єктивну необхідність кримінально-правової охорони. Як ми зазначали, ці процеси пов'язані з тенденціями інформатизації суспільних відносин. Вони можуть бути поділені на дві групи: 1) процеси, які мають істотне значення для позитивних трансформацій суспільства в бік розвитку та стабільності; 2) процеси, які, навпаки, мають небезпечний соціальний потенціал.

До першої групи слід відносити: 1) зростання суспільної цінності інформаційної діяльності, забезпечення доступу до інформації, що набуває істотного соціального, політичного та економічного значення; 2) отримання відносинами щодо продукування та захисту знання, створення потужних інформаційних ресурсів статусу чиннику ефективності рішень, що приймаються на рівні індивіда, суспільства або держави, інноваційності та гнучкості виробництва, а отже, і конкурентоспроможності національної продукції на глобальних ринках; 3) розширення сфери застосування інформаційних технологій як засобів, що забезпечують ефективність людської діяльності.

До другої групи належать процеси, що характеризуються великим потенціалом суспільної небезпечності, серед них слід зазначити: наявність соціальних небезпек, зумовлених розширенням сфери застосування інформаційних технологій, надмірну капіталізацію інформаційного простору; маніпуляції суспільною свідомістю в політичній сфері; формування надпотужних баз персональних даних, що утворює небезпеку системних порушень права на повагу до приватного життя й тотального контролю над особистістю; зростання рівня ідеологічної вразливості політичних систем через наявність потенціалів глибоких соціальних конфліктів, які можуть бути задіяні шляхом використання інформаційних технологій; утрата

навичок роботи з інформацією через надмірне насичення нею соціального буття.

Розгляд цих підстав у контексті кримінально-правового регулювання забезпечується шляхом аналізу відповідних принципів криміналізації. Останні поділяються на групи, що відображають істотні зв'язки кримінального права з різноманітними сферами соціальної реальності та системний характер сукупності кримінально-правових норм:

1) принципи, які виражають суспільну необхідність і політичну доцільність установлення кримінальної відповідальності, або соціальні й соціально-психологічні, тобто принципи, що забезпечують соціальну адекватність криміналізації, її припустимість з точки зору основних характеристик соціальних систем і процесів суспільного розвитку, відповідності кримінально-правової норми рівневі, характеру суспільної свідомості та стану громадської думки; 2) принципи, що визначаються вимогою внутрішньої логічної несуперечливості системи норм кримінального права або несуперечливості норм матеріально-процесуального права чи норм кримінального та інших галузей права (конституційного, цивільного, інформаційного та ін.), тобто системно-правові принципи криміналізації [256, с. 210].

Принцип суспільної небезпечності. Визнаючи складність формулювання операціональних критеріїв суспільної небезпечності, автори згаданого дослідження відзначають, що принцип суспільної небезпечності вказує на той "вихідний пункт руху пізнання, від якого воно повинно відправлятися при дослідженні питань обґрунтованості криміналізації діяння" [256, с. 217]. Таке положення, безсумнівно, є правильним, оскільки аксіомою науки кримінального права є твердження про те, що суспільна небезпечність являє собою атрибутивну властивість злочинів і полягає в тому, що діяння суб'єкта заподіює або створює загрозу заподіяння істотної шкоди суспільним відносинам. Тому в основі криміналізації лежить об'єктивна шкода, що заподіюється суспільним відносинам, або реальна небезпека її заподіяння [307, с.17]. Разом із тим, шкода, заподіяна злочином, є виявленням суспільної небезпечності, тому шкоду і суспільну небезпечність не можна ототожнювати. Остання полягає в тому, що, заподіюючи шкоду конкретним суб'єктам, їх життю, здоров'ю, власності, злочин посягає на соціальні, економічні, правові та моральні підвалини соціального порядку [261, с. 8].

У зв'язку з цим, заслуговує на увагу висновок Л.М. Кривоченко про те, що виникнення, зміна, втрата суспільної небезпечності діяння зумовлені об'єктивними закономірностями суспільного розвитку, нерозривним зв'язком з тими соціально-економічними процесами, що відбуваються в суспільстві [190, с. 74 – 75].

Як уже зазначалося, певні складнощі в дослідженні суспільної небезпечності більшість дослідників пов'язують із відсутністю чітких операціональних критеріїв її встановлення. Так, П.А. Фєфєлов убачає сутність суспільної небезпечності злочинного діяння в тому, що воно, маючи властивості соціальної практики, "несе в собі антисуспільну ціннісну орієнтацію і може служити прецедентом для повторення подібної діяльності в майбутньому" [364, с. 138]. Є.О. Гнатенко пропонує для визначення змісту суспільної небезпечності конкретних діянь звернутися до практичної філософії Канта. Кант не використовує поняття "суспільна небезпечність", однак у своїй статті "Про уявне право брехати задля людинолюбства" пропонує доволі простий критерій: "якщо ми уявно генералізуємо максиму вчинку, та виявиться, що такої генералізації ми не можемо бажати (при цьому руйнуватиметься суспільство або, що те ж саме, якийсь його інститут), то такий вчинок буде суспільно небезпечним" [69, с. 195 – 196]. Видається, що наведені положення дозволяють сформулювати достатньо чітке операціональне доповнення до аксіоматичних характеристик суспільної небезпечності та криміналізації: такий принцип криміналізації діяння, як його суспільна небезпечність, буде реалізований у тих випадках, коли уявна генералізація діяння, доцільність криміналізації якого досліджується, буде свідчити

про можливість істотних порушень суспільного ладу, його соціальних, економічних, правових або моральних підвалин.

Таким чином, *характер суспільної небезпечності* посягань на інформаційну безпеку визначається тим, що в умовах інформатизації суспільства, зростання соціальної значущості доступу до інформації, формування об'єктивних, повних та достатніх інформаційних ресурсів, використання з цією метою інформаційно-комунікаційних технологій істотну шкоду суспільству завдають посягання, які призводять до порушення можливості користування інформаційними ресурсами через обмеження доступу до них, спотворення процесу їх формування або унеможливлення користування інформацією через протиправні втручання в роботу інформаційних технологій. При чому до суспільно небезпечних слід відносити лише ті посягання, уявна генералізація яких свідчить про можливу небезпеку істотних соціальних наслідків.

Необхідно зазначити, що встановлена в попередній главі специфіка суспільних відносини інформаційної безпеки, яка полягає в тому, що їх значення є похідним від значущості тих суспільних відносин, у межах яких виникає інформаційна потреба, детермінує і певну специфіку характеру суспільної небезпечності посягань на інформаційну безпеку, оскільки саме значення останніх відносин визначає суспільну цінність певних відносин інформаційної безпеки, характер суспільної небезпечності посягань на інформаційну безпеку, доцільність та інтенсивність відповідних заходів кримінально-правової охорони, визначається шкодою тим суспільним відносинам, у межах яких виникає інформаційна потреба. Іншими словами, знищення або блокування інформації, обмеження чи отримання неправомірного доступу до неї небезпечні не самі по собі, а тільки в контексті тих відносин, з якими пов'язане використання інформації, що є предметом певного посягання.

Ступінь суспільної небезпечності посягань на інформаційну безпеку визначається тяжкістю заподіяною шкоди, способом посягання, формою вини, мотивами, цілями, іншими об'єктивними та суб'єктивними ознаками. Як правильно зазначає

Л.М. Кривоченко: "Якщо характер суспільної небезпечності виду злочину дозволяє відмежовувати види злочинів, то ступінь цієї небезпеки визначає градацію в рамках одного й того ж виду, дозволяє дати порівняльну характеристику злочинів" [147, с. 47].

Принцип відносної поширеності діяння. Кримінальне право регулює форму реакції суспільства та держави на такі суспільно небезпечні вчинки індивідів, які є не випадковостями, а проявами деяких загальних тенденцій і закономірностей. Таким чином, діяння, що підлягають криміналізації, мають бути більш-менш поширеними. Водночас цей критерій установлює й певну верхню кількісну межу для однорідних суспільно небезпечних актів поведінки, що визначає можливість їх криміналізації. Слід погодитися з Г.А. Злобіним у тому, що оскільки злочинна поведінка є девіантною, такою, яка порушує реальні соціальні норми, не можуть підлягати криміналізації надто поширені форми поведінки. Спроба такої криміналізації неодмінно призведе до возведення в норму безкарності діянь, визначених злочинними [256, с. 218 – 219]. Буде спостерігатися перевантаження системи юстиції, тому практично неможливо буде реалізувати повною мірою принцип невідворотності покарання [144, с. 73].

Якщо більшість дослідників поділяють положення щодо недоцільності криміналізації надто поширених діянь, то в питанні "нижньої" межі поширеності немає такої єдності. Так, Н.А. Лопашенко зазначає, що діяння, яке переслідується в кримінальному порядку, не може бути випадковим або рідким для суспільства, воно має бути типовим, таким, що повторюється в різних умовах [217, с. 290]. Подібні положення можна бачити й у згаданому фундаментальному дослідженні підстав кримінально-правової заборони [256]. Однак більш аргументованою видається інша точка зору. Для того щоб забезпечити належний рівень кримінально-правового регулювання певних суспільних відносин, напевно, немає потреби чекати, доки посягання на них наберуть значення соціальної тенденції чи стануть "типовими"; скоріше за все, у таких випадках уже слід

говорити про серйозні вади кримінального законодавства. Тому видається послідовною думка В.К. Грищука про віднесення поширеності діяння до таких підстав криміналізації, які мають факультативне значення [75, с. 63]. С.Б. Гавриш стосовно декриміналізації так званих "мертвих" норм, що передбачають відповідальність за екологічні злочини зазначав, що існування в кримінальному законодавстві певної кількості "незастосовуваних" складів є допустимим і необхідним, оскільки ідеальний механізм дії кримінально-правової норми полягає, по суті справи, у її загальнопревентивному ефекті [65, с. 98]. Подібні положення містяться й у роботах інших дослідників [67, с. 80; 111, с. 90].

Таким чином, наступним критерієм криміналізації посягань на інформаційну безпеку є їх відносна поширеність, яка полягає в тому, що криміналізація буде обґрунтованою тільки в тих випадках, коли такі діяння не являють типового явища в житті суспільства.

Принцип співрозмірності позитивних та негативних наслідків криміналізації. Загальновизнаним у науці кримінального права є положення про те, що реалізація кримінальної відповідальності породжує певні небажані соціальні наслідки: негативне формування особистості тих, до кого застосовано кримінальне покарання, деформація міжособистісних відносин, порушення функціонування економіки та інших сфер суспільного життя тощо. Криміналізація ніколи не може розглядатися як абсолютне благо, вона завжди являє жертвування одними інтересами суспільства заради інших, більш значущих. Тому встановлення кримінального покарання за певне діяння допустиме лише тоді, коли є підстави обґрунтовано передбачати, що позитивні соціальні результати застосування кримінального права істотно перевищать невідворотні негативні наслідки криміналізації [256, с. 220].

Однак найбільш небезпечним соціальним наслідком криміналізації слід визнавати викривлення розвитку суспільних відносин, появу таких видів соціальної активності, які суперечать суспільним потребам. Аналізуючи проблемні аспекти

криміналізації, В.К. Грищук влучно цитує А.В. Малька, що одним із результатів оптимального правового регулювання є "викликання до життя" необхідної, корисної правової поведінки [222, с. 63, наводиться за 75, с. 65]. Використовуючи цю метафору, можна сформулювати таке положення: порушення принципу співрозмірності позитивних і негативних наслідків криміналізації небезпечне тим, що може "викликати до життя" нові соціально небезпечні форми поведінки.

Сказане має пряме відношення до питань криміналізації посягань на інформаційну безпеку. Так, незбалансований підхід до кримінально-правового забезпечення доступу до інформації може унеможливити для певної частини суспільства реалізацію інформаційної потреби через надмірну правову зарегульованість або, навпаки, надлишкові кримінально-правові гарантії такого доступу призведуть до неможливості реалізації в повному обсязі права власності на інформацію. Невиважені законодавчі рішення у сфері криміналізації посягань на відносини формування інформаційного ресурсу можуть спричинити або масштабні маніпуляції з масовою свідомістю, зумовлені зловживанням правовими гарантіями невтручання в діяльність засобів масової інформації, або згортання процесів демократизації через надто широкі правові можливості держави у сфері контролю за діяльністю мас-медіа. Як правильно зазначає російський дослідник В.В. Балдіцин, мета нормативного регулювання діяльності засобів масової інформації полягає в досягненні такого результату, коли, з одного боку, забезпечується реалізація свободи слова в різноманітних її проявах, а з іншого боку, здійснюється контроль за дотриманням морально-етичних і правових норм у процесі отримання та інтерпретації інформації [18].

Принцип кримінально-політичної адекватності криміналізації означає її відповідність основним тенденціям соціальної політики суспільства й держави, рівневі й характеру суспільної свідомості й стану громадської думки [77, с. 69]. Отже, криміналізація посягань на інформаційну має відповідати таким завданням сучасної соціальної політики, як забезпечення

розвитку інформаційного суспільства, розширення доступу до інформаційних ресурсів, формування об'єктивних, повних і достатніх інформаційних ресурсів, забезпечення функціонування інформаційних технологій. Разом із цим, важливою складовою цього принципу криміналізації є відповідність кримінально-правової заборони суспільній свідомості. Достатньо відомою є позиція І.Є. Фарбера, який зазначав: "Будь-яке покарання викликає в суспільній психології різноманітні правові відчуття: сором, страх, співчуття, схвалення, засудження тощо. При конструюванні законодавчої норми треба знати, на збудження або масове розповсюдження яких саме правових емоцій слід насамперед орієнтуватися" [362, с. 94]. Отже, криміналізація посягань на інформаційну безпеку має не тільки відповідати напрямкам соціальної політики, але й забезпечувати прогнозовані зміни в суспільній свідомості. Останнє є дуже важливим саме для правового регулювання інформаційної сфери. Її складність і багатомірність дозволяє стверджувати, що правове регулювання в ній не може здійснюватися простими, лінійними заходами, а його наслідки є багаторівневими. Як приклад закономірності функціонування інформаційної сфери можна навести стрімке зростання популярності та попиту на щось нестандартне, таке, що суттєво відрізняється від контексту. Так, творчість музичного колективу "Ленінград" набула значної популярності саме через заборону концертів цієї групи в Москві. Зростання кількості новин із цього приводу привело до збільшення зацікавленості стосовно доволі спірної з моральної точки зору лірики. Отже, питання обґрунтованості криміналізації має розглядатися з урахуванням того, що в інформаційній сфері заборона може викликати зацікавленість, а в деяких випадках навіть сприяти популяризації певних форм соціальної активності.

Системно-правові принципи криміналізації поділяються на загальноправові та кримінально-правові**.** Аналіз цих принципів і розв'язання в ході встановлення кримінально-правової заборони завдань, що їх стосуються, продиктовані необхідністю відповідності нової кримінально-правової норми як чинній

системі кримінального права, так і всій правовій системі країни взагалі, а також положенням міжнародних зобов'язань, прийнятих на себе країною [256, с. 228].

Загальноправові системні принципи криміналізації включають у себе принцип конституційної адекватності, принцип системно-правової несуперечливості криміналізації конкретного діяння, принцип міжнародної необхідності та допустимості криміналізації, принцип процесуальної здійсненності переслідування.

Принцип конституційної адекватності. Конституція України в статті 17 однією з найважливіших функцій держави визнає забезпечення інформаційної безпеки. Це положення конкретизується в низці інших норм Основного закону, що встановлюють права та свободи громадян. Так, ст. 31 встановлює таємницю листування, ст. 32 закладає основи спеціального правового режиму персональних даних, передбачає конституційно-правові ґарантії так званої інформаційної приватності, ст. 34 передбачає свободу думки та слова, ст. 50 містить правові гарантії отримання достовірної інформації про стан довкілля тощо. Отже, на конституційно-правовому рівні передбачено базові засади нормативно-правового регулювання інформаційної безпеки, і криміналізація посягань на неї є цілком конституційно адекватною.

Принцип системно-правової несуперечливості криміналізації конкретного діяння. Його дотримання полягає в з'ясуванні того, чи не суперечить кримінально-правова новела, що планується, нормам інших галузей права, чи не визначає вона злочинним те, що допускається або дозволяється іншим чинним законом [256, с. 231]. Для цілей нашого дослідження цей принцип важливий актуалізацією завдання ретельного дослідження конструктивних галузей права у сфері регулювання інформаційної діяльності на предмет відсутності суперечностей із законодавчими новаціями, що будуть пропонуватися.

Принцип міжнародно-правової необхідності та допустимості криміналізації. Міжнародна спільнота приділяє велику увагу нормативному регулюванню інформаційної безпе-

ки. Це цілком зрозуміло, якщо враховувати транскордонні властивості інформаційних технологій і, відповідно, транснаціональний характер суспільно небезпечних посягань у цій сфері. Саме ця специфіка вимагає створення єдиного правового нормативно-правового поля інформаційної безпеки. У четвертій главі ми повернемося до питання відповідності національного кримінального законодавства міжнародним нормативно-правовим документам.

Принцип процесуальної здійсненності переслідування. Кримінальний закон може бути практично функціональним та достатньо ефективним лише в тому випадку, коли всі передбачені нормою ознаки складу злочину можуть бути нормально доведені. У зв'язку з цим обов'язковим етапом прийняття рішення щодо доцільності криміналізації має бути розв'язання проблеми засобів доведення нового злочинного діяння, їх законності, допустимості та ефективності [256, с. 232 – 235]. У контексті нашого дослідження значущість цього принципу зумовлюється таким. Соціальні потреби в кримінально-правовій охороні інформаційної безпеки викликають необхідність розгляду достатньо складних соціальних матерій, таких як, наприклад, маніпуляції суспільною свідомістю та комерціалізація інформаційного простору тощо в контексті криміналізації. Дотримання при цьому принципу процесуальної здійсненності переслідування дозволить уникнути в результаті дослідження законодавчих пропозицій декларативного характеру.

Кримінально-правові системні принципи криміналізації являють собою вимоги до змісту й форми кримінально-правових норм, які продиктовані внутрішніми закономірностями системи чинного кримінального законодавства [256, с. 235]. Так, ***принцип відсутності прогалин та ненадлишковості заборони*** передбачає аналіз того, чи не створює новела, що пропонується, нормативної прогалини або, навпаки, надлишковості в системі чинного кримінального законодавства. Це правило має велике значення для встановлення кримінально-правових заборон у сфері інформаційної безпеки.Як ми вже зазначали, вона включається як необхідний елемент до складу

великої кількості інших систем суспільних відносин: національної, внутрішньої, міжнародної, економічної, екологічної безпеки тощо. Тому посягання на інформаційну безпеку повинні криміналізуватися тільки з урахуванням можливостей охорони відповідних суспільних відносин засобами чинного кримінального законодавства. Наприклад, керуючись цим принципом у главі третій, ми здійснимо аналіз доцільності криміналізації розповсюдження або збуту комп'ютерної інформації з обмеженим доступом в контексті наявності в чинному законодавстві великої кількості норм, що встановлюють відповідальність за незаконні дії з відомостями, що складають таємну або конфіденційну інформацію.

Принцип визначеності та єдності термінології. Зміст цього принципу полягає у вимозі використання для формулювання кримінально-правової заборони тільки визначених у законі термінів та обов'язкового визначення тих, які не визначені, але використовуються [256, с. 238]. Однак для цілей криміналізації посягань на інформаційну безпеку вимоги до термінології слід доповнити ще одним положенням. Оскільки розглядана сфера кримінально-правового захисту багато в чому пов'язана з досягненнями науково-технічного прогресу, то видається необхідним обмеження використання понять, пов'язаних із певним рівнем технологічного розвитку. Справа в тому, що розвиток сучасних інформаційних технологій відбувається дуже швидко, і використання в кримінальному законодавстві термінів, пов'язаних із конкретним рівнем технології, поставить кримінальний закон у певну залежність та вимагатиме його постійного коригування з огляду на досягнення технологічного характеру. При цьому принципової зміни суспільних відносин та небезпечності посягань не буде, змінюватиметься тільки технічна база охоронюваних суспільних відносин. З урахуванням вказаного вельми спірним видається доцільність використання в тексті кримінального закону (розділ XVI) термінів "електронно-обчислювальна машина", "автоматизована система", "комп'ютерна мережа" тощо. Детальніше ми розглянемо це питання у відповідній главі.

Принцип повноти складу передбачає конкретність і визначеність кримінально-правової норми, що встановлює караність певного діяння, тобто визначення в законі всіх ознак діяння, необхідних для визнання особи винною у вчиненні злочину [256, с. 239]. У науці вже висловлювалися погляди щодо певних порушень цього принципу в ході криміналізації посягань на інформаційну безпеку. Так, Н.А. Лопашенко, критикуючи положення російського кримінального законодавства щодо відповідальності за порушення правил експлуатації електронно-обчислювальних машин, системи електронно-обчислювальних машин або їх мережі (ст. 274 КК РФ), зазначає, що неоднозначність закону в питанні характеристики форми вини такого посягання породжує, принаймні, дві можливі версії щодо її змісту: злочин може бути вчинений з прямим або непрямим умислом або є можливою як умисна, так і необережна форма вини [217, с. 302 – 303]. Аналогічна норма наявна і в національному законодавстві (ст. 363 КК України), що з необхідністю порушує питання про дотримання принципу повноти складу при криміналізації цього посягання.

Нарешті, ***принцип співрозмірності санкції та економії репресії*** полягає в обґрунтованому та виваженому підході до визначення санкції, а також означає, що криміналізація діяння може бути здійснена тільки тоді, коли немає і не може бути норми, яка б достатньо регулювала певні суспільні відносини методами інших галузей права. Інакше кажучи, ефективний вплив на правопорушників заходами цивільного, трудового або адміністративного права є достатньою підставою для відмови від криміналізації [256, с. 241]. Стосовно реалізації цього принципу видається доцільним навести такий приклад. Деякі зі злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку сформульовані так, що дозволяють говорити про наявність ознак їх складів навіть у випадках очевидної відсутності суспільної небезпечності. Так, незаконне знищення несуттєвої комп'ютерної інформації, залежно від суб'єкта цих дій, формально підпадає під ознаки складу злочину, передбаченого

ч. 1 ст. 361 або ч. 1 ст. 362 КК. Зрозуміло, що в такій ситуації слід використовувати положення ч. 2 ст. 11 КК, однак, разом із цим, така ситуація, як видається, свідчить про необхідність розгляду можливостей інших галузей права, додаткового аналізу чинного законодавства в контексті дотримання принципу економії репресії.

2.2. Метод контекстної законодавчої оцінки суспільної небезпечності діяння

Той факт, що кримінально-правова охорона інформаційної безпеки забезпечується за допомогою норм, що передбачають посягання на різноманітні родові об'єкти, зумовлює істотну специфіку методології дослідження. З метою врахування означеної специфіки було розроблено метод контекстної законодавчої оцінки суспільної небезпечності діяння.

Злочин – це діяння, що визнане соціумом як суспільно небезпечне. Оцінку цієї небезпечності, у тому числі й при встановленні розмірів санкцій відповідних кримінально-правових норм, має давати законодавець. Як правильно зазначає О.О. Книженко: "Диференціація заходів кримінально-правового впливу здійснюється на законодавчому рівні й полягає у встановленні в нормах кримінального законодавства форм та меж заходів кримінально-правового впливу" [129, с. 299]. При цьому "загальні вимоги щодо санкції полягають у тому, що покарання, зазначене в санкції, має відбивати ступінь суспільної небезпечності названого в диспозиції діяння та бути узгодженим із санкціями статей, що передбачають відповідальність за вчинення інших, близьких за видом та характером злочинів" [85, с. 35].

Однак через недостатність методології досить часто законодавча оцінка суспільної небезпечності діяння не відповідає об'єктивним соціальним потребам у кримінально-правовому впливі, є далекою від фактичної небезпечності посягання. Законодавчим оцінкам суспільної небезпечності властива суб'єк-

тивність і відсутність єдиного виваженого підходу [**Ошибка! Источник ссылки не найден.**, 268]. Одним із наслідків такого становища є набуття Кримінальним кодексом "рис розбалансованості" [381, с. 7 – 8]. Ю.А. Пономаренко зазначає, що, попри беззаперечне положення науки кримінального права стосовно відповідності суворості покарання ступеневі суспільної небезпечності злочину, непоодинокими є випадки його порушення [274]. Чинному КК властиві такі недоліки, як: надмірна суворість або надмірна м'якість санкцій; неспіврозмірність санкцій за злочини приблизно рівного ступеня суспільної небезпечності; неспіврозмірність санкцій основного та кваліфікованого складів злочинів тощо [275].

Названі недоліки повною мірою властиві системі кримінально-правових засобів забезпечення інформаційної безпеки. Наприклад, важко пояснити, чому розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132) є більш небезпечним, ніж, умисне розголошення лікарської таємниці, якщо таке діяння спричинило *тяжкі наслідки* (ст. 145). Бракуватиме аргументів і для пояснення приблизно однакової небезпечності некваліфікованого несанкціонованого втручання в роботу комп'ютерної техніки чи мереж електрозв'язку, що призвело до витоку інформації (ч. 1 ст. 361) та викрадення чи привласнення офіційних документів, *якщо вони спричинили порушення роботи підприємства, установи чи організації* (ч. 2 ст. 357).

Очевидно, що встановлення об'єктивної законодавчої оцінки суспільної небезпечності передбачає дослідження певного закону в контексті вже існуючих заборон. Тому аналіз кримінально-правових засобів охорони інформаційної безпеки потребує таких методів дослідження, які не обмежуються рамками одного розділу Особливої частини КК. Виникає питання методологічної основи порівняння кримінально-правових санкцій. На сьогодні найбільш поширеним індикатором суворості санкцій є її медіана, що дорівнює половині різниці максимальної та мінімальної меж санкції [268]. Однак цей показник

характеризується низкою недоліків, які значно обмежують можливості його використання. По-перше, він не враховує положення санкцій щодо додаткових покарань. По-друге, у разі порівняння покарань різних видів його використання пов'язане з застосуванням правил складання покарань (ст. 72 КК), серед яких відсутні положення щодо співвідношення таких покарань, як позбавлення волі на певний строк і штраф, а також позбавлення волі та позбавлення права обіймати певні посади або займатися певною діяльністю. Разом із тим, можливість представлення санкції, що передбачає таке покарання, як штраф, у вигляді іншого покарання існує. Для цього можна скористатися положеннями ч. 5 ст. 53. Проте такий підхід себе не виправдовує, оскільки в разі дотримання правил, що містяться в згаданих нормах, не завжди одержуються результати, які можна використовувати для порівняння суворості санкції. Так, якщо спробувати представити мінімуми та максимуми санкцій у вигляді позбавлення волі та скористатися означеною формулою, медіана більше ніж 30 санкцій буде мати негативне значення (ст.ст. 209-1, ч. 1 ст. 362, ч. 3 ст. 176, ч. 3 ст. 232-1 та ін.). Нонсенс, до якого приходимо в цьому разі, свідчить, що метод не є універсальним. По-третє, очевидним недоліком є й те, що в деяких випадках медіани санкцій, які істотно відрізняються за ступенем тяжкості, є однаковими або медіана більш суворої санкції є меншою, ніж медіана менш суворої. Наприклад, санкція ч. 2 ст. 414 (від 2 до 10 років позбавлення волі) є менш суворою, ніж санкція ч. 3 ст. 399 (від 8 до 15 років позбавлення волі), однак медіана ч. 2 ст. 414 є більшою. Інший приклад: порівняємо санкцію ч. 3 ст. 399 та ч. 3 ст. 377 (від 5 до 12 років позбавлення волі). За умови очевидної різниці суворості санкцій маємо однакову медіану. При цьому наявність у КК санкцій з достатньо великою різницею верхньої та нижньої меж є цілком обґрунтованою: у певних випадках існує необхідність законодавчої бази для врахування різноманітних за інтенсивністю чинників фактичної суспільної небезпечності конкретних злочинів. Таким чином, необхідність приведення законодавчих оцінок суспільної небезпечності посягань на ін-

формаційну безпеку у відповідність до їх фактичної небезпечності, а також відсутність універсальної та ефективної методології порівняння суворості санкцій зумовили розроблення *методу контекстного дослідження законодавчої оцінки суспільної небезпечності злочинів.*

Сутність методу полягає в тому, що кожний злочин розглядається в контексті інших з позицій порівняння та зіставлення видів і розмірів покарань, які можуть бути за нього призначені. Вихідним положенням є аксіоматичне судження про те, що законодавча оцінка суспільної небезпечності певного посягання дається в санкції відповідної норми Особливої частини КК. Таким чином, для того щоб розглядати певну конкретну кримінально-правову заборону в контексті інших за ознакою законодавчої оцінки суспільної небезпечності, необхідно з урахуванням положень науки кримінального права порівняти суворість санкцій конкретних злочинів і систематизувати кримінально-правові заборони за цією ознакою. Місце, отримане певним посяганням у цій системі, і буде являти контекстну законодавчу оцінку суспільної небезпечності посягання.

Ключовим питанням для використання методу контекстного дослідження законодавчої оцінки суспільної небезпечності злочинів є система правил визначення більш суворої та менш суворої санкції. Видається, що її основу мають складати достатньо розроблені наукою кримінального права положення щодо тлумачення ст. 5 КК України стосовно зворотної дії в часі закону, який пом'якшує кримінальну відповідальність. Найбільш вдало їх виклали В.І. Борисов та Ю.А. Пономаренко: "пом'якшення караності діяння має місце у випадках:

1) одночасного зниження верхньої і нижньої меж покарання;

2) зниження тільки верхньої або нижньої межі покарання при зберіганні незмінною іншої межі;

3) введення альтернативного більш м'якого основного покарання;

4) вилучення альтернативного більш суворого основного покарання;

5) заміни безальтернативного основного покарання більш м'яким;

6) зниження верхньої і/або нижньої меж додаткового покарання;

7) перетворення обов'язкового додаткового покарання на факультативне;

8) заміни додаткового покарання більш м'яким видом;

9) вилучення додаткового покарання" [193, с. 18].

Якщо виходити з наведених положень, то видається можливим сформулювати таку систему правил порівняння санкцій для здійснення контекстного дослідження законодавчої оцінки суспільної небезпечності злочинів:

1) більш суспільно небезпечним слід уважати злочин, за який може бути призначено більш суворе покарання;

2) за наявності альтернативних основних покарань більш небезпечним слід уважати той злочин, за вчинення якого можливим є призначення більш суворого альтернативного покарання;

3) за умови однакової верхньої межі основного покарання більш небезпечним є злочин, за який санкцією статті Особливої частини передбачено додаткове покарання;

4) за умови однакової верхньої межі основного покарання та наявності додаткових більш небезпечним є злочин, за який санкцією статті Особливої частини передбачено більш суворе додаткове покарання;

5) додаткове покарання одного виду є більш суворим, якщо воно є обов'язковим.

Необхідно зазначити, що ця система правил потребує певного уточнення у зв'язку з прийняттям Закону України "Про внесення змін до деяких законодавчих актів України щодо гуманізації відповідальності за правопорушення у сфері господарської діяльності" від 15 листопада 2011 року [98]. Справа в тому, що запроваджені цим законом зміни до ст. 12 КК, поро-

джують певні суперечності між положеннями КК щодо суворості покарань. Так, ст. 51 КК, яка визначає систему покарань, містить перелік видів покарань, упорядкований за ступенем суворості. Найменш суворим покаранням є штраф, і це положення означений закон не змінює. Тому з його прийняттям маємо випадки (37 санкцій) коли певні санкції з позицій ст. 51 КК слід розглядати як менш суворі, але з позицій ст. 12 ці санкції характеризуватимуть більш тяжкі злочини. Наприклад, за незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва (ч.1 ст. 203-1) закон передбачає основне покарання у вигляді штрафу від трьох до п'яти тисяч неоподатковуваних мінімумів доходів громадян. Відповідно до оновлених положень ст. 12 таке посягання слід відносити до злочинів середньої тяжкості. Водночас до злочинів невеликої тяжкості слід відносити посягання, за які передбачено покарання до двох років позбавлення волі. Візьмемо для прикладу статтю 140, яка передбачає відповідальність за неналежне виконання професійних обов'язків медичним або фармацевтичним працівником, якщо це спричинило тяжкі наслідки для хворого. За такий злочин передбачено покарання у вигляді: 1) позбавлення права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або 2) виправних робіт на строк до двох років, або 3) обмеження волі на строк до двох років, або 4) позбавлення волі на той самий строк. Кожне з означених покарань з позицій ст. 51 КК є більш суворим, ніж штраф у розмірі від трьох до п'яти тисяч неоподатковуваних мінімумів доходів громадян (ч. 1 ст. 203-1). Таким чином, санкція ч. 1 ст. 140 є більш суворою, ніж санкція ч. 1 ст. 203-1. Проте з позицій нової редакції ст. 12 КК: ч. 1 ст. 140 передбачає відповідальність за злочин невеликої тяжкості, а ч. 1 ст. 203-1 – середньої. Очевидно, що така ситуація потребуватиме в подальшому певних змін до законодавства в частині визначення системи покарань. Одночасно для цілей нашого дослідження маємо зазначити, що сформульована система правил порівняння санкцій буде використовуватися з урахуванням класифікації злочинів, передбаченої в чинній редакції ст. 12.

Тобто спочатку вся сукупність санкцій буде об'єднана в групи на підставі положень ст. 12. Після цього кожна з таких груп буде систематизована за наведеними правилами порівняння суворості санкцій.

Цілком зрозуміло, що виконання поставленого завдання передбачає опрацювання достатньо значного масиву інформації. Для того щоб отримати достовірні результати та мати можливість оперативного оновлення даних щодо законодавчої оцінки суспільної небезпечності злочинів (наприклад при внесенні змін до КК або в ході обговорення певних законотворчих пропозицій), необхідно звернутися до методів правової інформатики.

Перший етап ранжирування кримінально-правових заборон за рівнем законодавчої оцінки суспільної небезпечності передбачає формалізацію та систематизацію даних щодо змісту санкцій. Як відомо, формалізація – це представлення певної змістової ділянки у вигляді формальної системи. Остання у свою чергу являє собою знакову модель, яка задає множину об'єктів шляхом опису вихідних об'єктів і правил побудови нових [379, с. 114].

Кінцева мета поставленого завдання – порівняння законодавчих оцінок суспільної небезпечності злочинів – зумовлює специфіку необхідної формальної системи. Так, дослідження норм КК щодо системи та видів покарань дозволяє дійти висновку, що будь-яку з санкцій статей Особливої частини можна представити за допомогою множинності, яка складається з 27 елементів. Саме вони і є формальною системою для представлення законодавчої оцінки суспільної небезпечності злочину. Отже, застосована нами формальна система являє послідовність числових показників такого змісту (додаток 2).

Використовуючи зазначену формальну систему, ми представили відомості щодо санкцій наявних у чинному КК норм у формі матриці, рядки якої відповідають санкціям певних законів про кримінальну відповідальність, а стовпці – видам покарань. Подальше виконання завдання ранжирування кримінально-правових санкцій за ступенем суворості (законодавчої

оцінки суспільної небезпечності), передбачає сортування рядків отриманої матриці відповідно до наведених вище положень щодо порівняння суворості санкцій законів про кримінальну відповідальність. Це завдання потребує звернення до наступного методу правової інформатики – методу алгоритмізації. Алгоритм є певною послідовністю дій, виконання якої дає можливість досягти поставленої мети. Головними властивостями алгоритмів є дискретність, скінченність і визначеність. Дискретність проявляється в тому, що процедура розв'язання завдання розпадається на послідовність кроків (дискретизація за часом), а на кожному кроці обробляється порція інформації кінцевого обсягу (дискретизація за величиною). Скінченність алгоритму полягає в тому, що: 1) отримання результату має досягатися за скінченну кількість кроків; 2) набір дій, з яких побудовано алгоритм, теж скінченний. Під вимогою визначеності мається на увазі, що на кожному кроці алгоритму дії мають бути суворо визначені, опис кожного з етапів не дозволяє довільного тлумачення [379, с. 115 – 116].

Загальний принцип алгоритму ранжирування, застосованого для методу контекстної законодавчої оцінки суспільної небезпечності посягання, має такий вигляд. По-перше проводиться сортування санкцій за верхньою межею найбільш суворого покарання. По-друге виконується сортування за елементами, що характеризують додаткові покарання, у порядку зменшення їх суворості (конфіскація майна, позбавлення права обіймати певні посади або займатися певною діяльністю, штраф, спеціальна конфіскація). По-третє, здійснюється сортування за елементами, що характеризують альтернативні основні покарання також у порядку зменшення суворості. При цьому, ураховуючи, що наявність альтернативних основних покарань свідчить про більш м'яку санкцію, відповідні елементи матриці (пусті, ті, які свідчать про відсутність певних альтернативних покарань у конкретних санкціях) замінюються на значення, яке є більшим, ніж фактичне максимальне значення певної групи елементів (наприклад 99999). Це дозволяє в ре-

зультаті сортування розмістити кримінально-правові заборони в порядку, що відповідає зазначеному вище положенню про вплив альтернативних покарань на рівень законодавчої оцінки суспільної небезпечності.

Таким чином, маємо 10 послідовних груп для сортування, які виділяються за ознакою найбільш суворого основного покарання. Порядок сортування в кожній з виділених груп визначається відповідно до сформульованого вище загального принципу ранжирування. Використовуючи наведені визначення елементів формальної системи опису санкцій, викладемо в таблиці порядок сортування для кожної з визначених груп (додаток 3).

Отримана в результаті цієї системи операцій сортування послідовність аналізується з позицій порівняння. Рядок матриці, який опиниться на першому місці, буде відповідати злочину з найвищим рівнем законодавчої оцінки суспільної небезпечності. Рівень кожної наступної заборони визначається рекурентним шляхом: якщо множина елементів, що характеризують певну санкцію, еквівалента множині, яка відповідає попередньому злочину, то рівень законодавчої оцінки суспільної небезпечності цього злочину є таким само, як і в попереднього посягання, в іншому випадку показник рівня збільшується на одиницю. Таким чином, для кожної заборони, що міститься в Особливій частині КК, установлюється рівень законодавчої оцінки суспільної небезпечності. При цьому описаний алгоритм повністю відповідає означеним раніше вимогам. Він є дискретним, оскільки чітко виділено етапи розв'язання завдання. Виконання всіх етапів завжди приводитиме до побудови системи кримінально-правових санкцій, упорядкованої за ступенем законодавчої оцінки суспільної небезпечності, отже, алгоритм є скінченним. І, нарешті, йому властива визначеність: на кожному етапі використовується суворо визначений перелік дій, вільне тлумачення неможливе.

Для інформативного представлення результатів використання описаного методу пропонується використовувати чис-

ловий показник під назвою "індекс контекстної законодавчої оцінки суспільної небезпечності". Сутність цього показника полягає в тому, що він дозволяє представити місце, отримане конкретною кримінально-правовою забороною в результаті побудови описаного вище рейтингу, у вигляді числа зі значенням більше нуля, але не більше ста. Для найбільш небезпечного посягання він дорівнюватиме 100, для посягань, що знаходяться в середині побудованого рейтингу, – близько 50, індекс же посягань, що характеризуються найбільш м'якими санкціями, буде близьким до одиниці.

Розраховувати зазначений показник пропонується за формулою:

$$I_i^{\text{конт}} = \frac{N_{max} - N_i + 1}{N_{max}} \times 100,$$ де

$I_i^{\text{конт}}$ – індекс контекстної законодавчої оцінки суспільної небезпечності конкретного злочинного посягання;

$\mathbf{N_{max}}$ – максимальне значення побудованого рейтингу (місце, яке отримав найменш небезпечний злочин);

$\mathbf{N_i}$ – числове вираження місця, яке отримало в побудованому рейтингу те посягання, для якого встановлюється індекс.

Описаний алгоритм реалізовано в програмних засобах MS Access та MS Excel.

Використання запропонованого методу для дослідження засобів кримінально-правової охорони інформаційної безпеки дозволить по-новому підійти до оцінки обґрунтованості суворості відповідних кримінально-правових санкцій. Контекстна законодавча оцінка суспільної небезпечності, на відміну від існуючих методів порівняння, забезпечує можливість аналізу кожної кримінально-правової санкції в порівнянні з генеральною сукупністю, що дозволяє з великою ймовірністю прогнозувати значну ефективність методу, наближення законодавчих оцінок суспільної небезпечності певних посягань до їх фактичної, об'єктивної небезпечності.

Достатньо перспективним видається використання розглянутого методу в законотворчій роботі. В.Я. Тацій указував на те, що "правотворчій діяльності останніх років багато в чому властивий безсистемний, а іноді навіть хаотичний характер, а законопроекти, що виносяться на розгляд парламенту, не завжди проходять належну наукову експертизу. Все це, безумовно, знижує ефективність запобіжної функції закону про кримінальну відповідальність, негативно позначається на правозастосовній діяльності й призводить до нігілістичного ставлення громадян до вимог закону" [330, с. 17]. Аналізуючи можливі шляхи розвитку національного законодавства про кримінальну відповідальність, В.І. Борисов обґрунтовував доцільність саме *системних змін* у межах чинного КК [30, с. 283]. Установлення індексу контекстної законодавчої оцінки суспільної небезпечності в процесі роботи над проектами кримінально-правових норм дозволить чітко структурувати та скерувати дискурс щодо суворості санкції майбутньої норми, а отже, забезпечить *системний підхід* до вдосконалення КК, сприятиме попередженню законотворчих помилок.

Використання запропонованого методу може забезпечити певний розвиток і компаративістським кримінально-правовим дослідженням. Зрозуміло, що аналіз КК зарубіжної країни потребуватиме певного перегляду алгоритму порівняння та матриці даних залежно від передбаченої цим кодексом системи покарань. Однак використання запропонованого методу та встановлення індексів комплексної законодавчої оцінки суспільної небезпечності дозволяє приводити "до єдиного знаменника" заборони, передбачені кримінальними кодексами різних країн. Наприклад, вельми інформативним, як видається, буде порівняння індексів посягань, передбачених різними КК, але близьких за змістом об'єктивних і суб'єктивних ознак.

Разом із цим, необхідно зазначити, що метод має певні обмеження у використанні. Природно, що кількість заборон з певною інтенсивністю санкцій є неоднаковою. Так, наприклад, санкцій з верхньою межею в розмірі 15 років позбавлення волі у КК нараховується 43, 10 років – 72, 5 років – 164. З урахуван-

ням цього легко передбачити, що метод буде чітко "спрацьовувати", коли необхідно встановити, який злочин є більш суспільно небезпечним, або коли є необхідність систематизувати певну групу злочинів за ступенем суворості санкцій. Проте одного індексу контекстної законодавчої оцінки суспільної небезпечності посягання недостатньо для відповіді на питання, наскільки певна санкція є суворішою за іншу. Так, різниця індексів злочинів, передбачених ст. 257 (98,20) та ч. 3 ст. 286 (90,09), складає 8,11, при цьому верхня межа санкції за бандитизм – 15 років позбавлення волі, а за кваліфіковане порушення правил безпеки дорожнього руху – 10. Водночас, різниця індексів злочинів, передбачених ч. 1 ст. 194 (48,20) та ст. 118 (38,29), складає 9,91, при цьому верхня межа санкції за умисне знищення чужого майна – 3 роки позбавлення волі, а за вбивство при перевищенні меж необхідної оборони – 2. Тому, застосовуючи метод для розв'язання завдань щодо оцінки того, наскільки санкція за певний злочин суворіша за інший, бажано крім індексу контекстної оцінки використовувати також додаткові критерії, наприклад верхню межу основного покарання.

Підсумовуючи викладене, звернемося ще раз до дослідження В.К. Грищука. Аналіз рівня кримінально-правового регулювання в теоретичному аспекті дозволяє констатувати, що він може бути: "1) недостатнім, коли є необхідність кримінально-правового регулювання певних суспільних відносин; 2) достатнім, коли врегульовані кримінально-правовими засобами усі суспільні відносини, які об'єктивно вимагають такого регулювання…; 3) надлишковим (кримінально-правова зареґульованість), коли кримінально-правове регулювання поширено за межі об'єктивної необхідності" [75, с. 67]. "Кримінальне законодавство … при умові дотримання наукових основ правотворчості завжди є закономірним результатом розвитку суспільства. Воно служить активною формою відображення стану розвитку економічної, політичної, правової і духовної сфери життя суспільства, об'єктивізації інтересів суспільного розвитку. Маючи такі властивості воно в стані справляти зворотний

позитивний вплив на розвиток суспільних процесів" [75, с. 79 – 80]. Цілком зрозуміло, що досягнення бажаного – достатнього – рівня кримінально-правового регулювання відносин інформаційної безпеки можливе лише шляхом чіткого та послідовного врахування як загальних засад криміналізації суспільно-небезпечних діянь, так і специфічних соціальних потреб у кримінально-правовій охороні інформаційної безпеки. Побудова дієвої системи кримінально-правових засобів охорони інформаційної безпеки дозволить стимулювати позитивний розвиток відносин інформатизації в країні, забезпечити стабільний поступ до інформаційного суспільства, який є домінуючою тенденцією світових соціальних процесів та об'єктивною необхідністю для України.

Таким чином, до основних засобів кримінально-правової охорони інформаційної безпеки України слід відносити норми, які встановлюють відповідальність за посягання у сфері забезпечення доступу до інформаційного ресурсу, його формування, а також використання інформаційних технологій. Керуючись установленими в цій главі положеннями щодо доцільності криміналізації та вимог до її змісту, а також запропонованою методологією контекстної законодавчої оцінки суспільної небезпечності посягань, у подальших главах ми здійснимо аналіз цих засобів кримінально-правової охорони. Однак через те, що обсяг роботи не дозволяє провести аналіз усього масиву відповідних законів про кримінальну відповідальність, для виконання завдань дослідження та забезпечення якісного аналізу ми зупинимося на основних проблемах кримінально-правової охорони кожної з визначених складових інформаційної безпеки.

Висновки до другої глави

1. Основним засобом кримінально-правової охорони інформаційної безпеки є встановлення та реалізація кримінальної відповідальності за суспільно небезпечні посягання на неї.

2. Підставами криміналізації посягань на інформаційну безпеку виступають як соціальні процеси, що мають істотне значення для позитивних трансформацій суспільства в бік розвитку та стабільності, так і процеси, які, навпаки, мають небезпечний соціальний потенціал.

3. Характер суспільної небезпечності посягань на інформаційну безпеку визначається тим, що в умовах інформатизації суспільства, зростання соціальної значущості доступу до інформації, формування об'єктивних, повних та достатніх інформаційних ресурсів, використання з цією метою інформаційно-комунікаційних технологій істотну шкоду суспільству завдають посягання, що призводять до порушення можливості користування інформаційними ресурсами через обмеження доступу до них, спотворення процесу їх формування або унеможливлення користування інформацією через протиправні втручання в роботу інформаційних технологій. При цьому суспільна небезпечність посягань на інформаційну безпеку не є самостійною, вона залежить від соціальної значущості тих відносин, у межах яких використовується інформація, що є предметом посягання.

4. Приймаючи рішення про криміналізацію посягань на інформаційну безпеку, треба обов'язково враховувати її можливі негативні наслідки: неможливість для певної частини суспільства реалізувати інформаційну потребу через надмірну правову зарегульованість; неможливість реалізації в повному обсязі права власності на інформацію через надлишкові кримінально-правові гарантії доступу до інформаційних ресурсів; масштабні маніпуляції з масовою свідомістю зумовлені зловживаннями правовими гарантіями невтручання в діяльність засобів масової інформації; згортання процесів демократизації через надто широкі правові можливості держави у сфері контролю за діяльністю мас-медіа тощо.

5. Установлення кримінально-правових заборон у сфері інформаційної безпеки передбачає ретельне дослідження конструктивних галузей права у сфері регулювання інформаційної діяльності та ратифікованих міжнародно-правових

зобов'язань на предмет відсутності суперечностей із законодавчими новаціями, що будуть пропонуватися.

6. З огляду на те, що досліджувана сфера кримінально-правового захисту тісно пов'язана з досягненнями науково-технічного прогресу, необхідно з метою забезпечення стабільності кримінального законодавства при формулюванні змісту новацій обмежити використання понять, що відповідають певному рівневі технологічного розвитку.

7. Запропоновано метод контекстного дослідження законодавчої оцінки суспільної небезпечності злочинів. Сутність його полягає в тому, що кожний злочин розглядається в контексті інших з позицій порівняння та зіставлення видів і розмірів покарань, які можуть бути за нього призначені. Контекстна законодавча оцінка суспільної небезпечності, на відміну від існуючих методів порівняння, забезпечує можливість аналізу кожної кримінально-правової санкції в порівнянні з генеральною сукупністю, що дозволяє з великою ймовірністю прогнозувати значну ефективність методу, наближення законодавчих оцінок суспільної небезпечності певних посягань до їх фактичної, об'єктивної небезпечності. Достатньо перспективним видається використання розглянутого методу в законотворчій роботі, він може забезпечити певний розвиток і компаративістським кримінально-правовим дослідженням.

Глава 3

Злочини у сфері використання інформаційних технологій

Аналіз груп кримінально-правових заборон, що забезпечують охорону суспільних відносин інформаційної безпеки, уважаємо доцільним розпочати з розгляду проблем кримінальної відповідальності за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку. Таке рішення може бути обґрунтоване насамперед тим, що саме розвиток інформаційних технологій зумовив необхідність наукового аналізу проблем, які складають предмет дослідження. Крім того, як було зазначено в попередній главі, початок наукових досліджень соціальних наслідків інформатизації був детермінований знову ж таки чинниками технологічного характеру.

"Кіберзлочинність", "хакери", "комп'ютерний злом", "крадіжка машинного часу" – ці терміни вже перестали бути екзотикою для юристів. На сьогодні "комп'ютерні" злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Так, якщо у 2000 році "несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків даних, зареєстровано не було" [12, наводиться за 78, с. 121], а у 2001, відповідно до статистики МВС, було зареєстровано 5 таких злочинів, то вже у 2002 році їх було 30, у 2005 – 62, у 2007 – 145, у 2009 – 217. Тобто за вісім років ми спостерігаємо зростання більше ніж у 40 разів (!) кількості злочинів у сфері використання комп'ютерної техніки, зареєстрованих підрозділами МВС України. Зазначимо також, що наведені дані характеризують лише зареєстровані випадки. Проте на рівні монографічних

наукових досліджень доведено, що комп'ютерна злочинність характеризується високою латентністю, яка головним чином пов'язана з небажанням потерпілих подавати заяву до органів міліції; недосвідченістю правоохоронних органів у розслідуванні цих злочинів; складнощами в їх кваліфікації та доказуванні [320] Отже, наведене переконливо свідчить про те, що "комп'ютерні" злочини набули значення достатньо реальної загрози й потребують адекватних заходів протидії. Це ставить перед державою та суспільством завдання щодо розроблення засобів і методів боротьби з ними, удосконалення нормативної бази для цього.

Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини – розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж"; двічі положення цього розділу змінювалися та доповнювалися (Закони України "Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку" від 5 червня 2003 року та "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України" від 23 грудня 2004 року). Зростання кількісних показників комп'ютерної злочинності та постійне оновлення відповідних законів про кримінальну відповідальність краще за все підтверджують необхідність наукового аналізу проблеми.

Вихідним положенням у дослідженні кримінально-правової охорони суспільних відносин від посягань у сфері використання комп'ютерної техніки, безсумнівно, є аналіз чинників їх суспільної небезпечності.

Істотні зміни в суспільних відносинах на сучасному етапі розвитку викликані науково-технічним прогресом. Упровадження новітніх технологій в усі сфери життя суспільства неминуче приводить до значного розширення інформаційних потоків, зростання інформаційної потреби *("інформаційний вибух")*. Щоб діяти ефективно, сучасній людині необхідно ма-

ти набагато більший обсяг інформації, ніж людині, яка жила, приміром, на початку XX століття.

Однак зміна кількісних характеристик інформаційних процесів приводить до певної суперечності: з одного боку, для ефективної та результативної діяльності людині потрібні зростаючі обсяги інформації, з іншого боку, фізична здатність людини до зберігання, передачі й перероблення інформації обмежена.

Подолання такої ситуації пов'язане з розвитком суспільних процесів, які отримали назву *інформатизація*. Відповідно до Закону України "Про Національну програму інформатизації" вона являє собою "сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки".

Із процесом інформатизації тісно пов'язаний процес *комп'ютеризації:* розвиток і впровадження в різні сфери життя й діяльності людини технічної бази, яка забезпечує оперативну роботу з інформацією. Комп'ютерна техніка стала важливою умовою існування та розвитку суспільства, бо саме вона дозволяє зберігати, опрацьовувати та передавати величезні обсяги інформації, без яких ефективна діяльність тепер неможлива. Отже, комп'ютеризація як реакція людства на описану ситуацію "інформаційного вибуху" є технічною основою сучасного етапу інформатизації. Розвиток комп'ютерної техніки характеризується стрімким зростанням показників швидкості роботи та збільшенням обсягів інформації, яку дозволяють опрацьовувати комп'ютери. Завдяки успіхам технології ці процеси супроводжуються зменшенням відношення ціни та продуктивності ЕОМ, що зумовлює значне розширення сфери застосування комп'ютерної техніки.

Тож розширення сфери використання комп'ютерної техніки являє собою закономірний результат соціальної тенденції, що полягає в зростанні інформаційної потреби при здійсненні будь-якої діяльності. Відповідно, соціальне значення використання інформаційних технологій є не самостійним, а залежить від значення того виду діяльності, для інтенсифікації якого вони використовуються. Так, широке використання комп'ютерних технологій для управління економічними процесами потенційно небезпечне відповідними масштабними посяганнями. На думку експертів Організації з Безпеки та Співробітництва в Європі (ОБСЄ), злочинність, пов'язана з використанням комп'ютерних систем та мереж, здатна створити не менший хаос, ніж теперішня економічна криза. Шкода, яку щороку заподіює кіберзлочинність у світі, оцінюється приблизно у 100 млрд. доларів США і має тенденцію до зростання [126]. Також фахівці відзначають, що ці злочини набувають міжнародного характеру та загрожують економічним основам держав і світовій економічній системі [14]. Слід відзначити, що небезпека досліджуваних злочинів багаторазово збільшується, коли злочинець отримує доступ до автоматизованих систем, які використовуються в національній обороні [366, с. 58 – 62], керуванні рухом повітряного або наземного транспорту, контролі над небезпечним виробництвом та в інших сферах людської діяльності, які становлять підвищену небезпеку. Зазначимо, що силові відомства Росії та США визнають комп'ютерні злочини як реальну загрозу безпеці країни. Так, у ФСБ РФ заявляють про те, що в найближчому майбутньому існує небезпека терористичних кібератак на інформаційні мережі державних структур та приватних компаній, пов'язаних із керуванням об'єктами антикризової інфраструктури [125]. У свою чергу, аналітичний звіт американських фахівців "Оцінка загроз національній безпеці 2008 – 2013", містить дані про те, що загроза кібертероризму в найближчі п'ять років збільшуватиметься [353]. Відповідну оцінку цим негативним явищам дає і національний законодавець. Закон України "Про основи національної безпеки України" від 19 червня 2003 року до загроз

національній безпеці в інформаційній сфері відносить, зокрема, комп'ютерну злочинність та комп'ютерний тероризм.

З урахуванням сказаного цілком обґрунтованим видається такий висновок: *суспільна небезпечність злочинів у сфері використання комп'ютерної техніки головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології*. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це й визначає суспільну небезпечність конкретного посягання у сфері використання інформаційних технологій. Такий висновок відповідає і визначеним у попередній главі соціальним потребам у кримінально-правовій охороні суспільних відносин інформаційної безпеки у сфері використання інформаційних технологій.

Дослідження відповідності чинного кримінального законодавства вказаній специфіці суспільної небезпечності та соціальній потребі кримінально-правової охорони як необхідної передумови передбачає аналіз юридичного змісту складів злочинів, передбачених ст.ст. 361 – 363-1 КК України, та їх відмежування від суміжних складів. Спробу такого аналізу й буде здійснено в цій главі. Зазначимо також, що для цілей дослідження достатньо розгляду основних складів досліджуваних злочинів.

3.1. Аналіз складів злочинів, передбачених ст.ст. 361-361[1] КК України

У попередніх роботах [120, 385] ми доводили, що родовим об'єктом злочинів, передбачених у розділі XVI КК "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку", є частина інформаційних суспільних відносин, яку можна визначити як *інформаційні відносини, засобом реалізації яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку*. Інакше кажучи, злочини, передбачені цим розділом, посягають на *певну частину* інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів. У кримінальному законі наводяться чотири види таких засобів:

- електронно-обчислювальна машина (комп'ютер) – функціональний пристрій, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати розрахунки без участі людини [315, с. 7];

- автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, що здійснює цю діяльність [1, с. 2];

- комп'ютерна мережа – сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів [315, с. 7];

- телекомунікаційна мережа (мережа електрозв'язку) – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням [106].

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, можуть бути поділені на чотири види:

1) інформаційні відносини, засобом забезпечення яких є комп'ютери;

2) інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;

3) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

4) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

Перший вид цих інформаційних відносин – це найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Суб'єкти таких відносин використовують комп'ютерну техніку для виконання порівняно нескладних операцій, таких як підготування документів, проведення інженерних розрахунків, організація та робота з базами даних. Зазначимо, що під електронно-обчислювальною машиною розуміються не тільки комп'ютери в їх "класичному", можна сказати, звичному вигляді, тобто "системний блок – монітор – клавіатура – принтер", але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини. Так, у практиці російських правоохоронних органів траплялися випадки знищення інформації, яка зберігалася в пам'яті електронних касових апаратів. У результаті такого втручання знищувалася або модифікувалася інформація щодо платежів, які надійшли до каси, що в подальшому дозволяло приховувати реальні доходи від податкових органів [311]. Вчинене, безсумнівно, являє собою ухилення від сплати податків, але, крім цього, подібні дії необхідно додатково кваліфікувати як втручання в роботу ЕОМ, що призвело до знищення або перекручення комп'ютерної інформації. Адже касовий апарат містить процесор і може виконувати розрахунки без участі людини, тобто є електронно-обчислювальної машиною за визначенням. Те саме стосується й мобільних телефонів. Тому випадки так званого "перепрошивання" мобільних телефонів, незаконної зміни їхніх IMEI-кодів слід також кваліфікувати як несанкціоноване втручання в роботу ЕОМ, що призвело до підроблення комп'ютерної інформації.

Використання комп'ютерних систем відноситься до більш складних інформаційних відносин. Слід зазначити, що аналіз нормативно-правових актів показує невідповідність Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року (цей закон змінив Закон України "Про захист інформації в автоматизованих сис-

темах" від 5 липня 1994 року) та ДСТУ 2226-93 "Автоматизовані системи. Терміни та визначення" від 1 липня 1994 року. Термін "автоматизована система" визначається в цих нормативних актах неоднаково. Так, відповідно до закону інформаційна (автоматизована) система – це "організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів". Названий стандарт визначає автоматизовану систему інакше: "організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність" [1, с. 2]. На нашу думку, визначення, яке дається в законі, не зовсім вдале: керуючись ним, наприклад, неможливо відмежувати автоматизовану систему від електронно-обчислювальної машини, оскільки вона теж призначена для опрацювання даних, до її складу входять процесор, контролери, накопичувачі інформації (засоби обчислювальної техніки та зв'язку), її необхідним елементом є програмне забезпечення. У свою чергу, визначення, яке міститься в стандарті, є досить чітким і характеризує призначення автоматизованої системи – автоматизація певного виду людської діяльності. Визначення автоматизованої системи з огляду на її призначення видається більш вдалим для використання в контексті кримінально-правового дослідження, тому що дає можливість правильно вирішувати питання про соціальну значущість інформаційних відносин, пов'язаних з автоматизованими системами, а отже, і про суспільну небезпечність посягань на ці відносини. Автоматизовані системи використовуються для виконання широкого кола завдань: управління підприємством, технологічне підготування виробництва, контроль і випробування промислової продукції, управління службами життєзабезпечення підприємства і т.ін. Наприклад, одним із видів автоматизованих систем є система автоматизованого проектування, яка "призначена для автоматизації технологічного процесу проектування виробу, кінцевим результатом якого є комплект проектно-конструкторської документації, достатньої для виготовлення та подальшої експлуатації об'єкта проекту-

вання" [1, с. 12.]. Виходячи з призначення цієї системи можна зробити висновок, що суспільна небезпечність незаконного втручання в її роботу полягає: по-перше, у заподіянні шкоди інформаційним відносинам у сфері розроблення продукції та, по-друге, у загрозі заподіяння шкоди відносинам, що забезпечують випуск доброякісної продукції.

Третій вид інформаційних відносин, які утворюють досліджуваний родовий об'єкт, пов'язаний із використанням комп'ютерних мереж, що бувають двох видів: локальні, які об'єднують комп'ютери в межах однієї організації, і глобальні, які забезпечують зв'язок між різними організаціями, юридичними та фізичними особами. Найвідомішою і найпоширенішою глобальною комп'ютерною мережею є Інтернет, що застосовується в основному для таких видів роботи з інформацією: електронна пошта; передавання файлів; віддалений доступ – можливість підключатися до віддаленого комп'ютера й працювати з ним в інтерактивному режимі [68, с. 30 – 31]. Порушення цього виду інформаційних відносин полягає, як правило, у зменшенні ефективності роботи комп'ютерних мереж, неможливості або значній складності задоволення інформаційної потреби суб'єктами цих відносин.

Інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку, полягають у наданні й отриманні послуг електричного зв'язку, тобто у використанні мереж електрозв'язку для передавання або приймання інформації. Стосовно до визначення змісту цих суспільних відносин певний інтерес становить питання їх відмежування від інформаційних відносин, засобом забезпечення яких є комп'ютерні мережі. Закон України "Про телекомунікації" від 18 листопада 2005 року містить поняття "інформаційна система загального доступу", яке визначається таким чином: "сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних". Дані, відповідно до закону, – це інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки. Отже, можна дійти висновку, що комп'ютерні мережі, тобто технічні засоби, за допомо-

гою яких здійснюється опрацювання й передавання комп'ютерної інформації, відносяться до телекомунікаційних мереж, а інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі, – це певна частка інформаційних суспільних відносин, пов'язаних із використанням мереж електрозв'язку. Зазначимо, що таке розуміння є правильним, враховує сучасні тенденції розвитку комп'ютерних технологій. У найближчому майбутньому нас очікує ситуація, коли для зв'язку будуть використовуватися виключно комп'ютерні мережі (мережі, що забезпечують зв'язок між комп'ютерами). Уже зараз ми маємо мобільний зв'язок, цифрові АТС тощо. Отже, наявність у назві розділу XVI КК України та диспозиціях статей цього розділу терміна "мережа електрозв'язку" (відповідно до згаданого закону "телекомунікаційна мережа") можна визначити як відображення сучасних тенденцій розвитку технологій зв'язку. Однак наявність у законі про кримінальну відповідальність разом із цим терміном іншого – "комп'ютерна мережа" – фактично приводить до того, що під мережею електрозв'язку треба розуміти всі телекомунікаційні мережі, крім комп'ютерних (мережі міського, міжміського та міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення тощо). Таким чином, під інформаційними відносинами, засобом забезпечення яких виступають мережі електрозв'язку, слід розуміти суспільні відносини у сфері використання телекомунікаційних мереж за винятком комп'ютерних мереж.

Із визначенням родового об'єкта злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку пов'язана ще одна проблема – проблема найменування злочинів, які посягають на цей об'єкт. Закон визначає ці злочини поняттям "злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку".

У літературі дедалі частіше використовується таке їх визначення, як "*комп'ютерні злочини*". При цьому різні дослідники по-різному визначають обсяг цього поняття. Досить поши-

реним є віднесення до комп'ютерних злочинів всіх суспільно небезпечних посягань за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [117, с. 14; 2, с. 72; 26, с. 65] або "злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби" [20, с. 11; 290, с. 243; 70, с. 39 – 40; 212, с. 87; 26, с. 161]. Згідно з таким розумінням комп'ютерної злочинності комп'ютерним злочином може визнаватися будь-який злочин – розкрадання, шпигунство, незаконне збирання відомостей, які становлять комерційну таємницю, і т.ін., якщо він вчиняється з використанням комп'ютера. Видається, що таке розуміння комп'ютерних злочинів є неправильним, бо не дозволяє відбити їх сутність, специфіку та відрізнити від інших злочинів, у яких комп'ютер є лише знаряддям, засобом або предметом. Крім того, його використання в науковому контексті може призвести лише до плутанини через відсутність чітких меж дослідження.

Послідовним, відповідним системі законодавства про кримінальну відповідальність буде визначення, яке ґрунтується на найважливішій ознаці злочинів – їх об'єкті. Класифікація за родовим об'єктом – це системоутворюючий фактор сукупності норм Особливої частини КК. Тому визначення комп'ютерних злочинів має конструюватися на основі специфічних ознак їх родового об'єкта. Таким чином, у подальшому під комп'ютерними злочинами ми будемо розуміти ***суспільно небезпечні, протиправні, кримінально карані, вчинені суб'єктом злочину винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку (ст.ст. 361 – 363-1 КК).*** Зазначимо також, що терміни "комп'ютерні злочини", "злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку", "злочини у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку", а також "злочини у сфері використання інформаційних технологій" ми будемо використовувати як

тотожні. Аргументація щодо включення до наукового дискурсу терміна "злочини у сфері використання інформаційних технологій" наводиться в наступній главі.

Принагідно зауважимо, що деякі дослідники для найменування розгляданих злочинів пропонують використовувати термін, запозичений з КК Російської Федерації 1996 року, – "злочини у сфері комп'ютерної інформації" [3]. Однак цю пропозицію не можна назвати вдалою. Відповідно до національної законотворчої традиції та логіки систематизації норм Особливої частини КК, сполучення "у сфері" завжди використовується для вказівки на певну групу суспільних відносин, які виступають родовим об'єктом, наприклад: "у сфері господарської діяльності", "у сфері службової діяльності", "у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації" тощо. Оскільки комп'ютерна інформація не є сукупністю суспільних відносин за визначенням, то найменування "злочини у сфері комп'ютерної інформації" слід визнати беззмістовним.

Дослідження об'єкта комп'ютерних злочинів показує, що, крім розглянутого родового об'єкта, ці посягання можуть характеризуватися й наявністю додаткових факультативних об'єктів. Видається, що такими об'єктами можуть бути відносини в різних сферах діяльності людини, пов'язані з використанням електронно-обчислювальних машин, систем, комп'ютерних мереж або мереж електрозв'язку. Як правило, наявністю додаткового факультативного об'єкта характеризуються кваліфіковані комп'ютерні злочини, відповідальність за які пов'язується з настанням значної шкоди. У таких посяганнях від суспільних відносин, які виступають додатковим об'єктом, залежить характер значної шкоди, що визначається в кожному конкретному комп'ютерному злочині. Заподіюючи шкоду інформаційним відносинам, злочинець завдає або ставить під загрозу завдання шкоди ті суспільні відносини, для інтенсифікації яких застосовується комп'ютерна техніка. Такими можуть бути відносини адміністративного управління, управління виробництвом,

відносини, пов'язані з забезпеченням безпеки руху, відносини щодо розроблення нових технологій тощо.

Наприклад, у 2007 році слідчим відділом управління СБУ в Луганській області було порушено кримінальну справу за ст. 361 КК України. Винна особа використовувала реквізити доступу до мережі Інтернет, які належали одній з туристичних агенцій міста, унаслідок чого блокувала доступ до мережі законному користувачеві. Події відбувалися в самий розпал туристичного сезону, отже, через дії зловмисника працівники туристичної агенції були значно обмежені в можливостях замовляти квитки для проїзду клієнтів, зв'язуватися з іншими туроператорами [93], тобто блокування комп'ютерної інформації спричинило перешкоди в здійсненні господарської діяльності.

Несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Безпосереднім об'єктом несанкціонованого втручання є охоронювана кримінальним законом структурно організована та нормативно врегульована система соціально значущих відносин власності на комп'ютерну інформацію, яка забезпечує свободу реалізації права кожного учасника на задоволення інформаційної потреби [385]. Механізм заподіяння шкоди означеним суспільним відносинам полягає в порушенні, позбавленні або обмеженні реалізації власником інформації повноважень володіння, розпоряджання або користування нею. А зміст права власності на інформацію визначався в попередніх роботах як *сукупність права та можливості особи: володіти носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія* [120, 385].

Останнє визначення стало предметом критики в роботах деяких авторів. Так, Д.С. Азаров зазначає, що "хибність такого підходу можна проілюструвати одним простим прикладом: певна особа поміщує свою власність (інформацію) у банківський сейф (носій). Невже через те, що сейф не належить цій особі,

вона перестає бути власником того майна, що міститься у сейфі? Звичайно, ні. Так і комп'ютерна інформація, що належить одному власнику, може зберігатися на носії, який належить іншому (приміром створення окремою фізичною особою власної інформаційної сторінки в мережі Інтернет, яка розміщується на сервері провайдера). Отже, наведене зайвий раз переконує в тому, що визначати сутність права власності на певний об'єкт крізь категорію власності на інший є некоректним" [3, с. 53].

Погодимося з тим, що приклад є достатньо вдалим. Проте інформація, як ми доводили раніше, без носія не може бути включена в суспільні відносини, бути їх предметом. Це неможливо. Відповідно, потенційно неправильними слід визнавати намагання визначити власність на інформацію незалежно від її носія. Таким чином, наведений приклад корисний тим, що вимагає розгляду можливих видів відносин власності на комп'ютерну інформацію залежно від правового режиму її носія, але ні в якому разі не підтверджує "хибності підходу".

Найбільш поширеною є ситуація, коли право власності на комп'ютерну інформацію, пов'язане з носієм, що також належить власнику цієї інформації. У подальшому такий вид права власності на комп'ютерну інформацію будемо називати простим. Ускладнюється ця схема у випадках, коли інформація обробляється з використанням електронно-обчислювальних машин, які не належать власнику інформації. Крім розміщення інтернет-сторінки на сервері провайдера, це також буває при створенні електронної поштової скриньки на поштовому сервері або власного акаунту в соціальній мережі, веденні блогу на спеціалізованому сайті тощо. Ці випадки в термінах Закону України "Про захист інформації в телекомунікаційних системах" слід визначати як такі, коли власником інформації та власником системи є різні особи. Відповідно до ст. 5 цього закону відносини між власником інформації та власником системи визначаються договором. Як свідчить практика укладання таких договорів, вони містять положення стосовно надання власнику інформації як послуг, пов'язаних з обчислювальними можливостями систем, так і права користування носіями ін-

формації власника системи. Наприклад, у типовому договорі щодо надання доступу до мережі Інтернет, розміщеному на сайті ТОВ ТРК "Бриз" (м. Одеса), в числі іншого зазначається, що абоненту надається електронна поштова скринька, яка визначається як "простір на комп'ютерах Провайдера, призначений для тимчасового зберігання електронної пошти Абонента" [332], тобто абонентові такої мережі надається можливість користуватися носіями інформації власника системи. Інший приклад: у типовому договорі хостингу, яким визначаються засади розміщення сайту в мережі Інтернет, російського ТОВ "Аензет" (м. Новосибірськ) [333] спеціально обумовлюється, що до послуги розміщення сайту входить "дисковий простір для сайту" на сервері ТОВ "Аензет" розміром 500 Мб. Таким чином, право власності на комп'ютерну інформацію у випадках, коли власник інформації та власник системи є різними особами, відрізняється від простого права власності на комп'ютерну інформацію змістом повноважень володіння. Якщо за простої власності на комп'ютерну інформацію володіння полягає в тому, що особа має право та можливість володіти носієм комп'ютерної інформації, то в нашому випадку його слід визначати як наявність в особи права та можливості користуватися носієм інформації.

Отже, з урахуванням зробленого уточнення зміст права власності на комп'ютерну інформацію будемо визначати таким чином: *сукупність права та можливості особи: володіти або користуватися носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія.* При цьому зауважимо, що право власності є складовою частиною права на інформацію, яке визначається Законом України "Про інформацію" як "можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів" [103]. Як свідчить визначення, право на інформацію є достатньо складною категорією і включає можливість особи не тільки

володіти, користуватися та розпоряджатися нею, до нього також відноситься можливість отримання та поширення інформації. Ці складові розгляданого права охороняються іншим комплексом кримінально-правових норм, який ми будемо досліджувати в главах, присвячених відповідно охороні доступу до інформаційного ресурсу та його формування.

Необхідно зауважити, що зміни в редакції статті 361 КК (Закони України "Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку" від 5 червня 2003 року та "Про внесення змін до Кримінального та Кримінально-процесуального кодексів України" від 23 грудня 2004 року) зумовили появу нових характеристик безпосереднього об'єкта несанкціонованого втручання. Нова редакція аналізованої статті дає підстави стверджувати, що, крім права власності на комп'ютерну інформацію вона охороняє й *суспільні відносини надання та отримання послуг електрозв'язку*. До цих суспільних відносин можна застосувати термін "альтернативний безпосередній об'єкт злочину". Відповідно до змісту Закону України "Про телекомунікації" від 18 листопада 2003 року всі мережі електрозв'язку поділяються на мережі загального користування (мережі, доступ до яких відкрито для всіх споживачів телекомунікаційних послуг) та мережі спеціального користування. Зміст цих відносин полягає в тому, що оператори та провайдери телекомунікаційних послуг забезпечують їх споживачам можливість передавання та приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних або інших електромагнітних систем. Зауважимо, що комп'ютерні мережі за визначенням також слід відносити до мереж електрозв'язку. Однак наявність у диспозиції однієї статті таких двох термінів, як "комп'ютерна мережа" та "мережа електрозв'язку", свідчить про необхідність обмежувального тлумачення терміна "мережа електрозв'язку" в диспозиції статей розділу XVI КК України: до мереж електрозв'язку відносяться всі телекомунікаційні мережі, крім комп'ютерних.

Зазначимо, що у вітчизняній науці висловлюються й інші думки щодо безпосереднього об'єкта несанкціонованого втручання. Так, Д.С. Азаров наполягає на тому, що основним безпосереднім об'єктом цього злочину виступають "окремі суспільні відносини, які існують з приводу здійснення певною особою (особами) інформаційної діяльності щодо комп'ютерної інформації чи з приводу обміну інформацією мережами електрозв'язку і яким заподіяна чи створена загроза заподіяння істотної шкоди конкретним злочином". Зміст суспільних відносин інформаційної діяльності щодо комп'ютерної інформації полягає у взаємозв'язку права суб'єкта цієї діяльності на створення, збирання, пошук, розповсюдження, використання, споживання, перетворення, введення, копіювання, зчитування, знищення, реєстрацію комп'ютерної інформації та обов'язків інших учасників відносин цьому не перешкоджати [6, с. 32 – 39]. Додатковим безпосереднім об'єктом розгляданого злочину, на погляд Д.С. Азарова, є суспільні відносини власності щодо певної інформації, яким "завжди завдається шкода, оскільки інформація завжди перебуває у чиїйсь власності" [3, с. 62]. Подібні положення містяться й у дослідженні М.В. Рудика [305, с. 89].

Близьким є й визначення безпосереднього об'єкта несанкціонованого втручання, яке запропонував С.О. Орлов: "суспільні відносини щодо обробки інформації в комп'ютерних системах та телекомунікаційних мережах та забезпечення їх нормальної роботи" [254, с. 184]. Зауважимо, що дослідження С.О. Орлова було здійснено до прийняття змін та доповнень 2004 року, але його висновки можуть використовуватись і при аналізі складу злочину, передбаченого чинною редакцією ст. 361 КК.

Наведені визначення, як видається, не відповідають сутності несанкціонованого втручання як посягання, суспільна небезпечність якого зумовлена непорушенням обробки інформації чи нормальної роботи обладнання, а значенням, цінністю інформації якає предметом посягання. Як ми вже зазначали, комп'ютеризована обробка інформації чи безвідмовне функціонування комп'ютерних пристроїв не мають самостійного

суспільного значення. Вони отримують його тільки з огляду на цінність інформації, для роботи з якою застосовуються. Тому саме по собі порушення інформаційної діяльності щодо комп'ютерної інформації або порушення функціонування комп'ютерної техніки не може вважатися суспільно небезпечним. У зв'язку з цим логічним наслідком визнання безпосереднім об'єктом досліджуваного злочину відносин, які існують з приводу здійснення інформаційної діяльності, або відносин забезпечення нормальної роботи комп'ютерної техніки буде відсутність чітких критеріїв визначення суспільної небезпечності конкретних посягань. А це вже, у свою чергу, має не тільки теоретичні наслідки, але й потенційно небезпечне ускладненнями в правозастосовній практиці, оскільки повертає нас до проблеми критеріїв віднесення конкретних посягань до малозначних діянь (ч. 2 ст. 11 КК). Розглянемо два приклади:

1) особа незаконно втручається в роботу ЕОМ і знищує інформацію про новітні наукові розробки;

2) особа незаконно втручається в роботу ЕОМ і знищує інформацію неістотного змісту, яка зовсім не впливає на діяльність її власника.

Цілком зрозуміло, що суспільна небезпечність незаконного втручання в другому прикладі, на відміну від першого, недостатня для визнання такого діяння злочином. Однак якщо визначати об'єкт несанкціонованого втручання як інформаційну діяльність щодо комп'ютерної інформації або як безпеку використання засобів комп'ютерної техніки, то ці два приклади слід розглядати як такі, що мають однаковий ступінь суспільної небезпечності. Адже і в першому, і в другому було заподіяно приблизно однакову шкоду інформаційній діяльності або безпеці використання ЕОМ.

У свою чергу розуміння в подібній ситуації несанкціонованого втручання як посягання на відносини власності на інформацію дозволяє обгрунтовано довести відсутність суспільної небезпечності в другому випадку. Саме використання категорії "власність" дозволяє включити до аргументації питання

цінності предмета й адекватно розв'язати завдання визначення суспільної небезпечності.

Предметом злочину, передбаченого ст. 361 КК України, судячи з диспозиції є *інформація,* але аналіз об'єкта й форм об'єктивної сторони несанкціонованого втручання дає підстави стверджувати, що до предметів цього злочину відносяться комп'ютерна інформація та інформація, що передається каналами зв'язку.

Комп'ютерна інформація. Об'єкт і предмет будь-якого злочину є взаємозалежними, взаємозумовленими. Тому, аналізуючи ознаки предмета несанкціонованого втручання, необхідно виходити з викладеної вище характеристики змісту безпосереднього об'єкта як *відносин власності на інформацію.* У попередніх роботах [120, 385] ми доводили, що фізичною ознакою комп'ютерної інформації як предмета злочину є наявність носія – предмета або сигналу, фізичні, хімічні чи інші властивості якого використовуються для зберігання, передавання й опрацювання інформації, що розпізнається електронно-обчислювальною машиною. Економічна ознака комп'ютерної інформації як предмета злочину виражається в тому, що вона є цілісною, доступною, конфіденційною, такою, що має ціну. Юридична ознака комп'ютерної інформації виражається в тому, що вона повинна бути чужою для винного й мати свого власника.

Отже, комп'ютерна інформація як предмет злочину визначалася таким чином: *відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну* [120, 385].

Необхідно зазначити, що запропоноване нами визначення комп'ютерної інформації стало предметом наукової дискусії, у ході якої були висловлені зауваження, які потребують контраргументації. Ключовим аспектом критики колег було положення про те, що в запропонованому визначенні комп'ютерна інформація нібито ототожнюється з її носієм або одне поняття фактично підмінюється іншим [3, с. 96; 220, с. 81; 86]. По-перше, у роботі, на яку посилаються дослідники, автор зазначав,

що "інформація є нематеріальним об'єктом, який включається в систему суспільних відносин за допомогою носія – матеріального об'єкта" [120, с. 25], тобто ні в якому разі не ототожнював носій з інформацією. Дійсно, специфіка комп'ютерної інформації як предмета злочину полягає в тому, що вона може існувати на різних носіях, але в кожному конкретному випадку несанкціонованого втручання в роботу комп'ютерної техніки предметом є інформація на певному, чітко визначеному носієві. Ознаки саме цього носія повинні бути встановлені та досліджені в ході досудового слідства та підтверджені під час судового розгляду кримінальної справи. Отже, не можна виключати носій інформації з характеристики предмета досліджуваного злочину.

Однак науковці, що оспорюють запропоноване визначення, заперечують останнє положення й тому формулюють хибні висновки. Так, С.В. Дрьомов уважає, що комп'ютерна інформація як предмет злочину, передбаченого ст. 362 КК України, є річчю нематеріального світу [86, с. 132]. О. Мазуренко та Н. Розенфельд пропонують визнавати комп'ютерну інформацію предметом не матеріальним, а віртуальним, оскільки сама по собі вона не має зовнішнього представлення, але може набути його завдяки застосуванню до неї спеціальних засобів та способів – комп'ютерних систем, які надають їй форми, придатної для сприйняття та обробки, вона "не має фізичної матеріальної ознаки" [220, с. 82]. Викладена позиція означених дослідників щодо предмета злочину як речі нематеріального світу або віртуального предмета є дещо спірною. По-перше, вона не узгоджується з загальновизнаними положеннями стосовно сутності категорій "ідеальне" та "матеріальне". "Ідеальне" – це категорія для позначення особливої, нематеріальної природи тих образів дійсності, що виникають у людській свідомості [365, с. 168]. "Матеріальне", на протилежність ідеальному, являє собою визначеність об'єктів, процесів людської діяльності, що виражає насамперед їхню причетність до матерії, тобто незалежне від волі й свідомості людей існування. [365, с. 279]. Не потребує додаткової аргументації той факт, що предмет

посягань у сфері використання комп'ютерної техніки існує незалежно від свідомості винної особи, тобто є матеріальним. Знищення, перекручення або блокування комп'ютерної інформації настає не у свідомості правопорушника або потерпілої особи, а в об'єктивній дійсності. По-друге, нематеріальний або віртуальний предмет, напевно, має встановлюватися та досліджуватися відповідними слідчими діями – нематеріальними, такими, що відбуваються у свідомості. Маємо очевидний нонсенс, отже, пропозиція, щодо комп'ютерної інформації як нематеріального предмета не може бути визнана правильною.

Д.С. Азаров, який також критикує запропоноване вище визначення, не вважає комп'ютерну інформацію ідеальною: на його думку, вона "безумовно володіє ознаками матерії" [3, с. 98]. Однак носій інформації, як він уважає, не є атрибутивною властивістю досліджуваного предмета. Питання про те, чи можна інформацію (зокрема комп'ютерну) визнавати предметом злочину, треба вирішувати, не пов'язуючи її з носієм. [3, с. 97]. З точки зору Д.С. Азарова, канали зв'язку, поля або сигнали не є носіями, вони, "за своїми технічними характеристиками призначені не для зберігання інформації, а для її передавання від одного носія до іншого і не можуть зберігати інформацію у постійному, незмінному стані" [3, с. 72 – 73]. Отже, інформація в процесі передачі її каналами зв'язку характеризується відсутністю носія. Аналогічне розуміння ми має відображення й у роботі О. Мазуренко та Н. Розенфельд, які під комп'ютерною інформацією пропонують розуміти інформацію, "що зберігається на електронних носіях або передається між ними, незалежно від способу її фізичного або логічного представлення, і може створюватися, оброблятися, змінюватися та використовуватися за допомогою електронно-обчислювальних машин, систем та комп'ютерних мереж" [220, с. 82]. Такі твердження ґрунтуються на невиправдано вузькому розумінні носія інформації та суперечать аксіоматичним положенням як інформатики так і чинного законодавства. В. Вєхов зазначає, що комп'ютерна інформація *завжди* опосередкована через матеріальний (машинний) носій, поза яким вона існува-

ти не може. Він уважає, що носій являє собою"будь-який технічний пристрій, фізичне поле або сигнал, призначені для фіксації, зберігання, накопичення, перетворення та (або) передачі комп'ютерної інформації" [54, с. 17]. Такий підхід є абсолютно справедливим і підтверджується також положеннями національного закону "Про державну таємницю", який до матеріальних носіїв секретної інформації відносить "матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо" [100]. Отже, комп'ютерною інформацією є відомості, які подані у формі, що дозволяє її опрацювання за допомогою відповідних технічних засобів. При цьому форма цього подання не обмежується записом комп'ютерної інформації на певний диск або флеш-карту, вона включає також оперативну пам'ять комп'ютера, сигнали в каналах зв'язку тощо.

Означена помилка приводить як О. Мазуренко та Н. Розенфельд, так і Д.С. Азарова до висновку про те, що стосовно комп'ютерної інформації некоректно використовувати термін "річ". Якщо в комп'ютерної інформації не завжди є носій, то вона й не річ. Крім того, вона "не може бути визнана речовим предметом матеріального світу, оскільки будь-які речі можуть сприйматися за допомогою органів чуття безпосередньо, без участі у цьому процесі яких-небудь спеціальних засобів" [220, с. 81]. У цьому положенні спостерігається змішування понять "річ" та "тіло". Річчю слід уважати "все те, що перебуває у відношенні з чимось або має якісь властивості, категорія мисленя, яка фіксує відособленість (практичну і теоретичну) одних предметів від інших. Один предмет відрізняється від іншого своїми властивостями, які становлять якісну межу речі… Якщо межі між речами мають просторовий характер, вони звуться тілами" [365, с. 446]. Сказаного цілком достатньо для того, щоб обґрунтовано застосовувати до комп'ютерної інформації категорію "річ". Вона завжди характеризується наявністю носія, має власні змістовні та формальні властивості, якими відрізняється від інших речей, існує незалежно від свідомості людини,

саме тому вона є річчю матеріального світу. Отже комп'ютерна інформація цілком відповідає класичному визначенню предмета злочину. Цей висновок, у свою чергу, вимагає критично оцінити пропозиції деяких науковців "дещо розширити поняття предмета злочину" [3, с. 98], та відносити до нього "явища об'єктивного світу" [220, с. 80] або "матеріальні утворення" [3, с. 99].

Разом із цим, не можна не погодитися, що суспільний розвиток, і це особливо рельєфно проявляється при дослідженні комп'ютерних злочинів, вимагає певного вдосконалення методологічних засад дослідження предмета. Найбільш вдало це завдання розв'язав Є.В. Лащук, який обґрунтовано довів, що предмет злочину – "це факультативна ознака об'єкта злочину, що знаходить свій прояв у матеріальних цінностях (котрі людина може сприймати органами чуття чи фіксувати спеціальними технічними засобами), з приводу яких та (або) шляхом безпосереднього впливу на які вчиняється злочинне діяння"[204, с. 10]. При цьому "фізична ознака характеризує матеріальність предмета злочину… матеріальними (фізичними) слід вважати цінності, що можуть сприйматися органами чуття людини або спеціальними технічними засобами" [204, с. 10]; "соціальна ознака характеризує предмет злочину як цінність – те, що оцінюється, тобто включено у систему відносин між людьми" [204, с. 10]; "юридичну ознаку предмета злочину визначають: наявність злочинних діянь, вчинених з приводу відповідних матеріальних цінностей та (або) спрямованих безпосередньо на них; підпорядкованість предмета об'єкту злочину; суб'єктивне ставлення злочинця до предмета (бажання вплинути на нього певним чином); форма визначення (як саме – безпосередньо чи опосередковано предмет злочину визначений у кримінально-правовій нормі) та факультативність (предмет не є обов'язковим для всіх складів злочинів)" [204, с. 11]. Саме такий підхід до розуміння предмета злочину ми й будемо використовувати надалі.

Інформація, що передається каналами зв'язку. Співвідношення категорій "інформація, що передається мережами елект-

розв'язку" та "комп'ютерна інформація", яка теж відноситься до предметів незаконного втручання, можна визначити таким чином: якщо комп'ютерна інформація – це відомості, подані у формі, яка дозволяє опрацьовувати їх за допомогою ЕОМ, то інформацією, що передається мережами електрозв'язку, є *відомості, подані у формі, що дозволяє їх приймати або передавати засобами електрозв'язку*. Інформація в цих мережах передається за допомогою сигналів, які є матеріальними носіями передавання інформації. Слід зауважити, що електричні сигнали в мережах електрозв'язку можуть бути носіями комп'ютерної інформації. Наприклад, у комп'ютерних мережах телефонні лінії використовуються для зв'язку між ЕОМ, що знаходяться в мережі. У такому разі інформація, що передається мережею електрозв'язку, є комп'ютерною, а її знищення чи перекручення треба розглядати як наслідок несанкціонованого втручання в роботу комп'ютерної мережі.

Диспозиція статті 361 КК України дозволяє зробити висновок про те, що *об'єктивна сторона несанкціонованого втручання* характеризується такою структурою: *діяння* – несанкціоноване втручання в роботу ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку; *суспільно небезпечні наслідки* – витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації, порушення встановленого порядку маршрутизації інформації (перелічені наслідки є альтернативними, тобто для наявності складу злочину достатньо настання хоча б одного з наслідків); *причинний зв'язок між діянням та наслідками*.

Стосовно визначення несанкціонованого втручання серед науковців немає єдиної точки зору. Так, деякі автори вважають що воно може проявлятися в несанкціонованому доступі, котрий розуміється як доступ до інформації, пов'язаний з подоланням програмних, технічних чи організаційних заходів захисту, або в несанкціонованому впливі на інформацію, що здійснюється з порушенням методів і процедур автоматизованого опрацювання інформації [37, с. 15 – 17]. Стаття 361 КК не містить указівки на те, що несанкціоноване втручання обов'язково має супроводжуватися подоланням засобів захисту інфо-

рмації, отже, таке визначення є не зовсім вдалим. А.А. Музика та Д.С. Азаров визначають несанкціоноване втручання як вплив на інформаційні процеси за умови, що він є несанкціонованим. При цьому зазначається, що фізичний вплив безпосередньо на ЕОМ, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку чи відповідні носії інформації не охоплюється складом злочину, передбаченого ст. 361 КК України. На думку названих авторів, такі діяння, вчинені з метою заволодіння інформацією, знищення, пошкодження, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку маршрутизації інформації, за наявності підстав можуть кваліфікуватися за ст. 360 КК або як відповідний злочин проти власності [236, с. 26 – 29]. Коментуючи цю позицію, зазначимо, що вона є більш вдалою, але має схожу ваду: диспозиція ст. 361 не обмежує спосіб вчинення діяння, вона не містить указівки на те, що діяння не може бути вчинене шляхом безпосереднього фізичного впливу на засоби комп'ютерної техніки або телекомунікації.

Аксіомою є таке положення: діяння, що належить до об'єктивної сторони складу злочину, є суспільно небезпечним, тобто заподіює істотну шкоду суспільним відносинам, охоронюваним кримінальним законом, або створює реальну загрозу її заподіяння [190, с. 119 – 120]. Інакше кажучи, зміст діяння визначається об'єктом злочину, діянням є дія або бездіяльність, яка заподіює або може заподіяти шкоду об'єкту. Оскільки, як було зазначено раніше, безпосередній об'єкт досліджуваного злочину характеризується певною подвійністю, можна виокремити такі види несанкціонованого втручання, які розрізняються за змістом:

- несанкціоноване втручання в роботу ЕОМ, автоматизованих систем і комп'ютерних мереж;

- несанкціоноване втручання в роботу мереж електрозв'язку.

Виділення видів несанкціонованого втручання на підставі специфіки об'єкта дозволяє сформулювати ще одне положення: зміст ознак несанкціонованого втручання в роботу комп'ютерної техніки визначається тим, що воно заподіює шкоду відно-

синам власності на комп'ютерну інформацію, а несанкціонованого втручання в роботу мереж електрозв'язку – тим, що воно заподіює шкоду відносинам надання й отримання послуг електрозв'язку.

Втручання в роботу ЕОМ, систем або комп'ютерних мереж слід розуміти як зміну режиму роботи електронно-обчислювальної машини, системи, комп'ютерної мережі. Конкретизуємо зміст ознак цього діяння, установивши його фізичну, соціальну та юридичну ознаки. *Фізична* ознака втручання виявляється в тому, що *воно полягає у впливі на матеріальний носій комп'ютерної інформації або засоби її автоматизованого опрацювання.* Суспільна небезпечність(*соціальна* ознака) несанкціонованого втручання визначається тим, що діяння ставить під загрозу функціонування електронно-обчислювальних машин, систем і комп'ютерних мереж у сфері зберігання, опрацювання, зміни, доповнення, передавання й одержання інформації, тобто заподіює шкоду суспільним відносинам права власності на комп'ютерну інформацію. *Протиправність* як обов'язкова ознака аналізованого діяння характеризується в законі за допомогою терміна "несанкціоноване". Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року під несанкціонованими діями щодо інформації в системі розуміються дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Викладене дозволяє дати таке визначення несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж: *зміна режиму роботи ЕОМ, системи або комп'ютерної мережі, вчинена шляхом впливу на носій комп'ютерної інформації або засоби її автоматизованого опрацювання, з порушенням встановленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію.*

До наслідків несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж відносяться: 1) витік; 2) втрата; 3) підробка; 4) блокування комп'ютерної інформації; 5) спо-

творення процесу обробки комп'ютерної інформації; 6) порушення встановленого порядку маршрутизації комп'ютерної інформації.

Безперечним є те, що якісні характеристики суспільно небезпечних наслідків залежать від змісту об'єкта посягання. На думку Н.Ф. Кузнєцової, злочинний наслідок – це сполучна ланка між об'єктом і злочинним діянням [197,с. 10.]. А.А. Пінаєв наголошує, що наслідки визначаються об'єктом злочину [267, с. 58]. Отже, цілком обґрунтованим буде таке положення: перелічені суспільно небезпечні наслідки несанкціонованого втручання в роботу ЕОМ, систем або комп'ютерних мереж являють собою різні форми порушення права власності на комп'ютерну інформацію.

Так, *витік* інформації відповідно до статті 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження. Зазначимо, що витік матиме місце не тільки в тих випадках, коли суб'єкт посягання отримує незаконний доступ до інформації, але й тоді, коли такий доступ отримують треті особи.

Термін "*втрата комп'ютерної інформації*", як видається, є тотожним термінові "знищення комп'ютерної інформації", являючи собою *такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, що дозволяє опрацьовувати її за допомогою комп'ютерної техніки*.

Слід зазначити, що комп'ютерна інформація, у певних випадках її знищення, деякий час фактично не втрачається: змінюється лише перший символ в імені файлу, і тому він стає непридатним під час використання стандартних, традиційних програмних засобів. Фізичне місце на носієві, яке відповідає такому файлу, уважається вільним, тому інформація фактично втрачається лише після того, як на це місце буде записано нову інформацію. Тобто у власника певний час є можливість

відновити знищену інформацію. У зв'язку з такою особливістю комп'ютерної інформації висловлювалися пропозиції щодо кваліфікації дій винної особи як замаху на знищення, у разі відновлення інформації або існування її копії (про яку винному відомо не було) [88, с. 93]. Однак правильним і послідовним видається підхід до вирішення цього питання А.Г. Волєводза, який пише, що можливість відновити комп'ютерну інформацію за допомогою апаратно-програмних засобів або отримати її від іншого користувача не звільняє винного від відповідальності [58, с. 67 – 68]. Доцільним у зв'язку з цим буде відзначити, що можливість відновлення певних предметів у разі їх пошкодження не означає необхідності застосування в таких випадках норм про попередню злочинну діяльність. Зауважимо, що кваліфікація знищення комп'ютерної інформації незалежно від можливості її відновлення сприйнята і на рівні судової практики. Так, у вироку за звинуваченням особи в злочині, передбаченому ст. 272 КК РФ (ст. 361 КК України) суддя Центрального районного суду м. Барнаула Т.Д. Попова справедливо зазначає: "Наявна у користувача можливість відновити знищену інформацію за допомогою засобів програмного забезпечення або отримати дану інформацію від іншої особи не звільняє винного від відповідальності" [293].

Підробка комп'ютерної інформації являє собою порушення такого повноваження власника, як користування, адже через підробку власник повністю або частково втрачає можливість реалізовувати свою інформаційну потребу. Зважаючи на це, можна так визначити підробку комп'ютерної інформації: *зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.*

Блокування комп'ютерної інформації також є специфічною формою порушення повноваження користування інформацією. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року містить термін "блокування інформації в системі", який визначається

таким чином: дії, унаслідок яких унеможливлюється доступ до інформації в системі. Отже, блокування являє собою ситуацію, коли комп'ютерна інформація не знищена, не підроблена, але використання її неможливе. Можна сформулювати таке визначення: *блокування комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.*

Прикладом несанкціонованого втручання в роботу комп'ютерної мережі, що призвело до блокування інформації, можуть слугувати так звані розподілені атаки відмови від обслуговування (DDoS-атаки, Distributed Denial of Service attacks), які полягають у надсиланні дуже великої кількості запитів на один або кілька серверів, що викликає їх перевантаження та призводить до того, що інформаційний ресурс, доступ до якого забезпечується сервером, стає недоступним.

Спотворення процесу обробки комп'ютерної інформації. Обробка інформації в автоматизованій системі відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року являє собою виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. З урахуванням цього спотворення процесу обробки комп'ютерної інформації можна визначити як *отримання в результаті операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми*.

Порушення встановленого порядку маршрутизації комп'ютерної інформації матиме місце, коли комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням установленого порядку.

Для прикладу несанкціонованого втручання в роботу комп'ютерної мережі розглянемо вирок Корольовського районного суду м. Житомира в справі № 1-162/2009 від 5 березня 2009 року [157] за обвинуваченням В., який, перебуваючи за місцем свого проживання й використовуючи власний персональний комп'ютер та викрадений комутатор, несанкціоновано втрутився в роботу комп'ютерної мережі фірми-провайдера шляхом незаконного підключення до неї. Після цього використовував інформаційні ресурси цієї мережі у власних інтересах, що призвело до блокування інформації та порушення встановленого порядку її маршрутизації, оскільки законним абонентам мережі було блоковано доступ до її ресурсів.

Суд правильно кваліфікував дії Л. як *несанкціоноване втручання в роботу комп'ютерної мережі*, що призвело до *блокування* інформації (яке полягає в тому, що абонентам, робота яких у мережі проходила через сервер, незаконний доступ до якого отримав винний, було блоковано доступ до ресурсів цієї мережі), і *порушення встановленого порядку її маршрутизації* (яке полягає в тому, що особа, яка не має законного права користуватися ресурсами комп'ютерної мережі, отримала до неї доступ, не передбачений власником мережі).

Несанкціоноване втручання в роботу мережі електрозв'язку являє собою зміну режиму її роботи. Оскільки, як було зазначено, до складу мережі електрозв'язку входять технічні засоби та споруди зв'язку, *фізичну властивість* несанкціонованого втручання в роботу мережі електрозв'язку можна визначити як *зміну режиму роботи мережі, що вчинена шляхом впливу на засоби або споруди зв'язку*. Суспільна небезпечність такого діяння, його *соціальна* ознака полягають у тому, що воно ставить під загрозу суспільні відносини щодо надання й отримання послуг електрозв'язку, унаслідок цього діяння абоненти мережі отримують неякісні послуги зв'язку або не отримують їх зовсім. *Протиправність* як обов'язкова ознака несанкціонованого втручання в роботу мереж електрозв'язку полягає в тому, що це діяння є порушенням установленого нормативно-правовими актами режиму користування мережами елект-

розв'язку. Слід погодитися з М.І. Пановим, який зазначає, що системи електрозв'язку належать певному власнику – юридичній або фізичній особі, і "на втручання в їх роботу винна особа не має ні дійсного, ні передбачуваного права" [193, с. 975]. Отже, можна запропонувати таке визначення: *несанкціоноване втручання в роботу мережі електрозв'язку –порушення встановленого режиму роботи мережі, вчинене шляхом впливу на засоби або споруди зв'язку, що ставить під загрозу суспільні відносини щодо надання й отримання послуг електрозв'язку.*

До наслідків несанкціонованого втручання в роботу мереж електрозв'язку відносяться: 1) витік; 2) втрата; 3) підробка; 4) блокування інформації, що передається каналами зв'язку; 5) порушення встановленого порядку маршрутизації інформації, що передається каналами зв'язку. Специфіка об'єкта й предмета цього посягання визначає й особливості змісту його суспільно небезпечних наслідків.

Отже, *витік* інформації, що передається мережею електрозв'язку, можна визначити за аналогією з витоком комп'ютерної інформації таким чином: результат несанкціонованого втручання в роботу мережі електрозв'язку, унаслідок якого інформація, що передається мережею, стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї.

Втрата інформації, що передається мережами електрозв'язку, – це порушення електрозв'язку у вигляді неотримання абонентом мережі інформації, якому вона надсилається.

Підробкою інформації буде такий вплив на носій інформації, що передається мережею електрозв'язку, у результаті якого абонент отримує відомості, які не збігаються з тими, що було йому надіслано.

Блокування інформації, що передається каналами зв'язку, є результатом несанкціонованого втручання в роботу мережі електрозв'язку у вигляді неможливості або значного ускладнення протягом певного часу отримувати чи надсилати інформацію за допомогою цієї мережі.

Порушення порядку маршрутизації інформації в мережі електрозв'язку, як правило, матиме місце, коли інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним не отримується, а також у випадках отримання інформації, що передається в мережі, на кінцеве обладнання, яке не є складовою цієї мережі. Типовими прикладами несанкціонованого втручання в роботу мереж електрозв'язку з настанням таких наслідків є незаконне підключення телефонних апаратів до мереж телефонного зв'язку, а також незаконне підключення телевізійних приймачів до мереж кабельного телебачення. Однак зазначимо, що існують і більш складні види порушення порядку маршрутизації, які пов'язані, зокрема, з маршрутизацією вхідного міжнародного трафіку на телефонні мережі загального користування. У судовій практиці такий вид досліджуваних наслідків траплявся в контексті правової оцінки дій осіб, які займалися незаконною діяльністю щодо надання послуг IP-телефонії [169].

Під *спотворенням процесу обробки* інформації, що передається каналами електрозв'язку, необхідно розуміти отримання в результаті роботи технічного засобу зв'язку результатів, що не відповідають його характеристиці. Необхідно зазначити, що підробка та спотворення процесу обробки інформації в мережі електрозв'язку можуть характеризуватися спільним суспільно небезпечним результатом (заподіянням об'єкту однакової шкоди), однак різним є механізм її заподіяння: підробка вчиняється шляхом впливу на носій інформації, а спотворення процесу оброблення – шляхом впливу на технічний засіб зв'язку.

Причинний зв'язок як обов'язкова ознака об'єктивної сторони несанкціонованого втручання в роботу ЕОМ, систем, комп'ютерних мереж або мереж електрозв'язку полягає в тому, що діяння (несанкціоноване втручання) з необхідністю спричиняє настання наслідків: воно передує настанню зазначених

суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку є необхідною умовою, без якої б наслідки не настали.

Несанкціоноване втручання буде закінченим з моменту настання суспільно небезпечних наслідків.

Для прикладу несанкціонованого втручання в роботу мережі електрозв'язку розглянемо вирок Придніпровського районного суду м. Черкаси в справі № 1-223/07 від 12 червня 2007 року [162] за обвинуваченням Л. у вчиненні злочину, передбаченого ч. 2 ст. 361 КК України. Підсудний умисно, без дозволу К., яка згідно з договором про надання послуг електрозв'язку є абонентом ВАТ "Укртелеком", протягом одного місяця, з метою незаконного отримання для себе телефонних послуг здійснив несанкціоноване втручання до робочої мережі електрозв'язку, що виразилось у підключенні до її телефонного номеру та здійсненні телефонних розмов за послугою "Аудіотекст".

Ураховуючи зазначене а також те, що підсудний у подібний спосіб незаконно підключався до телефонних номерів ще трьох інших абонентів, суд правильно кваліфікував його дії як *несанкціоноване втручання в роботу мережі електрозв'язку*, яке спричинило *блокування* інформації абонента, що для абонента виразилося в неможливості користування телекомунікаційними послугами, та *вчинене повторно порушення встановленого порядку маршрутизації*, унаслідок чого телекомунікаційна інформація ВАТ "Укртелеком" фактично не надходила до кінцевого обладнання дійсного абонента, хоча обладнання ВАТ "Укртелеком" фіксувало, що абонент користується послугою.

Суб'єкт несанкціонованого втручання загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Суб'єктивна сторона несанкціонованого втручання виражається в тому, що особа: а) усвідомлювала суспільну небезпечність втручання, тобто фактичні та соціальні ознаки діяння, його несанкціонованість; б) передбачала наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення порядку її

маршрутизації; в) бажала або свідомо припускала настання цих наслідків. Тобто суб'єктивна сторона аналізованого складу може виражатись у вигляді як прямого, так і непрямого умислу.

Кримінальна відповідальність за незаконні дії зі шкідливими програмними або технічними засобами. Безпосередній об'єкт злочину, передбаченого ст. 361-1 КК, складають суспільні відносини власності на комп'ютерну інформацію та відносини надання й отримання послуг електрозв'язку. Зазначимо, що специфіка механізму заподіяння шкоди цим суспільним відносинам у результаті вчинення означеного злочину полягає в тому, що через створення, розповсюдження або збут шкідливих програмних чи технічних засобів створюється реальна загроза порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

До *предметів* злочину відносяться:

- шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

- шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Зазначимо, що в науці висловлювалися й інші погляди щодо характеристики предмета злочину, передбаченого ст. 361-1 КК України. Так, С.Ю. Ільченко крім шкідливих програмних і технічних засобів до предметів 361-1 відносить також електронно-обчислювальні машини, системи, комп'ютерні мережі та мережі електрозв'язку [113, с. 12]. О.А. Федотов також уважає, що до предметів посягань у сфері використання комп'ютерної техніки слід відносити обчислювальну техніку як інформаційну структуру і матеріальний носій інформації [363]. Аналіз цієї пропозиції вимагає звернення до класичного визначення предмета злочину, яке сформулював В.Я. Таційй: "будь-які речі матеріального світу, із певними властивостями яких кримінальний закон пов'язує наявність у діяннях особи

ознак конкретного складу злочину" [329, с. 47]. Видається, що не потребує додаткових аргументів той факт, що наявність у кримінальному законодавстві такої норми, як 361-1, зумовлена небезпечними властивостями саме шкідливих програмних або технічних засобів. Отже, електронно-обчислювальні машини, системи, комп'ютерні мережі та мережі електрозв'язку не можуть уважатися предметами досліджуваного злочину за визначенням.

У подальшому викладі шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, будуть називатися скорочено – *шкідливі програмні та технічні засоби*. Тож, до предметів злочину, передбаченого ст. 361-1 КК, закон відносить програмні та технічні засоби, які: а) є шкідливими та б) призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Передбачена в законі ознака "шкідливі" характеризує ці програмні та технічні засоби як такі, використання яких заподіює шкоду інформаційним відносинам, засобом забезпечення яких є комп'ютерна техніка чи мережі електрозв'язку, або створює небезпеку її заподіяння. Наступна ознака, "призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку", указує на їх спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж електрозв'язку. На відміну від будь-яких інших комп'ютерних програм та обладнання шкідливі програмні та технічні засоби спеціально розробляються для несанкціонованого втручання, тобто порушення режиму роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Тому під *шкідливими програмними засобами*, призначеними для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам.

Технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, – це різного роду пристрої, устаткування, розроблені для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам. Прикладом кримінальної відповідальності за незаконні дії з подібними пристроями може слугувати вирок Ленінського районного суду м. Кіровограда в справі № 1-133/10 від 10 червня 2010 року [154], яким засуджено особу, котра здійснила збут технічного пристрою "Portable mobile signale jammer". Засуджений продавав пристрій, який заглушував сигнал стільникового або мобільного зв'язку. При цьому він, як особа обізнана зі шкідливими властивостями пристрою, надавав консультацію щодо його технічних параметрів, зазначаючи, що при його використанні блокуються будь-які дзвінки мобільного зв'язку. Згідно з висновком судової комп'ютерно-технічної експертизи поданий на дослідження пристрій – у робочому стані, при користуванні досліджуваним пристроєм відбувається переривання (якщо з'єднання вже відбулося) та блокування (якщо абонент, що викликається, перебуває в зоні дії працюючого пристрою) з'єднань оператора мобільного зв'язку між абонентами, пристрій виконує шкідливі функції щодо блокування та переривання розмов у мережі ДжіСМ зв'язку і за своєю дією є шкідливим технічним пристроєм.

Ураховуючи функції вказаного пристрою – переривання та блокування розмов (інформації) у межах електрозв'язку, а також його здатність впливати на процес передавання сигналу (інформації) та відсутність можливості його застосування за

будь-яким іншим призначенням, він обґрунтовано був визнаний таким, що призначений для несанкціонованого втручання в роботу мереж електрозв'язку.

Злочин, передбачений ч. 1 ст. 361-1 КК, відноситься до злочинів із *формальним* складом, тобто вважається закінченим із моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Досліджувана норма передбачає такі форми *об'єктивної сторони*:

1) створення шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;

2) розповсюдження шкідливих програмних або технічних засобів;

3) збут шкідливих програмних або технічних засобів.

Створення шкідливих програмних або технічних засобів являє собою результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу. Зазначимо, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети використання, розповсюдження або збуту.

Розповсюдження шкідливих програмних – це оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх "закладання" в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення [385].

Для прикладу розповсюдження шкідливих програм шляхом надання доступу розглянемо вирок Кіровського районного суду м. Кіровограда в справі № 1-57/08 від 16 січня 2009 року [175] за обвинуваченням А. у вчиненні злочину, передбаченого ч. 1. ст. 361-1 КК України. У вироку зазначається, що А., користуючись локальною комп'ютерною мережею гуртожитків, діючи умисно, завантажив у власний комп'ютер програмні засоби. Ці засоби пізніше експертним шляхом було визнано програмами для віддаленого зчитування паролів або нейтралізації засобів захисту комп'ютерних програм чи інформації, які після встановлення паролів та їх нейтралізації надають можливість доступу до певної комп'ютерної інформації, комп'ютер-

ної програми, комп'ютерної мережі, операційної системи та здійснення непомітно для власника чи законного користувача несанкціонованої передачі інформації сторонній особі.

Після цього А. надав вільний доступ до свого комп'ютера всім абонентам локальної мережі. Суд правильно кваліфікував дії А. за ч.1 ст. 361-1 КК як розповсюдження шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп'ютерної техніки.

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну специфіку. Крім простого передавання таких засобів можливим є їх установлення в електронно-обчислювальні машини, системи або комп'ютерні мережі, які продаються або передаються на іншій основі, наприклад здаються в оренду. Отже, розповсюдження шкідливих технічних засобів можна визначити таким чином: *оплатне або безоплатне передавання шкідливого технічного засобу, а також його установлення в ЕОМ, системи або комп'ютерні мережі.*

Треба зазначити ще одну особливість розповсюдження шкідливих програмних і технічних засобів. Воно може здійснюватися як за згодою особи, якій ці засоби надаються, так і без неї. У ряді випадків згода особи на одержання шкідливого програмного або технічного засобу може виключати суспільну небезпечність, а отже, караність діяння. До таких випадків слід віднести придбання шкідливих програм або технічних засобів для перевірки систем інформаційної безпеки, створення антивірусних програм, а також із метою проведення досліджень. Водночас кримінальна відповідальність не виключається, якщо названі засоби купуються для вчинення злочинів або правопорушень. Відсутність в особи, яка розповсюджує шкідливі програмні та технічні засоби за згодою особи, що їх купує, відомостей про мету їх подальшого використання не виключає суспільної небезпечності, а отже, злочинності розповсюдження.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний із відчу-

женням предмета. Тобто якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий програмний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває. Отже, під збутом шкідливих програмних або технічних засобів слід розуміти *їх оплатне або безоплатне відчуження*. Типовим прикладом збуту шкідливих програм є продаж дисків з записаними на них шкідливими програмами [177].

Розгляд форм об'єктивної сторони цього злочину був би неповним без коментування деяких результатів дисертаційного дослідження Т.В. Міхайліної. Дослідниця обґрунтовує такі положення. Розповсюдження шкідливих програмних засобів – це "передача фізичного носія зі шкідливими програмними засобами виключно в безоплатний спосіб або передача (чи пропозиція) шкідливих програм для ЕОМ через автоматизовані системи чи комп'ютерні мережі в оплатний чи безоплатний спосіб" [235, с. 13]. Розповсюдження шкідливих технічних засобів – "їх фізичне відчуження виключно в безоплатний спосіб" [235, с. 14]. Збут шкідливих програмних засобів – "форма передачі або реалізації шкідливих програмних засобів, внаслідок якої вони передаються у володіння або розпорядження інших осіб виключно на платній основі… під час збуту відбувається незаконне відчуження шкідливих програмних засобів виключно на фізичному носії" [235, с. 14]. Як можна зрозуміти, збут шкідливих технічних засобів являє собою їх фізичне відчуження виключно на платній основі. Спроба автора відійти від запропонованої вище класифікації розповсюдження та збуту на підставі відчуження предмета видається не зовсім вдалою. Дослідниця змішує у своїх визначеннях принципово різні характеристики дій щодо шкідливих програмних і технічних засобів. Навряд чи можна вважати послідовним таке положення: якщо передача дисків є платною – має місце збут, розповсюдженням буде тільки безоплатна передача дисків з шкідливим програмним забезпеченням,а також надання платного або без-

оплатного доступу до них, наприклад, через Інтернет. Принципова різниця збуту та розповсюдження навіть на лінгвістичному рівні у тому, що при збуті предмет не залишається в особи, яка його здійснює. При розповсюдженні ж це має місце та взагалі робить його можливим.

Суб'єкт даного злочину загальний, ним є фізична, осудна особа, що досягла 16-річного віку.

Оскільки злочин, передбачений ст. 361-1 КК,відноситься до злочинів із формальним складом,зміст його *суб'єктивної сторони* визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажанні вчинення таких дій. Отже, у цій формі умисел може бути тільки прямим, а його специфіка виражається в тому, що свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджувані засоби *спеціально призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку*.

Обов'язковою ознакою суб'єктивної сторони цього комп'ютерного злочину є усвідомлення особою специфічних властивостей та призначення технічних і програмних засобів, які вона розповсюджує. У випадку якщо особа не усвідомлює властивостей програмних або технічних засобів, розповсюджуваних нею, виключається кримінальна відповідальність за їх розповсюдження. У цьому розумінні показовим є приклад розповсюдження шкідливих програм під виглядом нового програмного забезпечення. Особа розробляє програму з прихованою шкідливою функцією та подає її для загального користування в комп'ютерну мережу. Крім того, вона готує повідомлення, у якому пропонує, наприклад, за винагороду розповсюджувати цю програму всім, хто її скопіював. У такому разі кримінальна відповідальність осіб, які скопіювали цю програму й розповсюджують її, виключається через відсутність усвідомлення ними шкідливих властивостей предмета злочину. Якщо ж осо-

ба помилялася стосовно властивостей розповсюджуваних програмних або технічних засобів, тобто вважала їх шкідливими, але вони такими не були, відповідальність повинна наставати за замах на розповсюдження шкідливих програмних і технічних засобів.

Усвідомлення діяння як складовий елемент суб'єктивної сторони розповсюдження чи збуту шкідливих програмних або технічних засобів полягає в розумінні особою того, що в результаті її дій використання шкідливих засобів стає можливим для іншої особи або певної кількості осіб.

Кримінально-правова охорона комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК України). Об'єктом злочину – несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України), виступають суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом злочину є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. Тобто інформація, що є предметом злочину, передбаченого ст. 361-2 КК України, характеризується такими ознаками:

1) вона відноситься до інформації з обмеженим доступом;

2) зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

3) створена відповідно до чинного законодавства;

4) захищена відповідно до чинного законодавства.

До *інформації з обмеженим доступом* згідно зі статтею 30 Закону України "Про інформацію" [103] відноситься конфіденційна, таємна та службова інформація.

До таємної та службової інформації належать відомості, що становлять державну та іншу *передбачену законом* таємницю. Саме на рівні закону встановлюється порядок віднесення інформації до таких видів, а також порядок доступу до неї.

Наприклад, державна таємниця – вид таємної інформації, яка охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України та які віднесено законом до державної таємниці й поставлено під охорону з боку держави. Віднесення інформації до державної таємниці та порядок її використання визначаються Законом України "Про державну таємницю" від 21 січня 1994 року [100]. Перелік відомостей, що становлять державну таємницю, затверджується наказом директора Служби безпеки України.

До таємної інформації, крім державної, відноситься також інша передбачена законом таємниця, розголошення якої завдає шкоди особі, суспільству, державі. Такою може бути, наприклад, таємниця страхування [105], таємниця усиновлення, таємниця досудового слідства тощо.

Конфіденційною інформація є інформація про фізичну особу, а також інформація, доступ до якої обмежено *фізичною або юридичною особою*, крім суб'єктів владних повноважень [103]. Громадяни та юридичні особи, котрі володіють інформацією професійного, ділового, комерційного та іншого характеру, придбаною на власні кошти або такою, що є предметом їх професійного, ділового, комерційного та іншого інтересу, самостійно визначають її належність до конфіденційної. Наприклад, на підставі ч. 1 ст. 36 Господарського кодексу України, відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, але розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею.

Перелік відомостей, що складають комерційну таємницю підприємства, порядок роботи з ними й організація їх охорони визначаються наказом керівника, зміст якого не повинен суперечити положенням чинного законодавства. Підставою для прийняття такого наказу служить згадана норма Господарського кодексу, у якій зазначається: "Склад і обсяг відомостей, що складають комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону". Перелік відомостей, які не можуть складати комерційну таємницю, міститься в Постанові Кабінету Міністрів України № 611 від 9 серпня 1993 року "Про перелік відомостей, які не складають комерційну таємницю".

Використання терміна "інформація, яка зберігається (або оброблюється (ст. 362 КК України)) в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або на носіях такої інформації" є не зовсім вдалим, оскільки він громіздкий, а за змістом повністю відповідає більш вдалому термінові "комп'ютерна інформація", що використовувався в попередній редакції розділу XVI КК України. Крім того, навряд чи можна визнати доцільним розмежування термінів "інформація, що оброблюється..." (ст. 362 КК) та "інформація, що зберігається..." (ст. 361-2 КК) оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення. У цьому питанні можна погодитися з Д.С. Азаровим, який зазначає, що закон має визначати форму подання інформації, а не спосіб або засоби її оброблення чи зберігання [5, с. 29]. Таким чином, друга виділена нами ознака інформації як предмета злочину, передбаченого ст. 361-2 КК, полягає в тому, що вона є комп'ютерною, тобто подана у формі, що дозволяє її оброблення або зберігання з використанням комп'ютерної техніки.

Інформація, що є предметом цього злочину, *створена відповідно до чинного законодавства*, тобто розповсюдження або збут інформації, створеної з порушенням законодавства, не є злочином, передбаченим ст. 361-2 КК України.

Нарешті, предметом розгляданого злочину є тільки інформація, яка "захищена відповідно до чинного законодавства". Наприклад, відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року власник системи, у якій оброблюється інформація, що є власністю держави, або інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, зобов'язаний утворювати службу захисту інформації (ч. 2 ст. 9 закону). Крім того, така інформація повинна оброблятися із застосуванням "*комплексної системи захисту інформації з підтвердженою відповідністю*" (ч. 2 ст. 8 закону). У цьому випадку захищену подібним чином інформацію можна відносити до предметів посягання, передбаченого ст. 361-2 КК. Склад указаного злочину буде мати місце тоді, коли незаконно розповсюджується або збувається інформація, що зберігається з застосуванням комплексної системи захисту. Ця система являє собою сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації. Відповідно до чинного законодавства видачу атестатів відповідності комплексних систем захисту інформації здійснює Державна служба спеціального зв'язку та захисту інформації України [99].

Зауважимо, що деякі дослідники вважають предметом злочину, передбаченого ст. 361-2 КК, тільки ту інформацію, яка відповідно до закону підлягає обов'язковому захисту. Керуючись цим, доходять висновку про те, що предметом злочину тут може бути тільки інформація, що становить державну таємницю, конфіденційна інформація, що є власністю держави, банківська таємниця, а також таємниця телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікації [3, с. 91, с. 104]. Таке бачення видається необґрунтовано звуженим. У диспозиції статті 361-2 КК ідеться про інформацію, "захищену відповідно до чинного законодавства", а не про інформацію, "вимога щодо захисту якої міститься в законодавстві". Це означає, що до "інформації, захищеної відповідно до чинного законодавства", слід відноси-

ти як ту, що підлягає обов'язковому захисту, так і ту, захист якої може здійснюватися відповідно до закону. Українське законодавство в питанні створення систем захисту інформації містить не тільки імперативні, але й диспозитивні приписи. Наприклад, ч. 2 ст. 21 Закону України "Про інформацію" наділяє громадян та юридичних осіб правом самостійно визначати режим доступу до неї, включаючи належність її до категорії конфіденційної. Достатньо цікавим у цьому плані є регулювання права на захист від незаконного використання комерційної таємниці. Так, відповідно до ст. 162 Господарського кодексу України однією з умов наявності такого права є вживання належних заходів до охорони її конфіденційності. Отже, до предметів досліджуваного злочину слід відносити комп'ютерну інформацію з обмеженим доступом, яка створена відповідно до закону та захищена специфічними засобами, використання яких відповідає законодавству.

За конструкцією *об'єктивної сторони* злочин, передбачений ст. 361-2 КК України, є формальним. Він уважається закінченим із моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом.

Збут або розповсюдження інформації буде *несанкціонованим*, якщо вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженим доступом являє собою оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб. Одним із прикладів подібного діяння є незаконне розповсюдження персональних даних. Так, у 2003 році в продажу з'явилася база даних абонентів одного з лідерів російського ринку операторів стільникового зв'язку "Мобільні ТелеСистеми" (МТС). База даних містила такі персональні дані про абонентів компанії, як прізвище, ім'я, по батькові, дата народження, паспортні дані, індивідуальний номер платника податків тощо. При цьому інформація про появу такої бази даних за кілька тижнів розповсюджувалася в Інтернеті [234].

Під *збутом комп'ютерної інформації з обмеженим доступом* необхідно розуміти її оплатне або безоплатне відчуження.

Суб'єкт злочину – загальний. Якщо збут або розповсюдження інформації з обмеженим доступом вчиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, вчинене, за наявності відповідних ознак суб'єктивної сторони, необхідно кваліфікувати за статтею 232 або 328 КК України. Більш докладно питання відмежування злочину, передбаченого ст. 361-2 КК України, від суміжних буде розглянуто нижче.

Суб'єктивна сторона цього злочину характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпечність і протиправність збуту або розповсюдження комп'ютерної інформації з обмеженим доступом та бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Кримінальна відповідальність за незаконні дії з комп'ютерною інформацією, вчинені особою, яка має право доступу до неї. Як свідчить практика зарубіжних правоохоронних органів, досить часто комп'ютерні злочини вчиняються суб'єктами, котрі мають певні повноваження щодо роботи з інформацією, яка є предметом посягання. Так, Роберт Корні, консультант із питань безпеки в корпорації Ай-Бі-Ем, відзначає, що лише 3% порушень інформаційної безпеки пов'язані з діяльністю осіб, які не мають певного відношення до діяльності конкретних підприємств, компаній; інші 97% порушень вчиняють їх службовці [136, с. 219]. Спеціальні дослідження американських правоохоронних органів щодо порушень інформаційної безпеки в Національному центрі кримінальної інформації (National Crime Information Center) показали, що більшість таких порушень вчинено службовцями цієї організації [422]. Про те, що більшість злочинів у сфері використання електронно-обчислювальних машин, систем і комп'ютерних мереж вчиняються працівниками підприємств, установ чи організацій, які по-

страждали, свідчать і результати експертних опитувань працівників служб безпеки. На їхню думку, найбільша небезпека в плані вчинення комп'ютерних злочинів "виходить саме від безпосередніх користувачів, і ними вчиняється 94% злочинів, тимчасом як опосередкованими користувачами – тільки 6%" [26, с. 131]. Таким чином, практика боротьби з комп'ютерними злочинами свідчить про підвищену небезпечність цих злочинів у випадку їх вчинення особою, яка має право доступу до інформації, що є предметом посягання. Саме це й зумовило наявність у КК України ст. 362, яка передбачає відповідальність спеціального суб'єкта за незаконні дії з комп'ютерною інформацією.

Об'єктом цього злочину виступають суспільні відносини власності на комп'ютерну інформацію. *Предметом* злочину відповідно до диспозиції є інформація, яка опрацьовується в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації. Як уже зазначалося, термін, що вживається для характеристики предмета, є не зовсім вдалим: він громіздкий, а за змістом не відрізняється від більш вдалого – "комп'ютерна інформація". Отже, предметом цього злочину є комп'ютерна інформація, ознаки якої розглядалися вище.

Об'єктивна сторона розгляданого злочину характеризується наявністю декількох форм:

1) несанкціонована зміна комп'ютерної інформації;

2) несанкціоноване знищення комп'ютерної інформації;

3) несанкціоноване блокування комп'ютерної інформації;

4) несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;

5) несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

Несанкціонована зміна комп'ютерної інформації являє собою порушення права власності на інформацію шляхом перекручення без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особи, яка має право власності на таку інформацію.

Несанкціоноване знищення комп'ютерної інформації має місце тоді, коли вона перестає існувати у формі, яка дозволяє її опрацьовувати за допомогою комп'ютерної техніки.

Несанкціоноване блокування комп'ютерної інформації – позбавлення власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Якщо три перші форми являють собою прості, звичайні злочини з матеріальним складом і вважаються закінченими з моменту настання зазначених наслідків, то структура двох останніх – несанкціонованого перехоплення та копіювання – ускладнена наявністю похідного наслідку – витоку інформації, якому передують таки види порушення права власності на комп'ютерну інформацію, як несанкціоноване копіювання або перехоплення.

Оскільки *витік інформації* відповідно до статті 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року є результатом дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що *не мають права доступу до неї*, можна зробити висновок, що предметом несанкціонованого перехоплення або копіювання є тільки комп'ютерна інформація з обмеженим доступом (таємна або конфіденційна).

Копіювання комп'ютерної інформації – це "відтворення даних зі збереженням вихідної інформації" [264, с. 170]. Тож несанкціоноване копіювання можна визначити як відтворення, з перевищенням наданих власником прав доступу, комп'ютерної інформації з обмеженим доступом зі збереженням вихідної інформації. Наприклад, особа має право лише на ознайомлення та внесення змін до певної бази даних, а вона без дозволу власника створює її копію. Погодимося з С.В. Дрьомовим у тому, що для констатації факту копіювання однією з визна-

чальних обставин, що підлягають установленню, є тотожність змісту цієї інформації зі змістом отриманої. [89, с. 147].

Перехоплення являє собою специфічний вид копіювання. Для перехоплення, як зазначає С. Дрьомов, характерним є те, що предмет злочину (інформація) циркулює в мережі, та пропонує під несанкціонованим перехопленням інформації розуміти дії, спрямовані на привласнення або затримування інформації під час її маршрутування в комп'ютерній мережі [87, с. 56]. Слід погодитися з позицією щодо особливості предмета перехоплення, однак запропоноване його визначення видається не зовсім вдалим. По-перше, затримування інформації під час її маршрутування є не чим іншим, як блокуванням, відповідальність за яке передбачено в ч. 1 ст. 362. По-друге, "привласнення" видається не зовсім вдалим терміном для опису наслідків перехоплення, яке, ще раз зазначимо, являє собою специфічний вид копіювання. Його особливість полягає в способі отримання копії. Відповідно до Конвенції про кіберзлочинність, прийнятої в рамках Ради Європи 23 листопада 2001 року (ратифікована Україною у вересні 2005 року), *несанкціонованим перехопленням* є навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, не призначених для публічного користування, які проводяться з комп'ютерної системи, усередині її або на неї, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані. Отже, несанкціоноване перехоплення: 1) вчиняється за допомогою специфічних технічних засобів; 2) полягає в отриманні копії інформації під час її передавання від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем чи комп'ютерних мереж; 3) вчиняє особа, яка не має права на отримання інформації з обмеженим доступом, що є його предметом. Таким чином, *несанкціоноване перехоплення* – це отримання, з перевищенням наданих власником прав, копії інформації з обмеженим доступом за допомогою специфічних технічних засобів під час передавання цієї інформації від од-

ного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем чи комп'ютерних мереж, у яких опрацьовується така інформація.

Наприклад, під час роботи електронно-обчислювальної машини сигнали, які формують зображення на дисплеї, можуть за допомогою спеціального обладнання отримуватися на певній відстані від працюючого комп'ютера. Тож особа шляхом перехоплення отримуватиме ту комп'ютерну інформацію, яка відображається на дисплеї.

Суб'єкт злочину, передбаченого ст. 362 КК, спеціальний – особа, яка має право доступу до комп'ютерної інформації. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації.

Суб'єктивна сторона цього злочину характеризується виною у формі прямого або непрямого умислу: особа усвідомлює суспільну небезпечність і протиправність своїх дій і бажає або свідомо допускає настання наслідків. При цьому особа має усвідомлювати, що вчиняє такі дії, які є перевищенням повноважень, наданих власником інформації. Слід погодитися з С. Дрьомовим, який до змісту інтелектуального моменту умислу при несанкціонованих діях з інформацією, яка обробляється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, відносить також усвідомлення властивостей спеціального суб'єкта, які є конститутивними ознаками цього складу злочину [90, 116].

Достатньо цікавий приклад злочину, що розглядається, описується у вироку Косівського районного суду Івано-Франківської області в справі № 1-56/2007 від 7 червня 2007 року [173] за обвинуваченням Б. у вчиненні злочинів, передбачених ст.ст. 364, 366 та 362 КК України. Так, Б. працював у філії енергетичної компанії на посаді бухгалтера з реалізації та був *особою, яка має доступ до програми, призначеної для комп'ютерної обробки інформації* щодо розрахунків з юридичними особами.

Приватне підприємство "Ф." згідно з договором на постачання сплатило за використану електроенергію 382671,45 грн. У цей час Б., зловживаючи своїм службовим становищем, діючи умисно, в інтересах третіх осіб, а саме приватних підприємців Т., Р., Л., В., Д., незаконно занизив показник спожитої електроенергії ПП "Ф." і фактично сплачених за неї коштів у сумі 76008,07 грн., які безпідставно в програмі розрахунків з юридичними споживачами розніс указаним приватним підприємцям, що споживали електроенергію, але не здійснювали оплати за неї. Унаслідок цих умисних дій енергетичній компанії заподіяно тяжкі наслідки – шкоду на суму 76008,07 грн.

Суд правильно кваліфікував дії Б., що виразились у зловживанні службовим становищем, тобто умисному, в інтересах третіх осіб використанні свого службового становища всупереч інтересам служби, що заподіяло тяжкі наслідки, як злочин, передбачений ч. 2 ст. 364 КК України. Крім цього, правильною є й оцінка дій підсудного за ст. 366 як службового підроблення та ст. 362 як *несанкціонованої зміни комп'ютерної інформації, вчиненої особою, яка має доступ до неї.* Зазначимо, що в цьому випадку вчинене Б. службове підроблення обов'язково потребувало додаткової кваліфікації за ст. 362, оскільки спосіб, у який вчинено службове підроблення, являє собою самостійний злочин (ст. 362), що не охоплюється диспозицією відповідної норми про злочин у сфері службової діяльності.

Кримінальна відповідальність за порушення правил експлуатації комп'ютерної техніки чи мереж електрозв'язку та за порушення порядку чи правил захисту інформації, яка в них обробляється. Кримінальну відповідальність за порушення правил експлуатації комп'ютерних засобів оброблення інформації та мереж електрозв'язку, а також порушення порядку чи правил захисту інформації встановлено в ст. 363 КК України "Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється".

Об'єкт злочину, передбаченого цією статтею, складають суспільні відносини, у межах яких забезпечується безпека використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Диспозиція цієї статті є бланкетною, тобто містить посилання на інші нормативно-правові акти. Але, на жаль, сьогодні не можна сказати, що законодавство про безпеку експлуатації комп'ютерної техніки, мереж електрозв'язку та захист комп'ютерної інформації достатньо розвинене. Саме тому воно не містить окремих нормативно-правових актів, які б чітко визначали правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, порядок і правила захисту комп'ютерної інформації.

Правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являють собою вимоги, які ставить власник ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Вони, як правило, містяться в окремих підзаконних актах (наказах, розпорядженнях), що видаються власником комп'ютерної техніки або мережі електрозв'язку. Наприклад, правила експлуатації засобів обчислювальної техніки в Міністерстві фінансів України регламентуються Наказом міністра фінансів України № 248 від 1 квітня 2003 року "Про затвердження Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України". Цей наказ забороняє користувачам розкривати корпуси засобів обчислювальної техніки, вносити зміни до конфігурації або самостійно їх ремонтувати; під'єднання засобу обчислювальної техніки користувача до телекомунікаційної мережі, установлення, оновлення та вилучення програмного забезпечення здійснюють відповідні спеціалісти й т.ін.

Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Регламентація цієї діяльності здійснюється за допомогою визначення порядку та правил захисту комп'ютерної інформації. Видається, що *порядок захисту інформації* – це визначені нормативно-правовими актами вимоги щодо створення системи захисту інформації та організації її роботи. *Правила захисту інформації*, у свою чергу, являють собою вимоги щодо використання системи захисту інформації певного інформаційного ресурсу. Тобто якщо систему захисту певного інформаційного ресурсу не створено, то й неможливо порушити правила захисту цього ресурсу. Той факт, що систему захисту не створено, може бути визнаний, за наявності відповідних нормативно-правових положень, порушенням порядку захисту інформації.

На певну увагу заслуговують питання нормативної регуляції захисту комп'ютерної інформації. Зазначимо, що вони вирішуються майже на всіх рівнях: прийнято відповідні закони, їх положення конкретизуються указами Президента, рішеннями Кабінету Міністрів, нормативними документами міністерств і відомств. Базовим нормативним документом у сфері захисту комп'ютерної інформації є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року. У цьому законі формулюється, можна сказати, головний принцип регулювання питань захисту комп'ютерної інформації національним законодавством: *відповідальність за захист інформації покладається на власника системи (у якій вона обробляється), при цьому в тих випадках коли в системі обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вона повинна оброблятися в системі з застосуванням комплексної системи захисту інформації з підтвердженою відповідністю*. Тобто спеціальні вимоги встановлюються лише до захисту державної інформації або інформації, захист якої спе-

ціально передбачено в законі. Решта нормативних актів у сфері інформаційної безпеки конкретизує це положення.

Так, правові та організаційні засади технічного захисту інформації органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України й інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій установлюються Указом Президента України "Про Положення про технічний захист інформації в Україні" від 27 вересня 1999 року. Також указом Президента створюється відповідний орган державного управління – Департамент спеціальних телекомунікаційних систем та захисту інформації, що діє в складі Служби безпеки України. Цей департамент "реалізовує державну політику у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, забезпечує функціонування державної системи урядового зв'язку" [354], саме цей департамент, до речі, проводить сертифікацію засобів технічного захисту інформації.

Постанови Кабінету Міністрів України встановлюють чіткі вимоги щодо інформаційної безпеки в органах державної влади. Так, відповідні постанови уряду як обов'язкову складову державних автоматизованих інформаційних систем передбачають систему захисту інформації [283; 278; 277; 279]; на органи державної влади покладається вимога щодо забезпечення захисту інформаційного наповнення їх веб-порталів [284]; спеціальні вимоги щодо інформаційної безпеки ставляться до програмного забезпечення, яке використовується державними органами [281], та до провайдерів, котрі надають послуги доступу до мережі Інтернет органам державної влади [282], тощо.

У свою чергу, нормативні документи міністерств і відомств закріплюють конкретні організаційні та інженерно-технічні заходи безпеки щодо їх інформаційних ресурсів. Наприклад, Інструкція Національного банку України про безготівкові розрахунки в Україні в національній валюті [285] передбачає такий організаційний захід: якщо під час використання

систем "клієнт – банк", "клієнт – Інтернет – банк" клієнт не дотримується вимог, що встановлює банк, з питань безпеки опрацювання електронних розрахункових документів, банк має право припинити обслуговування клієнта за допомогою системи. Мають місце й такі організаційні заходи, як установлення інструкцій щодо використання відомчих мереж [250; 248], періодичне створення комісій з перевірки дотримання вимог інформаційної безпеки [247; 246] й навіть обмеження доступу до приміщень, у яких розташоване обладнання, що забезпечує роботу мережі [249]. До технічних заходів, передбачених відомчими нормативними документами, можна віднести обов'язкове включення до відомчих комп'ютерних мереж засобів технікного захисту інформації [287; 288] та встановлення відповідних вимог до обладнання та програмного забезпечення [302].

Спеціальних вимог щодо захисту комп'ютерної інформації, яка не є власністю держави, крім положення Закону України "Про захист інформації в автоматизованих системах", що захист інформації покладається на власника системи, національне законодавство не встановлює. Тому порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, у яких обробляється недержавна інформація, стосовно якої законодавство не встановлює спеціальних вимог щодо забезпечення її захисту, а також порушення порядку чи правил захисту такої інформації, якщо воно заподіяло істотну шкоду, буде вважатися злочином, передбаченим ст. 363 КК України, лише тоді, коли власником інформації або власником засобу автоматизованого опрацювання інформації у формі наказу, розпорядження або іншого офіційного документа закріплено відповідні правила експлуатації, порядок і правила захисту інформації.

Склад злочину, передбаченого цією статтею, матеріальний, отже, його *об'єктивна сторона* характеризується такими ознаками:

1) діяння – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих сис-

тем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;

2) суспільно небезпечні наслідки – значна шкода;

3) причинний зв'язок між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дозволяє зробити висновок про те, що діяння може виявлятися в трьох альтернативних формах:

- порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

- порушення порядку захисту комп'ютерної інформації;

- порушення правил захисту комп'ютерної інформації.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що ставляться власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад злочину є матеріальним, він буде вважатися закінченим від моменту настання суспільно небезпечних наслідків – значної шкоди. За змістом закону під значною в цій нормі слід розуміти будь-яку шкоду, заподіяну

порушенням нормативів інформаційної безпеки. При цьому в тих випадках, коли вона полягає в заподіянні матеріальних збитків, значною слід уважати таку шкоду, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Суб'єкт злочину, передбаченого ст. 363 КК, спеціальний – особа, яка відповідає за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

Суб'єктивна сторона цього злочину характеризується тим, що діяння може бути вчинено як умисно, так і з необережності, а стосовно наслідків можлива тільки необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад злочину, передбачений статтею 363 КК України, відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, необхідно кваліфікувати як умисне пошкодження майна (ст. 194 КК), або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має доступ до неї (ст. 362 КК).

Кримінальна відповідальність за масове розповсюдження повідомлень електрозв'язку (аналіз складу злочину, передбаченого ст. 363-1 КК України). Об'єкт перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку злочину складають суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки та мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію.

Предметом цього злочину є повідомлення електрозв'язку – відомості, подані у вигляді, що дозволяє їх передавати за допомогою комп'ютерних мереж або мереж електрозв'язку.

Оскільки склад злочину, передбачений статтею 363-1 КК, є *матеріальним*, до ознак його об'єктивної сторони належать: 1) діяння – масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки – порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причинний зв'язок між діянням та наслідками.

Отже, діяння як ознака об'єктивної сторони цього складу злочину полягає в розповсюдженні повідомлень електрозв'язку, тобто надісланні певним адресатам копій цих повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Розповсюдження слід уважати *масовим* тоді, коли одне або кілька повідомлень отримує більше ніж один адресат, адже в диспозиції аналізованої статті йдеться про множинність повідомлень електрозв'язку та їх адресатів. Зазначимо, що поняття "масове" в цій нормі використовується як оцінне, тобто встановлення того, чи було певне розповсюдження повідомлень електрозв'язку масовим, залежить від аналізу багатьох обставин конкретного розповсюдження (кількість повідомлень або копій повідомлень, їх розмір; кількість адресатів; час, який було використано для розповсюдження; технічні характеристики обладнання, що використовувалося для розповсюдження, тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в якій формі (письмово, усно, шляхом використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, що є предметом злочину.

Порушення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являє собою таку зміну режиму робо-

ти комп'ютерної техніки або мережі електрозв'язку, яка створює загрозу для їх функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням.

Припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в тимчасовому або остаточному припиненні функціонування комп'ютерної техніки або мереж електрозв'язку, невиконанні ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку.

Суб'єкт цього злочину загальний.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків. Особа усвідомлює, що вчиняє масове розповсюдження повідомлень електрозв'язку, і бажає вчиняти такі дії, а також вона бажає або свідомо допускає порушення чи припинення роботи комп'ютерної техніки чи мереж електрозв'язку або легковажно розраховує на ненастання таких наслідків.

Як приклад злочину, передбаченого цією статтею, можна навести випадок, що трапився у 2004 році в м. Челябінську (РФ). Основні обставини його такі [292]. А. створив комп'ютерну програму для масового розсилання коротких текстових повідомлень (SMS-повідомлень) на сайт ЗАТ "Уральський Джи Ес Ем" і через нього на машинні носії абонентів, яке призводило до несанкціонованого блокування інформації та порушення роботи комп'ютерної мережі. Після цього, усвідомлюючи, що використання програми спричинить блокування інформації та порушення роботи комп'ютерної мережі, привів її в дію. У результаті 23 травня 2003 року, у період від 00 годин 29 хвилин до 02 години 46 хвилин, абоненти Челябінського фрагмента мережі "Мегафон" ЗАТ "Уральський Джи Ес Ем" кількістю 11261 особа отримали SMS-повідомлення нецензурного змісту, що мало наслідками: 1) порушення роботи комп'ютерної мережі

ЗАТ "Уральський Джи Ес Ем", тобто створення аварійної ситуації, що класифікується, відповідно до чинної Інструкції про порядок дій інженера групи оперативно-технічного управління в аварійних ситуаціях, як подія першої категорії "аварія" (подія, яка призводить до погіршення роботи мережі в цілому або її окремих дільниць у результаті перевантаження обладнання, викликаного пересиланням надто великого обсягу інформації, та тимчасового створення перешкод для її функціонування відповідно до призначення); 2) блокування комп'ютерної інформації, тобто позбавлення абонентів мережі "Мегафон" ЗАТ "Уральський Джи Ес Ем" можливості приймати та надсилати інші SMS-повідомлення в зазначений період. Такі дії А. повторив і 24 травня 2003 року. На підставі КК України їх можна було б кваліфікувати за сукупністю злочинів як: 1) створення з метою використання шкідливої комп'ютерної програми, призначеної для несанкціонованого втручання в роботу комп'ютерної мережі (ст. 361-1 КК); 2) несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до блокування комп'ютерної інформації (ст. 361 КК); 3) масове розповсюдження повідомлень електрозв'язку, що призвело до порушення роботи комп'ютерної мережі (ст. 363-1 КК).

Питання кримінально-правових засобів протидії незаконному масовому розсиланню повідомлень електрозв'язку буде більш ретельно розглядатися в наступній главі.

3.2. Розмежування злочинів у сфері використання інформаційних технологій та їх відмежування від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки

Правильна правова оцінка злочину потребує не тільки зіставлення фактичних обставин його вчинення з юридичними ознаками конкретного складу злочину, але й відмежування його від інших, суміжних за деякими ознаками, складів злочи-

нів [328, с. 80]. Визначення критеріїв розмежування комп'ютерних злочинів між собою та ознак, що дозволяють відмежувати ці суспільно небезпечні діяння від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки, глибше проаналізувати зміст ознак досліджуваних злочинів, сприятиме їх правильній кваліфікації.

Розмежування комп'ютерних злочинів. Склади злочинів, передбачені статтями 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та 362 (несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) КК України характеризуються однаковим безпосереднім об'єктом. Цей об'єкт складають суспільні відносини, у межах яких реалізується право власності на комп'ютерну інформацію, а також суспільні відносини, пов'язані з наданням та отриманням послуг електрозв'язку (ст.ст. 361 та 361-1 КК). Водночас ці склади злочинів розрізняються за ознаками предмета. Так, предметом злочину, передбаченого ст. 361 КК, є комп'ютерна інформація та інформація, що передається мережами електрозв'язку, а злочину, передбаченого ст. 362 КК, – тільки комп'ютерна інформація. До предмета злочину, передбаченого ст. 361-1 КК, відносяться шкідливі програмні та технічні засоби. Різною є й конструкція об'єктивної сторони: посягання, передбачені статтями 361 та 362 КК, відносяться до злочинів з матеріальним складом, а передбачені ч. 1 ст. 361-1 – до злочинів із формальним складом. Розмежовувати ці склади злочинів можна й за ознаками суб'єкта: у складах злочинів, передбачених статтями 361 та 361-1 КК, він загальний, тимчасом як суб'єкт злочину, передбаченого

ст. 362 КК, спеціальний – особа, що має доступ до комп'ютерної інформації.

Однак головною ознакою, що дозволяє відмежувати злочини, передбачені статтями 361 та 362 КК, від злочину, передбаченого ст. 361-1, є, як видається, механізм заподіяння шкоди об'єктові – суспільним відносинам права власності на комп'ютерну інформацію: якщо статті 361 та 362 КК передбачають відповідальність за певні дії, що призводять до заподіяння шкоди предмету цих відносин, чим урешті-решт і заподіюється шкода об'єкту, то стаття 361-1 КК передбачає відповідальність за дії, що створюють небезпеку заподіяння шкоди цим суспільним відносинам. У зв'язку з цим зазначимо, що використання під час вчинення передбаченого ст. 361 або 362 КК злочину шкідливого програмного або технічного засобу, створеного суб'єктом раніше, потребує додаткової кваліфікації за ст. 361-1 КК як створення шкідливого програмного або технічного засобу з метою його використання.

Злочини, передбачені ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) та ч. 2 ст. 362 КК України, являють собою посягання на суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом і характеризуються тим, що їх предметом може бути тільки така комп'ютерна інформація. Між собою вони розрізняються за конструкцією об'єктивної сторони: перший відноситься до злочинів із формальним складом, другий – з матеріальним. Різним є й зміст дій суб'єкта. Злочин, передбачений ст. 361-2 КК, полягає в збуті або розповсюдженні комп'ютерної інформації, а ч. 2 ст. 362 КК передбачено відповідальність за перехоплення або копіювання такої інформації.

Злочин, передбачений ст. 363 КК (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них

оброблюється), відрізняється від інших посягань, передбачених розділом XVI КК України, майже всіма ознаками складу. Безпосереднім об'єктом більшості складів "комп'ютерних" злочинів є право власності на комп'ютерну інформацію, а злочин, передбачений ст. 363 КК, завдає шкоди відносинам щодо забезпечення встановленого порядку експлуатації комп'ютерної техніки, мереж електрозв'язку, а також порядку та правил захисту інформації. Диспозиція ст. 363 КК є єдиною бланкетною диспозицією в згаданому розділі, тобто тільки в цьому складі злочину діяння полягає в порушенні правил експлуатації комп'ютерної техніки, мереж електрозв'язку або порядку чи правил захисту інформації, передбачених певними нормативно-правовими актами. Спеціальним є й суб'єкт злочину цього злочину – особа, що відповідає за експлуатацію комп'ютерної техніки або мережі електрозв'язку. Суб'єктивна сторона характеризується змішаною формою вини: стосовно порушення правил (діяння) є можливим як умисел, так і необережність, а щодо настання істотної шкоди (наслідків) – тільки необережність. Якщо ж особа умисно порушує правила експлуатації комп'ютерної техніки або порядок чи правила захисту інформації й до настання зазначених наслідків вона ставиться також свідомо, ознаки складу злочину, передбаченого ст. 363 КК, відсутні. Залежно від обставин справи такі дії можна кваліфікувати як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має право доступу до неї (ст. 362 КК), або пособництво в несанкціонованому втручанні в роботу комп'ютерної техніки чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК).

Специфіка складу злочину, передбаченого ст. 363-1 КК (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку), полягає перш за все в ознаках об'єкта. Ця норма, як ми зазначали, захищає суспільні відносини щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності, тимчасом як більшість інших норм аналізованого розділу (усі, крім ст. 363 КК)

забезпечують кримінально-правову охорону відносинам власності на комп'ютерну інформацію, тобто певному виду інформаційної діяльності. Тому, якщо масове розсилання повідомлень електрозв'язку призводить, наприклад, до блокування комп'ютерної інформації, а функціонування засобів автоматизованого опрацювання інформації не порушено, ознаки складу злочину, передбаченого ст. 363-1 КК, відсутні. Такі дії можна, за наявності відповідних ознак, кваліфікувати як несанкціоноване втручання (ст. 361 КК), адже шкоду в такій ситуації заподіяно тільки відносинам власності на комп'ютерну інформацію. Водночас, якщо особа здійснила, наприклад, масове розповсюдження комп'ютерної інформації з обмеженим доступом, що внаслідок надмірного перевантаження призвело до порушення роботи комп'ютерної мережі, має місце ідеальна сукупність злочинів, передбачених статтями 361-2 та 363-1 КК. У цій ситуації шкода заподіюється і відносинам власності на комп'ютерну інформацію з обмеженим доступом, і відносинам щодо забезпечення безвідмовного функціонування технічних засобів інформаційної діяльності.

Відмежування злочинів у сфері використання інформаційних технологій від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки.

Останнім часом кількість повідомлень про вчинення злочинів проти власності з використанням комп'ютерної техніки значно збільшилася. Це є природним наслідком процесів інформатизації та комп'ютеризації. Дослідження національної судової практики (докладніше про дослідження в підглаві 4.3 та додатку 5) дозволяє зазначити, що за особливостями кримінально-правової оцінки випадки застосування комп'ютерної техніки для здійснення злочинів проти власності можуть бути поділені на дві групи: 1) використання комп'ютерної техніки як засобу вчинення злочину проти власності; 2) вчинення злочину у сфері використання комп'ютерної техніки (ст.ст. 361 – 363-1 КК) з метою подальшого вчинення злочину проти власності або приховування його слідів.

Посягання, які слід відносити *до першої групи*, полягають, як правило, у тому, що певна інформаційна система використовується злочинцем для незаконного заволодіння чужою власністю, при цьому ознаки комп'ютерного злочину відсутні. Винний не здійснює незаконного перекручення або знищення комп'ютерної інформації, не заподіює іншої шкоди функціонуванню комп'ютерних засобів, можна сказати, використовує їх у штатному режимі. Механізм учинення таких злочинів, як правило, полягає в тому, що злочинець через електронну систему переказу платежів, яка використовується тією чи іншою фінансовою установою, здійснює незаконний переказ коштів. Наприклад, у вересні 1997 року в Луганському відділенні АКБ "Укркомунбанк" бухгалтер операційного відділу використала комп'ютерну систему банку для викрадення 300 тис. гривень. Отримавши меморіальний ордер, вона ввела в систему реквізити не одержувача за цим ордером, а іншої організації, однак довести свій умисел до кінця не змогла, оскільки спрацювала система захисту. За цим фактом Ленінським РВ ЛМУ УМВС України в Луганській області було порушено кримінальну справу: дії бухгалтера правильно кваліфіковано як замах на розкрадання колективного майна в особливо великих розмірах. Ознаки комп'ютерного злочину в таких діях відсутні, оскільки винний, віддаючи команду комп'ютерній системі переказу платежів, не перекручує і не знищує комп'ютерну інформацію, яка зберігається в ній, і не завдає шкоди безпеці використання комп'ютерної техніки. КК містить спеціальну норму для кваліфікації таких дій. Частина 3 статті 190 передбачає кримінальну відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. Необхідно відзначити, що ця норма викликає багато зауважень у науковців і практиків. Насамперед вони стосуються того, що шахрайство являє злочин, пов'язаний з обманом, тобто повідомленням неправдивих відомостей людині, або зловживанням довірою людини, а отже, "не можна обманути комп'ютер або зловжити його довірою" [236, с. 56 – 57; 334, с. 86]. Однак при вчиненні такого шахрайства обманюється ніяк не комп'ютер, а людина, яка використовує комп'ютер для інтенсифікації діяльності, наприклад, щодо банківських розрахунків. Має місце, можна сказати, опосередкований обман, тобто певні неправдиві відомості повідомляються не безпосередньо людині, а опосередковано, через комп'ютер. Заслуговує на увагу аргументація С.А. Петрова, який критикує положення щодо неможливості застосування норм про відповідальність за шахрайство у випадках, коли воно поєднане з використанням комп'ютерної техніки, введенням недостовірної інформації або її зміною. "Змінюючи комп'ютерну інформацію, винна особа змінює дійсність, що існує, але особа, що створила або експлуатує комп'ютерну програму, про це не знає, у результаті чого дійсність не відповідає уявленням цієї особи про неї … можна говорити про обман" [265]. Тому вказана норма "має право на існування", і, ураховуючи, що використання комп'ютерної техніки значно підвищує ступінь суспільної небезпечності шахрайства, її використання видається доцільним. Разом із цим, слід погодитися з пропозицією А.В. Савченка про доцільність уточнення відповідної кваліфікуючої ознаки шахрайства таким чином: вчинене "шляхом незаконних операцій з використанням електронно-обчислювальної техніки, шкідливих програмних чи технічних засобів" [309, с. 121].

Типовим прикладом застосування ч. 3 ст. 190 для кваліфікації дій, які полягали у використанні комп'ютерної техніки для вчинення шахрайства, за відсутності ознак злочину у сфері використання інформаційних технологій, є вирок Соснівського районного суду м. Черкаси в справі № 1-569/09 від 11 грудня 2009 року [174]. Засуджений А., з метою заволодіння грошовими коштами шляхом обману користувачів мережі Інтернет, зареєструвався на інтернет-ресурсі "Aukro.ua" – цей сайт є інтернет-аукціоном з продажу та купівлі різноманітних товарів – і пропонував до продажу телефони, камери й інші електронні товари. Усі товари виставлялися на лотах за заниженими цінами з метою привабити якомога більше клієнтів. Після того як покупець вигравав аукціон, йому з "Aukro.ua"

надходило повідомлення про це, а також указувалися контактний телефон, e-mail та адреса продавця. Коли покупець зв'язувався з А., то останній повідомляв, що він дійсно продає товар, який виставлений на інтернет-аукціоні "Aukro.ua", пропонував перерахувати вартість товару на один із його "web-гаманців" платіжної системи "WebMoney", а після перерахування коштів товар мав бути надісланий покупцеві. Але після перерахування коштів покупець свого товару так і не отримував. Надалі А. відкрив платіжну картку "Миттєва" ЧФ ВАТ КБ "ПриватБанк", на яку переводив гроші, отримані шахрайським шляхом.

Слід зазначити, що на сьогодні ще одним із видів шахрайства, яке вчиняється з використанням електронно-обчислювальної техніки, є так званий фішинг. Він полягає в тому, що зловмисники масово надсилають електронні листи, у яких від імені якогось відомого банку, інтернет-магазину, фінансової компанії чи під іншим приводом, наприклад виграшу в лотереї, пропонують адресатам повідомити реквізити своєї пластикової картки, а потім використовують ці реквізити для заволодіння грошима адресатів.

Більш поширеними є випадки, віднесені нами до *другої групи*. Особливість кримінально-правової оцінки полягає тут у тому, що дії винної особи необхідно кваліфікувати не тільки як злочин проти власності, але і як "комп'ютерний" злочин. Як приклад можна навести такий випадок. З вересня до грудня 1999 року в Донецьку (досудове слідство провадилося прокуратурою Донецької області) головний інженер-програміст Центру інформаційних технологій і технічного забезпечення Донецької дирекції Українського державного підприємства електрозв'язку "Укртелеком" розробив комп'ютерну програму, яка дозволяє відшукувати в масиві фіксованої структури телефонні розмови, проведені з заданих номерів телефонів, відбирати їх і стирати інформацію про них у цьому масиві. Винний увійшов у змову з громадянином Пакистану, який навчався в Донецьку та залучав клієнтів. Спільно вони надавали їм за заниженими тарифами послуги міжнародного та міжміського

телефонного зв'язку, а інформацію про переговори, що здійснювалися клієнтами, знищували за допомогою програми, розробленої інженером-програмістом. Унаслідок таких дій підприємству електрозв'язку був заподіяно збитки в розмірі близько 150 тисяч гривень. Кваліфікувати дії головного інженера, якби вони були вчинені після набрання чинності змін до КК України, що передбачили нову редакцію розділу XVI КК, необхідно було б за сукупністю злочинів, передбачених ст. 192 КК (заподіяння значної матеріальної шкоди шляхом обману без ознак шахрайства), ст. 361 КК (несанкціоноване втручання в роботу автоматизованої системи обчислення плати за надання послуг міжміського та міжнародного зв'язку, яке спричинило підроблення комп'ютерної інформації) та ст. 361-1 КК (створення з метою використання шкідливої програми, призначеної для несанкціонованого втручання в роботу автоматизованої системи).

Схожий випадок стався влітку 2002 року в Херсоні. Студент одного з вищих навчальних закладів міста вчинив несанкціоноване втручання в роботу комп'ютерної мережі місцевого провайдера інтернет-послуг і перекрутив комп'ютерну інформацію про рахунки клієнтів та сплачений час роботи в мережі Інтернет (створив фіктивний рахунок). Після цього протягом кількох місяців безкоштовно користувався Інтернетом, чим заподіяв матеріальну шкоду провайдерові в розмірі 11000 грн. [314] За чинним КК подібні дії необхідно кваліфікувати як сукупність злочинів, передбачених статтями 192 і 361 КК.

Подібні випадки у світовій практиці одержали назву "крадіжка машинного часу". Такого роду злочини полягають у тому, що особа неправомірно використовує дороге комп'ютерне устаткування (наприклад суперкомп'ютери) або ресурси комп'ютерних мереж, *абонентом яких вона не є*. Найбільш поширеним видом подібних посягань у вітчизняній практиці є отримання доступу до мережі Інтернет за рахунок законних абонентів шляхом використання їх логінів і паролів. Видається, що правильною кваліфікацією подібних дій є оцінка їх як сукупності

злочинів, передбачених ст.ст. 192 та 361 КК України. Схожа тенденція спостерігається і в російський правозастосовчій практиці. Її дослідження, яке здійснив А.М. Копирюлін, дозволяє зробити висновок, що дії особи, яка неправомірно працює в мережі Інтернет під незаконно отриманими реквізитами, утворюють сукупність злочинів у сфері комп'ютерної інформації та злочинів проти власності, передбачених ст.ст. 272 та 165 КК РФ (ст.ст. 361 та 192 КК України) [139, с. 6]. Однак відповідальність за злочин, передбачений ст. 192 КК України, настає лише у випадку заподіяння матеріальної шкоди, що перевищує 50 неоподатковуваних мінімумів доходів громадян. Оскільки шкода, що заподіюється внаслідок більшості крадіжок машинного часу, значно менша, подібні дії отримують правову оцінку як блокування комп'ютерної інформації законних користувачів у той час, коли за їх рахунок та під їхніми іменами порушники отримували доступ до інформації (ст. 361), а також якщо отримання чужих логінів і паролів здійснювалося шляхом несанкціонованого втручання або особою, яка має доступ до комп'ютерної інформації, відповідно як несанкціоноване втручання, що призвело до витоку комп'ютерної інформації (ст. 361), або як злочин, передбачений ст. 362 КК. Так, у вироку Голованівського районного суду Кіровоградської області в справі № 1-156/08 від 16 вересня 2008 року [156] за обвинуваченням Р. у вчиненні злочину, передбаченого ч.1 ст. 361 КК України, зазначається таке. Р., перебуваючи в Голованівському відділенні Гайворонської МДПІ в кабінеті своєї дружини Р-вої при здійсненні нею процедури під'єднання до мережі Інтернет, діючи умисно, незаконно дізнався про інформацію з обмеженим доступом – логін і пароль доступу до мережі Інтернет указаного відділення Гайворонської МДПІ. Після цього протягом п'яти місяців, діючи умисно, незаконно використовуючи логін і пароль доступу до мережі Інтернет Голованівського відділення Гайворонської МДПІ, з власного комп'ютера неодноразово здійснював несанкціоноване втручання в роботу комп'ютерної мережі Інтернет, що призвело до блокування

інформації Голованівського відділення Гайворонської МДПІ стосовно звітності платників податків.

У висновку експерта зазначалося, що логін і пароль користувача жорстко пов'язані між собою, тобто з допомогою вищевказаного логіну користувач не може підключитися до Інтернету з використанням будь-яких інших паролів. Одночасна робота двох користувачів з однаковими логінами та паролями неможлива. Таким чином, *при виході до Інтернету будь-якої сторонньої особи доступ власникові логіну блокується*.

Коментуючи цей вирок, зазначимо також, що Р. здійснив більше 15 підключень із використанням указаних логіну та пароля, однак суд дав їм правильну оцінку як одиничному продовжуваному злочину, оскільки всі ці факти несанкціонованого втручання охоплювалися єдиним умислом і, отже, не утворювали повторності злочинів.

На окрему увагу заслуговує й те, що можливою є і кваліфікація дій винного за сукупністю злочинів, передбачених ч. 3 ст. 190 та ст.ст. 361 або 362 КК. Як приклад такого випадку, розглянемо вирок Корольовського районного суду м. Житомира в справі № 1-81/2007 від 5 січня 2007 року [181] за обвинуваченням Ц. та Ч. Серед злочинів, які їм інкримінувалися, були посягання, передбачені ч. 2 ст. 361 та ч. 3, ст. 190 КК України. Так, Ц. за попередньою змовою із Ч., з метою заволодіння чужим майном шляхом обману з використанням електронно-обчислювальної техніки та підключення до мережі Інтернет, у приміщенні Пункту колективного користування послугами Інтернет, шляхом підбору випадкових цифр логінів, паролів і трансферів, видавши себе за законного користувача, вчинив несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж для доступу до програмного комплексу віддаленого обслуговування клієнтів сайту, належного закритому акціонерному товариству комерційний банк (ЗАТ КБ) "ПриватБанк". Унаслідок несанкціонованого втручання зазнала витоку та блокування (зловмисники змінили реквізити доступу до облікового запису клієнта банку) конфіденційна інформація

про користувачів автоматизованої системи та інформація про банківський рахунок клієнта банку гр-на Т.

Отримавши доступ до конфіденційного рахунку за кредитною карткою клієнта банку Т., Ц. за попередньою змовою із Ч., продовжуючи свої злочинні дії, за рахунок кредитних коштів ЗАТ КБ "ПриватБанк" через мережу Інтернет вчинили шість фінансових операцій із придбання шести електронних ваучерів Закритого акціонерного товариства (ЗАТ) "Київстар GSM" на поповнення рахунку мобільного телефону на загальну суму 1525 грн. Отримавши з автоматизованої системи текстове повідомлення про авторизацію проведених операцій із зазначенням ідентифікаційного коду придбаних ваучерів, Ц. та Ч. шляхом уведення коду ваучерів у свій мобільний телефон з абонентською скретч-карткою для мобільного зв'язку вчинили фінансову операцію та поповнили рахунок своєї скретч-картки на загальну суму 1525 грн., тобто заволоділи чужим майном шляхом обману.

Таким чином, підсудні, використовуючи комп'ютерну техніку, *незаконно, без відповідного санкціонування, втрутились у діяльність комп'ютерної мережі* (серверу "Приват 24") та *отримали відповідну інформацію щодо кількості грошей на рахунках клієнтів банку (витік інформації)*, шляхом застосування нових паролів *блокували* доступ до інформації про стан відповідних рахунків (ст. 361 КК), після чого *шахрайськими діями заволоділи чужим майном – грошима* клієнтів ЗАТ КБ "Приват-Банк (ст. 190 КК).

Наведений і подібні випадки вимагають критично оцінити положення п. 19 Постанови Пленуму Верховного Суду України від 06.11.2009 р. № 10 "Про судову практику у справах про злочини проти власності" [286]. У постанові зазначається, що шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за частиною 3 статті 190 КК і додаткової кваліфікації не потребує. Це положення є справедливим тільки тоді, коли використання електронно-обчислювальної техніки не являло собою самостійного злочину у сфері використання комп'ютерної техніки (ст.ст. 361, 361-1, 362). Типовим прикладом такого

випадку є наведений раніше вирок, пов'язаний із засудженням особи за шахрайські дії, вчинені з використанням інформаційної системи інтернет-аукціону Aukro.ua. А якщо шахрайство або інший злочин проти власності пов'язані, наприклад, із незаконним втручанням у роботу комп'ютерної техніки (ст. 361), то необхідною є додаткова кваліфікація.

Разом із цим, зауважимо, що використання комп'ютерної техніки при незаконному заволодінні майном не завжди охоплюється складом ч. 3 ст. 190 КК. Наприклад, достатньо відомим є спосіб незаконного заволодіння чужим майном з використанням засобів автоматизованого опрацювання інформації, який отримав назву "метод салямі". Подібний спосіб використовується в банківських установах і полягає в такій зміні програмного забезпечення фінансового закладу, яка призводить до несанкціонованого перерахування на певний рахунок дуже невеликої кількості грошей при кожній трансакції, пов'язаній з перерахуванням великих сум і значними залишками на відповідних рахунках. Таким чином, на рахунку, який контролюється зловмисником, через деякий час, залежно від кількості операцій на значні суми, накопичується певна сума, яка в подальшому незаконно привласнюється. Подібні випадки, з позицій відповідальності за злочини проти власності, неправильно кваліфікувати як шахрайство, оскільки наявними є ознаки саме таємного заволодіння чужим майном – крадіжки. Зловмисник бажає якнайдовше залишатися непоміченим, саме тому гроші "знімаються" при операціях на великі суми та з рахунків з великими залишками. Тому в подібній ситуації правильною буде кваліфікація вчиненого як крадіжки та несанкціонованого втручання, що призвело до спотворення процесу обробки інформації.

Таким чином, особливістю кримінально-правової кваліфікації злочинів проти власності, які вчиняються з використанням комп'ютерної техніки, слід визнати необхідність розв'язання питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Відповідаю-

чи на це питання, слід керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформації, коли певна інформація була незаконно знищена, блокова, модифікована тощо. А в тих випадках, коли певні інформаційні системи використовуються за призначенням (наведений приклад з інтернет-аукціоном), додаткова кваліфікація не потрібна.

За змістом таких наслідків, як *втрата й знищення комп'ютерної інформації*, склади злочинів, передбачені статтями 361 та 362 КК, подібні до такого злочину проти власності, як *умисне знищення або пошкодження майна*: діяння в цих складах виражається в активній поведінці, яка спричиняє повну або часткову непридатність предмета злочину для використання за цільовим призначенням. Наслідки в цих складах також подібні. І в першому, і в другому власник предмета або істотно обмежується у своїх правах, або цілком втрачає можливість реалізувати своє право власності на предмет.

Тому основні відмінності цих складів слід шукати в ознаках об'єкта й предмета посягань. Відповідно до закону безпосереднім об'єктом умисного знищення або пошкодження майна (ст. 194 КК) є право власності на річ. Безпосереднім же об'єктом згаданих комп'ютерних злочинів є право власності на інформацію. Відмінність розгляданих суспільних відносин полягає в тому, що перші – це форма реалізації соціального інтересу щодо володіння, користування та розпоряджання *майном*, а другі – щодо *інформації*. Відмінність між інформацією і річчю полягає насамперед у їх фізичній властивості. Майно є об'єктом матеріального світу. Що ж стосується інформації, то вона, як зазначалося раніше, не може бути віднесена ні до матеріальних, ні до нематеріальних об'єктів: фізична властивість інформації полягає в наявності матеріального носія, але йому вона не тотожна.

Відмінність ознак об'єкта й предмета зумовлює різний зміст ознак об'єктивної сторони комп'ютерних злочинів, пов'язаних

зі знищенням інформації, та умисного знищення або пошкодження майна. Знищення або пошкодження майна полягає в порушенні, як правило, його фізичної цілісності, а знищення або перекручення комп'ютерної інформації не завжди супроводжується порушенням цілісності її носія. Однак якщо дії особи являють собою порушення фізичної цілісності комп'ютерної техніки (ознака об'єктивної сторони злочину проти власності), але мета, яку ставить суб'єкт, полягає в заподіянні шкоди відносинам власності на інформацію, то дії цієї особи слід кваліфікувати як знищення комп'ютерної інформації, оскільки знищення або пошкодження комп'ютерної техніки в цьому випадку є способом вчинення комп'ютерного злочину. Кваліфікувати подібні дії необхідно як сукупність злочинів, передбачених ст. 361 або ст. 362 КК, і, за наявності відповідних ознак, ст. 194 КК (умисне знищення або пошкодження майна).

Відмежування злочинів, передбачених ст.ст. 361 та 362 КК, *від несанкціонованого втручання у роботу Державного реєстру виборців (чч. 11, 12 ст. 158 КК) та незаконного втручання в роботу автоматизованої системи документообігу суду (ст. 376-1 КК)* слід проводити за правилами розв'язання конкуренції загальних і спеціальних норм. Стаття 376-1 та чч. 11, 12 ст. 158 КК являють собою види спеціальних заборон, загальними для них виступають ст.ст. 361 та 362 КК. Тому у випадках втручання в роботу названих спеціалізованих автоматизованих систем відповідальність настає тільки за статтею 158 або 376-1 КК.

На окрему увагу заслуговує питання *відмежування комп'ютерних злочинів від злочинів, що полягають у збиранні інформації з обмеженим доступом* (статті 111, 114, 231 та 330 КК України). Ці злочини, якщо їх предметом є відомості, що складають певну таємницю та являють собою комп'ютерну інформацію, збігаються за ознаками об'єктивної сторони з несанкціонованим втручанням, що призвело до витоку інформації (ст. 361), або з несанкціонованим перехопленням чи копіюванням, якщо воно призвело до витоку інформації (ч. 2 ст. 362).Такі ситуації слід відносити до конкуренції цілого та частини, яка має місце в тих випадках, коли вчинений злочин передбачений кількома

статтями Особливої частини кримінального закону, з яких одна охоплює все посягання, а інші — його частину [241, с. 430]. Як методологічну базу розв'язання таких випадків слід використовувати правила, які чітко сформулював В.О. Навроцький: 1) повинна застосовуватися стаття Особливої частини КК, яка найбільш повно охоплює всі ознаки вчиненого посягання (що охоплює посягання в цілому); 2) при цьому статті, які передбачають лише частину вчиненого посягання, не інкримінуються, якщо існує стаття, яка охоплює все посягання [241, с. 430 – 431]. Так, обов'язковою ознакою суб'єктивної сторони зазначених некомп'ютерних злочинів є мета – використання інформації, що є предметом посягання. Тому дії особи, яка використовує, наприклад, інформаційну систему Міністерства оборони України для отримання таємних даних з метою їх подальшого передавання іноземній державі, слід кваліфікувати тільки за ст. 111 або 114 КК. У разі відсутності такої мети вчинене, за наявності відповідних ознак, необхідно кваліфікувати як злочин, передбачений ст. 361 або ст. 362 КК України. Слід зазначити, що в практиці зарубіжних правоохоронних органів траплялися випадки посягання на закриту комп'ютерну інформацію без мети її використання. Наприклад, у лютому 1998 року громадянин Ізраїлю Ехуд Тенебаум здійснив незаконне втручання в роботу комп'ютерів Міністерства оборони США, де зберігалася закрита інформація. У процесі розслідування було встановлено, що мотив і мета зловмисника не дозволяють кваліфікувати його дії як шпигунство [407]. Якби ці події відбувалися на території України, то дії ізраїльського громадянина треба було б кваліфікувати як несанкціоноване втручання в роботу електронно-обчислювальних машин, яке призвело до витоку комп'ютерної інформації (ст. 361 КК). Зазначимо, що можлива й інша ситуація: особа з використанням комп'ютерної техніки вчиняє злочин, передбачений однією з розгляданих статей (111, 114, 231, 330), але крім цього заподіює певну шкоду відносинам власності на комп'ютерну інформацію, яка знаходиться за межами складів названих посягань (наприклад блокування інформації шляхом зміни паролів,

знищення інформації з метою приховання слідів тощо). У таких випадках дії винної особи додатково кваліфікуються за ст.ст. 361 або 362 КК.

Досить важливою проблемою є й *відмежування злочинів, пов'язаних із розголошенням або передаванням відомостей з обмеженим доступом (статті 111, 114, 132, 145, 168, 182, 232, 328, 330, 381, 387, 422), від несанкціонованого збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК). У* цих випадках слід також дотримуватися правил розв'язання конкуренції цілого та частини. Конкретизація відповідних складів тут головним чином залежить від ознак, що характеризують *суб'єкта* або *особу, якій передаються відомості*.

Так, відмежування злочинів, передбачених статтями 111, 114 та 330 КК (якщо відомості, що складають їх предмет, являють собою комп'ютерну інформацію), від несанкціонованого збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2 КК) слід проводити на підставі аналізу *ознак, що характеризують особу, якій передається комп'ютерна інформація.* Наприклад, якщо комп'ютерна інформація, що становить державну таємницю, передається представникові іноземної організації, наявним є склад злочину, передбачений ст. 111 або ст. 114 КК. Однак якщо така інформація передається іншій особі, дії (за відсутності ознак складу злочину, передбаченого ст. 328 КК) необхідно кваліфікувати за ст. 361-2 КК.

Злочини, передбачені статтями 132, 145, 232, 328, 330, 381, 387 та 422 КК (якщо їх предметом є відповідна комп'ютерна інформація), необхідно відмежовувати від несанкціонованого збуту або розповсюдження комп'ютерної інформації (ст. 361-2 КК) за ознаками суб'єкта. Усі перелічені некомп'ютерні злочини характеризуються наявністю спеціального суб'єкта, тому розповсюдження або збут комп'ютерної інформації, що є предметом цих злочинів, загальним суб'єктом необхідно кваліфікувати за ст. 361-2 КК. Крім того, обов'язковою ознакою об'єктивної сторони незаконного розголошення лікарської таємниці (ст. 145 КК) є настання тяжких наслідків, а обов'язковою ознакою об'єктивної сторони розголошення комерційної або

банківської таємниці (ст. 232) – настання істотної шкоди, тому розповсюдження комп'ютерної інформації, яка містить лікарську, банківську або комерційну таємницю, що не призвело до названих наслідків, слід кваліфікувати за ст. 361-2 КК.

Відмежування складу злочину, передбаченого ст. 361-2 КК, від розголошення таємниці усиновлення (удочеріння) (ст. 168 КК) та поширення конфіденційної інформації про особу (ст. 182 КК) здійснюється насамперед на підставі ознак об'єкта та суб'єктивної сторони. Несанкціоновані розповсюдження або збут комп'ютерної інформації відносяться до злочинів проти власності на неї, тимчасом як розголошення таємниці усиновлення та поширення конфіденційної інформації про особу відносять до злочинів проти відповідних конституційних прав людини й громадянина. Отже, якщо особа усвідомлює, що вона, наприклад, розповсюджує конфіденційну інформацію про конкретну особу або конкретну, персонально визначену групу осіб без їх згоди, має місце злочин проти конституційних прав та свобод – порушення недоторканності приватного життя (ст. 182). Але якщо особа не усвідомлює, чиї саме персональні дані вона розповсюджує, наприклад розміщує на інтернет-сайті електронну базу паспортних даних осіб, що прописані в певному місці, яка належить міському відділу внутрішніх справ, має місце злочин проти права власності на комп'ютерну інформацію з обмеженим доступом (у цьому випадку проти державної власності на комп'ютерну інформацію), тобто злочин, передбачений ст. 361-2 КК України.

Несанкціоновані дії, що призвели до витоку комп'ютерної інформації (ст. 361 та ч. 2 ст. 362 КК), слід відмежовувати й *від порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються через комп'ютер* (ст. 163 КК України). Незаконне отримання кореспонденції, що передається з використанням засобів електронної пошти, не відноситься до комп'ютерних злочинів, а являє собою злочин проти особистих прав і свобод людини. Від комп'ютерних злочинів цей склад відрізняється за предметом: предмет комп'ютерних злочинів – комп'ютерна інформація; предмет злочину, передбаченого ст. 163 КК України, – специфічний вид інформації, а саме кореспонденція; а також за об'єктом посягання: право власності на комп'ютерну інформацію та недоторканність приватного життя. Зазначимо, що йдеться лише про приватну кореспонденцію, тобто про листування між фізичними особами або між фізичною та юридичною особою. Ознайомлення зі змістом листування між юридичними особами слід кваліфікувати, за наявності мети розголошення або іншого використання отриманих відомостей, як умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю (ст. 231), або, за відсутності такої мети й залежно від ознак суб'єкта, як злочин, передбачений ст. 361 або 362 КК.

Значний інтерес у контексті питання відмежування комп'ютерних злочинів від порушення таємниці кореспонденції становить вирок Першотравневого районного суду м. Чернівці в справі № 1-235/2008 від 29 серпня 2008 року [164] за обвинуваченням Л. у вчиненні злочинів, передбачених ч. 2 ст. 361-1, ч. 2 ст. 361 та ч. 1 ст. 163 КК України. Так, Л. установив, що існує категорія шкідливих програмних засобів, які можна створювати шляхом спеціального налаштування вже створених програм. Однією з таких програм є Ardamax keyloger 2.9. Ця програма є трояном-кейлогером, яка здійснює електронне шпигунство за користувачем "зараженого" комп'ютера: інформація, що вводиться з клавіатури, знімки екрана, список активних програм і дії користувача з ними зберігаються у файл на диску та періодично відправляються зловмисникові. У мережі Інтернет він відшукав дистрибутив цієї програми й завантажив собі в комп'ютер. Ознайомившись детально з принципом її дії, він налаштував цю програму таким чином, щоб уся інформацію, яку вона збирала в чужих комп'ютерах, надсилалася на його електронну поштову скриньку. Усвідомлюючи, що створена ним комп'ютерна програма є шкідливою програмою (Trojan-Spy.Win32.Ardamax.n), призначеною для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), Л. вирішив розповсюдити її серед необмеженої кількості користувачів локальної мережі одного з провайдерів послуг

мережі Інтернет. Так, за допомогою власного комп'ютера і стандартного програмного забезпечення він навмисно розмістив цю шкідливу комп'ютерну програму на сервері локальної комп'ютерної мережі під назвою Winamp_6.0_New_Edition.exe. Знаючи, що Winamp.exe – назва популярного програвача комп'ютерної музики та фільмів, він тим самим намагався приховати від користувачів справжнє призначення цієї шкідливої програми й таким чином змусити активізувати її. Ю., один з абонентів локальної мережі, завантажила цю програму та, помиляючись щодо її дійсного призначення, активізувала її. Після зараження комп'ютера Ю. троянська програма Trojan-Spy.Win32.Ardamax.n стала в автоматичному режимі вести електронний журнал натискання користувача на клавіатуру та робити знімки з робочого столу (монітора), після чого зібрану інформацію періодично відправляла на електронну скриньку Л. Урешті-решт він незаконно ознайомився з реквізитами авторизації Ю. у комп'ютерній мережі та на сервері електронної пошти, а також зі змістом її листування з друзями та знайомими, яке здійснювалося за допомогою електронної служби миттєвих текстових повідомлень.

У результаті своїх злочинних дій Л. *створив і розповсюдив шкідливий програмний засіб* і *несанкціоновано втрутився в роботу електронно-обчислювальної машини* (комп'ютера) Ю., *що призвело до витоку інформації*, а також *порушив таємницю кореспонденції*, що передається через комп'ютер.

У цьому випадку суд правильно оцінив той факт, що серед відомостей, отриманих унаслідок несанкціонованого втручання в роботу комп'ютера Ю, є такі, які становлять таємницю кореспонденції, що передається через комп'ютер, а отже, вчинене потребує додаткової кваліфікації за ст. 163 КК. Крім цього, звернемо увагу ще й на те, що Л., як зазначено у вироку (для прикладу ми навели лише частину цього документа), здійснив подібні дії, тобто розповсюдження троянської програми та несанкціоноване отримання внаслідок її роботи на комп'ютерах потерпілих відповідних відомостей, стосовно ще шести потерпілих. Таким чином, Л. фактично здійснив кілька

розповсюджень шкідливих програм, несанкціонованих втручань і порушень таємниці кореспонденції. Суд, застосовуючи правила кваліфікації при повторності злочинів, дав вчиненим діянням правильну правову оцінку – як злочинам, вчиненим повторно.

Важливим питанням у визначенні критеріїв відмежування комп'ютерних злочинів від суміжних є формулювання ознак, які дозволяють розмежувати несанкціоноване втручання, що спричинило втрату або підробку комп'ютерної інформації (ст. 361 КК), або несанкціоновану зміну чи знищення комп'ютерної інформації, вчинену особою, яка мала право доступу до неї (ст. 362 КК), і злочини, передбачені ст. 357 КК "Викрадення, присвоєння, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження", ст. 358 КК "Підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів" і ст. 366 КК "Службове підроблення". Оскільки документ є одним із видів інформації, подібність зазначених складів полягає в тому, що ст.ст. 357, 358, 366 та ст. 361 і 362 КК України передбачають відповідальність за знищення або перекручення інформації. Видається можливим сформулювати таке правило: у тих випадках коли документ, що є предметом злочинів, передбачених ст.ст. 357, 358 або 366, являє собою комп'ютерну інформацію, є електронним, дії особи щодо його підроблення або знищення потребують, залежно від ознак суб'єкта, додаткової кваліфікації за ст. 361 або ст. 362 КК України. Таке правило пояснюється тим, що в означених випадках спосіб підроблення або знищення документа становить самостійний склад злочину. Мова тут ведеться насамперед про електронні документи, до яких відповідно до Закону України "Про електронні документи та електронний документообіг" від 22 травня 2003 року відносяться документи, інформація в яких зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (ст. 5).

Комп'ютерна технологія привела до появи нових об'єктів інтелектуальної власності: програмного забезпечення та топо-

графій інтегральних мікросхем, які стали новими видами предметів злочинів проти інтелектуальної власності (ст.ст. 176, 177 КК України). Отже, необхідним є відмежування несанкціонованого розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (ст. 361-2) від цих злочинів. Різниця між ними полягає в ознаках об'єкта й предмета. Безпосередніми об'єктами злочину, передбаченого ст. 176 КК, виступають авторські права (особисті немайнові та майнові права авторів, їх правонаступників, пов'язані зі *створенням* і використанням творів науки, літератури, мистецтва) і суміжні права (права виконавців, виробників фонограм, організаторів мовлення, пов'язані з використанням творів). Безпосередній об'єкт порушення прав на об'єкти промислової власності (ст. 177 КК) складають відносини володіння, розпоряджання, користування результатом *своєї творчості* в будь-якій сфері промисловості чи господарської діяльності [191, с. 120 – 125]. Ці норми *охороняють інтереси автора*, особи, яка створила певні об'єкти інтелектуальної власності. У свою чергу, незаконні розповсюдження або збут комп'ютерної інформації (ст. 361-2 КК) посягають на інший об'єкт – відносини володіння, користування та розпоряджання комп'ютерною інформацією з обмеженим доступом як її авторів, так і осіб, котрі такими не є.

З цього положення випливає другий критерій, який дозволяє відмежувати згаданий комп'ютерний злочин від порушення авторського права, а саме предмет посягання. Предметом першого з названих злочинів є комп'ютерна інформація з обмеженим доступом, предметом останнього – тільки об'єкти авторського права, до яких чинне законодавство України відносить, зокрема, програми для електронно-обчислювальних машин і бази даних.

Слід також відзначити, що потерпілим від злочину, передбаченого ст. 361-2 КК, може бути будь-яка фізична чи юридична особа або держава, якщо їй належить право власності на комп'ютерну інформацію, а потерпілим від порушення авторського права та суміжних прав визнається тільки автор того чи іншого об'єкта авторського права або особа, якій на законних

підставах належить виключне чи невиключне авторське право.

Отже, якщо особа розповсюджує за допомогою комп'ютерної мережі, наприклад, електронний варіант популярного художнього твору без згоди автора, наявним є склад злочину, передбачений ст. 176 КК (за умови настання вказаних у статті наслідків). Склад злочину, передбачений ст. 361-2 КК, у цій ситуації відсутній через відсутність предмета: електронний варіант художнього твору не є комп'ютерною інформацією з обмеженим доступом. А якщо предметом розповсюдження буде комп'ютерна інформація з обмеженим доступом, яка одночасно є й об'єктом авторського права, наприклад електронний варіант підручника з грифом "таємно", матиме місце сукупність злочинів, передбачених статтями 176 та 361-2 КК України.

Необхідно також зазначити, що деякі способи вчинення комп'ютерних злочинів потребують *додаткової кваліфікації*. Так, використання для несанкціонованого втручання (ст. 361 КК) або несанкціонованого перехоплення чи копіювання (ст. 362) спеціальних технічних засобів негласного отримання інформації потребує додаткової кваліфікації за ст. 359 КК "Незаконне використання спеціальних технічних засобів негласного отримання інформації". Якщо ж несанкціоноване втручання в роботу комп'ютерної мережі або мережі електрозв'язку вчиняється шляхом умисного пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, і це, крім наслідків, передбачених у статті 361 КК, призводить до тимчасового припинення зв'язку, вчинене належить кваліфікувати за сукупністю злочинів, передбачених статтями 361 та 360 КК України "Умисне пошкодження ліній зв'язку".

Таким чином, комп'ютерна техніка може використовуватися для вчинення багатьох злочинів, однак *використання комп'ютерної техніки ще не дозволяє говорити про те, що скоєно комп'ютерний злочин*. Основним критерієм відмежування цих

злочинів від суміжних, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу, *є об'єкт посягання*. А методологія процесу відмежування, як правило, полягає в застосуванні правил розв'язання конкуренції кримінально-правових норм, зокрема конкуренції цілого та частини, загальної та спеціальної норм.

Висновки до третьої глави

Проведений аналіз юридичного змісту основних складів злочинів, передбачених статтями 361 – 363-1 КК України дає можливість зробити такі висновки:

1. Родовим об'єктом злочинів, передбачених розділом XVI КК України, є частина інформаційних суспільних відносин, що визначається як інформаційні відносини, засобом забезпечення яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі та мережі електрозв'язку.

2. Альтернативними безпосередніми об'єктами несанкціонованого втручання в роботу електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку (ст. 361 КК України) є: 1) охоронювана законом про кримінальну відповідальність структурно організована та нормативно врегульована система соціально значущих відносин власності на комп'ютерну інформацію, яка забезпечує свободу реалізації права кожного учасника на задоволення інформаційної потреби; 2) охоронювані законом про кримінальну відповідальність суспільні відносини надання та отримання послуг електрозв'язку. При цьому зміст права власності на комп'ютерну інформацію охоплює сукупність права та можливості особи: володіти або користуватися носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носієві, змінювати її, визначати долю носія.

3. До предметів несанкціонованого втручання відносяться: комп'ютерна інформація – відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну; інформація, що передається мережами електрозв'язку, – відомості, подані у формі, що дозволяє їх приймати або передавати засобами електрозв'язку.

4. Злочин, передбачений ст. 361 КК, є злочином з матеріальним складом. Об'єктивна сторона несанкціонованого втручання характеризується наявністю двох форм: 1) несанкціоноване втручання в роботу ЕОМ, систем, комп'ютерних мереж, яке призвело до витоку, втрати, підробки, блокування комп'ютерної інформації, спотворення процесу обробки такої інформації, або порушення встановленого порядку її маршрутизації; 2) несанкціоноване втручання в роботу мережі електрозв'язку, яке призвело до витоку, втрати, підробки, блокування інформації, що передається в мережі, спотворення процесу обробки такої інформації, або порушення встановленого порядку її маршрутизації.

5. Суб'єкт несанкціонованого втручання – загальний, суб'єктивна сторона може виражатися у вигляді як прямого, так і непрямого умислу.

6. Безпосередній об'єкт злочину, передбаченого ст. 361-1 КК, складають суспільні відносини власності на комп'ютерну інформацію та відносини надання й отримання послуг електрозв'язку. При цьому механізм заподіяння шкоди цим суспільним відносинам у результаті вчинення означеного злочину полягає в тому, що через створення, розповсюдження або збут шкідливих програмних чи технічних засобів створюється реальна загроза порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

7. До предметів злочину, передбаченого ст. 361-1 КК України, відносяться: 1) шкідливі програмні засоби – програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого втручання в роботу комп'ютер-

ної техніки або мереж електрозв'язку, використання яких заподіює або створює загрозу заподіяння шкоди інформаційним відносинам; 2) шкідливі технічні засоби – різного роду пристрої, устаткування, розроблені для несанкціонованого втручання в роботу комп'ютерної техніки або мереж електрозв'язку, використання яких заподіює або створює загрозу заподіяння шкоди інформаційним відносинам.

8. Злочин, передбачений ст. 361-1 КК, є злочином з формальним складом. Його об'єктивна сторона може виражатися в одній з таких форм: створення шкідливих програмних або технічних засобів – результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу; розповсюдження шкідливих програмних засобів – оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх "закладання" в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення; розповсюдження шкідливих технічних засобів – оплатне або безоплатне передавання шкідливого технічного засобу, а також його установлення в ЕОМ, системи або комп'ютерні мережі; збут шкідливих програмних або технічних засобів – оплатне або безоплатне відчуження таких засобів.

9. Суб'єкт злочину, передбаченого ст. 361-1 КК, – загальний. Суб'єктивна сторона характеризується прямим умислом. При цьому кримінальна відповідальність за створення шкідливих програмних і технічних засобів настає тільки за наявності мети їх подальшого використання, збуту або розповсюдження.

10. Безпосереднім об'єктом несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України), виступають суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом. Предметом злочину є комп'ютерна інформа-

ція, яка характеризується наявністю трьох додаткових ознак: 1) відноситься до інформації з обмеженим доступом; 2) створена відповідно до чинного законодавства; 3) захищена відповідно до чинного законодавства.

11. За конструкцією *об'єктивної сторони* злочин, передбачений ст. 361-2 КК України, є формальним. Він уважається закінченим з моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом. Розповсюдження комп'ютерної інформації з обмеженим доступом – оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб. Збут комп'ютерної інформації з обмеженим доступом – її оплатне або безоплатне відчуження.

12. За конструкцією об'єктивної сторони злочин, передбачений ст. 362 КК, є матеріальним. Об'єктивна сторона представлена п'ятьма альтернативними формами. Три з них передбачено в ч. 1 ст. 362 КК: несанкціоновані зміна, знищення та блокування комп'ютерної інформації. Решта – у ч. 2 ст. 362: несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

13. Суб'єкт злочину, передбаченого ст. 362 КК, – спеціальний. Це особа, яка має право доступу до комп'ютерної інформації. Суб'єктивна сторона характеризується виною у формі прямого або непрямого умислу.

14. Об'єкт злочину, передбаченого статтею 363 КК, складають суспільні відносини, у межах яких забезпечується безпека використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

15. Склад злочину, передбаченого цією статтею, матеріальний, його *об'єктивна сторона* характеризується такими ознаками: діяння (три альтернативні форми) – порушення правил експлуатації електронно-обчислювальних машин (комп'юте-

рів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації; суспільно небезпечні наслідки – значна шкода; причинний зв'язок між діянням і суспільно небезпечними наслідками.

16. *Суб'єкт* злочину, передбаченого ст. 363 КК, – спеціальний. Це особа, яка відповідає за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Суб'єктивна сторона* злочину характеризується тим, що діяння може бути вчинене як умисно, так і з необережності, але до наслідків можливе тільки необережне ставлення.

17. Об'єктом злочину, передбаченого ст. 363-1 КК України, є суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки та мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію. Предметом цього злочину є повідомлення електрозв'язку.

18. Склад злочину, передбачений ст. 363-1 КК, – матеріальний. Об'єктивну сторону складають: 1) діяння – масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки – порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причинний зв'язок між діянням та наслідками.

19. Суб'єкт злочину, передбаченого ст. 363-1 КК, – загальний. Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків.

20. Дослідження відмежування комп'ютерних злочинів від суміжних дозволяє стверджувати, що комп'ютерна техніка може використовуватися для вчинення багатьох злочинів, однак використання комп'ютерної техніки ще не дозволяє говорити про те, що скоєно комп'ютерний злочин. Основним критерієм

відмежування цих злочинів від суміжних, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу, є об'єкт посягання. Методологія процесу відмежування, як правило, полягає в застосуванні правил розв'язання конкуренції кримінально-правових норм, зокрема конкуренції цілого та частини, загальної та спеціальної норм.

Глава 4

Удосконалення кримінально-правових засобів охорони інформаційної безпеки у сфері використання інформаційних технологій

Висновки, зроблені в попередній главі, а також сформульовані раніше положення щодо соціальної потреби в кримінально-правовій охороні інформаційної безпеки у сфері використання інформаційних технологій та методології дослідження криміналізації дозволяють перейти до аналізу якості кримінально-правової охорони в цій сфері та формулювання, за необхідності, відповідних змін і доповнень до чинного законодавства про кримінальну відповідальність.

4.1. Аналіз норм розділу XVI КК України з позицій дотримання принципів визначеності та єдності термінології, а також повноти складу

Перш за все вважаємо за доцільне звернути увагу на порушення принципу ***визначеності та єдності термінології***. Найбільш яскраво це можна проілюструвати невідповідністю норм кримінального та адміністративного законодавства. Так, ст. 148-1 Кодексу України про адміністративні порушення, що має назву "Порушення Правил надання та отримання телекомунікаційних послуг" установлює відповідальність за "здійснення дій, що призвели до зниження якості функціонування

телекомунікаційних мереж, або самовільне (без відома оператора телекомунікацій) отримання телекомунікаційних послуг". Виникають справедливі питання. Чим уважати незаконне підключення до мережі кабельного телебачення – самовільним отриманням телекомунікаційних послуг чи несанкціонованим втручанням у роботу мереж електрозв'язку, що призвело до витоку інформації? Чи правильно вважати використання Інтернету від імені та за рахунок чужих осіб несанкціонованим втручанням у роботу комп'ютерної мережі, а не знову ж таки самовільним отриманням послуг електрозв'язку? Стаття 212-6 КУпАП України має назву "Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем". У числі іншого цією нормою встановлюється відповідальність за "незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі". Як відмежувати це правопорушення від несанкціонованого втручання в роботу комп'ютерної мережі, що призвело до витоку комп'ютерної інформації?Зауважимо, що використання в одних випадках терміна "витік", а в інших – "копіювання" додає плутанини ще й тому, що витік не завжди пов'язаний з копіюванням, а копіювання не завжди призводить до витоку. Пригадаємо приклад, пов'язаний з отриманням логінів і паролів шляхом використання троянської програми [164]. У цій ситуації дії зловмисника щодо отримання реквізитів чужих облікових записів правильно кваліфіковані відповідно до кримінального законодавства як несанкціоноване втручання, що призвело до витоку інформації (ст. 361 КК). Однак ці дії, через використання різної термінології, можна розглядати і як незаконне копіювання комп'ютерної інформації (ст. 212-6 КУпАП). Справа в тому, що адміністративне та кримінальне законодавства "розмовляють різними мовами". Якщо адміністративне оперує категоріями "телекомунікаційна послуга", "інформаційна (автоматизована) система", то в кримінальному законодавстві за-

борони формулюються за допомогою термінів "електронно-обчислювальна машина", "комп'ютерна мережа", "мережа електрозв'язку" тощо. Маємо констатувати, що порушення принципу визначеності та єдності термінології зумовлює й порушення принципу ***економії репресії***. Оскільки через термінологічну невідповідність не видається можливим чітко та обґрунтовано розмежувати адміністративно-правове та кримінально-правове регулювання суспільних відносин у сфері використання інформаційних технологій.

Таким чином, необхідним є приведення розглянутих норм адміністративного та досліджуваних норм кримінального законодавства у змістову та термінологічну відповідність. Проте для формулювання пропозицій з цього питання необхідним є аналіз відповідності норм, об'єднаних у розділі XVI, принципу суспільної небезпечності діянь, які підлягають криміналізації. Таке дослідження надасть змістовні аргументи для розмежування кримінально-правових та адміністративно-правових засобів впливу на суспільні відносини у сфері інформатизації. Отже, до пропозицій щодо вдосконалення норм чинного законодавства в контексті встановленої термінологічної невідповідності повернемося пізніше.

До порушення принципу визначеності термінології слід також віднести використання в тексті закону таких термінів, як "електронно-обчислювальна машина", "автоматизована система" та "комп'ютерна мережа". Це пов'язано з відсутністю чітких законодавчих визначень цих понять. Так, терміни "електронно-обчислювальна машина" та "комп'ютерна мережа" визначаються державним стандартом (ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. Від 01.01.96), термін "автоматизована система" визначається як у Законі України "Про захист інформації в інформаційно-телекомунікаційних системах", так і в державному стандарті (ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Від 01.07.94.). Крім того, визначення, наведені в законі та стандарті, принципово різні.

Викликає певні сумніви й сама доцільність виокремлення в кримінальному законодавстві видів засобів опрацювання комп'ютерної інформації. Від виду такого засобу навряд чи залежить суспільна небезпечність комп'ютерного злочину. Не можна сказати, що несанкціоноване втручання в роботу ЕОМ, наприклад, більш суспільно небезпечне, ніж несанкціоноване втручання в роботу комп'ютерної мережі. Як уже зазначалося, суспільна небезпечність комп'ютерного злочину насамперед залежить від соціальної значущості суспільних відносин власності на інформацію, яким заподіюється шкода, змісту комп'ютерної інформації, що знищується, копіюється, перекручується або блокується.

Нарешті, наявність у кримінальному законі переліку засобів оброблення інформації зумовлює певні обмеження його застосування для протидії комп'ютерним злочинам: з появою нових, не передбачених у законі засобів таке законодавство неможливо буде застосовувати для захисту інформаційних суспільних відносин, пов'язаних із використанням новітнього обладнання.

З метою виправлення наведених термінологічних недоліків пропонується не визначати в тексті закону види засобів оброблення комп'ютерної інформації (електронно-обчислювальна машина, система, комп'ютерна мережа), а використовувати один загальний термін – "комп'ютерна система". Він визначається в Конвенції про кіберзлочинність, прийнятій у рамках Ради Європи 23 листопада 2001 року та ратифікованій Україною 7 вересня 2005 року. Під *комп'ютерною системою* в Конвенції пропонується розуміти будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичне опрацювання даних. Такий термін є більш вдалим, оскільки він повністю охоплює електронно-обчислювальну машину, автоматизовану систему та комп'ютерну мережу. Його використання дозволило б зробити редакцію статті більш лаконічною, не "прив'язувати" кримінальне законодавство до певного стану

розвитку інформаційних технологій, зробити його у зв'язку з цим стабільнішим.

Термінологічні суперечності спостерігаються у визначенні інформації як предмета злочинів, передбачених статтями 361 та 362 КК України. У кожній із цих статей використовується специфічний термін. Так, предметом несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361) є інформація. А предметом злочину, передбаченого ст. 362 КК України, є інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації.

Перш за все необхідно відзначити, що використання терміна "інформація, яка оброблюється (або зберігається) в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації" є не зовсім вдалим, оскільки він громіздкий, а за змістом повністю відповідає більш точному термінові "комп'ютерна інформація", що використовувався в попередній редакції розділу XVI КК України. І, як уже зазначалося, навряд чи можна визнати доцільним розмежування термінів "інформація, що оброблюється..." (ст. 362 КК) та "інформація, що зберігається..." (ст. 361-2 КК), оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення.

Однак головною термінологічною вадою визначення предмета означених посягань є використання категорії "інформація". Тут виникає питання: чи відносяться до комп'ютерної інформації комп'ютерні програми? Необхідно зауважити, що деякі автори дають позитивну відповідь на нього [346, с. 815; 347, с. 747], але це не можна визнати правильним. Комп'ютерні програми, що являють собою набір команд, відповідно до якого здійснюється автоматизована обробка даних, не є інформацією за визначенням. У зв'язку з цим не можна не пригадати

обґрунтовані висновки російського філософа В. Тюхтіна, котрий уважає інформацію властивістю суто людської свідомості та спілкування і пов'язує її з наявністю суб'єкта, який пізнає [196, с. 78]. Підтвердження висловлених положень ми знаходимо і в кримінальному законодавстві зарубіжних країн. Так, відповідно до системи визначень, які відкривають Частину 10.7 КК Австралії "Комп'ютерні злочини" до даних слід відносити інформацію або програму чи її частину (476.1 (1)) [337, с. 317 – 318]. Поняття "комп'ютерна інформація" та "комп'ютерна програма" розрізняють на законодавчому рівні також кримінальні кодекси Республіки Білорусь (ст. 351) [344], Естонії (ст.ст. 268 – 270) [351, с. 246 – 247], Литви (ст.ст. 196, 197) [343, с. 234], Латвії (ст. 242) [342, с. 290 – 291] та ін.

Неувага до такої специфіки інформації призводить деяких дослідників до формулювання висновків, які слід визнавати хибними навіть на рівні формальної логіки. Наприклад: "Комп'ютерна інформація – це відомості про навколишній світ та процеси, що в ньому відбуваються, які представлені у формі даних, зафіксованих в електронному вигляді. Зазначеним поняттям охоплюється і будь-яка комп'ютерна програма, під якою ми пропонуємо розуміти побудовану за особливими правилами сукупність даних, що забезпечує функціонування та керування комп'ютерними системами та/або телекомунікаційними мережами, виконання ними певних завдань" [3, с. 104]. Керуючись такими визначеннями, важко відповісти до чого слід відносити комп'ютерну програму – до відомостей про навколишній світ чи відомостей про процеси, що в ньому відбуваються. Отже, аналіз змісту термінів, використаних у диспозиції статей 361 та 362 КК України, свідчить про те, що неправильною слід уважати кваліфікацію за означеними нормами в тих випадках, коли мало місце несанкціоноване втручання, що призвело до знищення або спотворення програмного забезпечення, або несанкціоноване знищення програмного забезпечення особою, яка має право доступу до комп'ютерної інформації. Такі дії можна кваліфікувати як несанкціоноване втручання, що призвело до блокування інформації, спотворення процесу

обробки інформації, порушення встановленого порядку її маршрутизації або як пошкодження чи знищення майна. Зрозуміло, що таке положення звужує можливості використання означених норм для протидії комп'ютерним злочинам.

З урахуванням зазначених недоліків законодавства, пов'язаних із використанням категорії "інформація", пропонуємо звернутися до Конвенції про кіберзлочинність, яка для позначення предмета передбачених у ній злочинів використовує термін "комп'ютерні дані", тобто "будь-яке подання фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою". Отже, під комп'ютерними даними розуміються комп'ютерна інформація і комп'ютерні програми. Якщо предметом досліджуваних злочинів замість інформації визнати комп'ютерні дані, зазначених вище проблемних питань при кваліфікації незаконних діянь щодо програмного забезпечення можна уникнути. За наявності таких змін у законодавстві знищення чи перекручення як інформації, так і програмного забезпечення можна буде кваліфікувати як знищення або перекручення комп'ютерних даних. Структуру ознак комп'ютерних даних як предмета злочину доцільно залишити такою, яка пропонувалася для характеристики предмета досліджуваних злочинів відповідно до чинного законодавства, та включити до неї фізичну, економічну та юридичну ознаки.

Таким чином, стосовно відповідності норм розділу XVI КК України принципу визначеності та єдності термінології маємо зазначити таке: 1) означені закони про кримінальну відповідальність при формулюванні ознак злочинних діянь використовують термінологію, що різниться з тією, яка використана при формулюванні ознак суміжних адміністративних правопорушень, *відсутність єдності* термінології значно зменшує ефективність відповідних норм як кримінального, так і адміністративного законодавства; 2) норми розділу містять терміни, які *неоднаково визначаються* як на рівні законодавства, так і на рівні наукового тлумачення, що звужує можливості його

використання для охорони відповідних суспільних відносин; 3) необґрунтованим, через небезпеку "технологічної залежності" законодавства, слід визнавати й використання в диспозиціях означених норм переліку технічних засобів оброблення інформації.

Як зазначалося раніше, однією з умов ефективної криміналізації є конкретність і визначеність кримінально-правової норми, що встановлює караність певного діяння, визначення в законі всіх ознак діяння, необхідних для визнання особи винною у вчиненні злочину, тобто дотримання принципу ***повноти складу***. Порушення цього принципу стосовно криміналізації злочинів у сфері використання комп'ютерної техніки та мереж електрозв'язку полягає як у формулюванні занадто громіздких законодавчих визначень, які ускладнюють установлення змісту ознак конкретних складів злочинів, так і в недостатній визначеності складів конкретних комп'ютерних злочинів у диспозиціях відповідних кримінально-правових норм.

Так, зміст ст. 361 КК свідчить про те, що *законодавець передбачив кримінальну відповідальність за абсолютно самостійні склади злочинів в одній нормі*. Несанкціоноване втручання в роботу комп'ютерної техніки та несанкціоноване втручання в роботу мереж електрозв'язку не збігаються, як це можна було побачити, за ознаками об'єкта, предмета й об'єктивної сторони. Наслідком намагання законодавця передбачити кримінальну відповідальність за посягання на різні основні об'єкти в одній нормі є невизначеність і неконкретність ознак складів цих посягань. Так, законодавче визначення предмета злочину, передбаченого ст. 361 КК, – "інформація". Використання загального, такого, що охоплює всі види інформації, поняття свідчить про намагання законодавця за допомогою одного терміна визначити два принципово різні види інформації, які, судячи з аналізу диспозиції статті, є предметами несанкціонованого втручання: комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку. Проте подібне законодавче формулювання залишає певну невизначеність у розумінні предмета цього злочину. Наприклад, чи можна вважати пред-

метом несанкціонованого втручання інформацію на паперових носіях, яка виявилася замкненою в кімнаті, доступ до якої був заблокований автоматизованою системою безпеки внаслідок несанкціонованого порушення режиму її функціонування? Закон не дає чіткої відповіді, отже, маємо констатувати недостатню визначеність кримінально-правової норми. У зв'язку з цим видається доцільним передбачити кримінальну відповідальність за несанкціоноване втручання в роботу мереж електрозв'язку в окремій статті КК.

Наступним порушенням принципу повноти складу є відсутність у кримінальному законі чітких положень щодо змісту суб'єктивної сторони злочинів, передбачених ст.ст. 361 – 363-1 КК. Це породжує можливість принципово різних тлумачень змісту законодавчих положень та, відповідно, не кращим чином впливає на ефективність кримінально-правової охорони. Наприклад, вище ми зазначали, що суб'єктивна сторона злочину, передбаченого ч. 1 ст. 361 КК, України характеризується прямим або непрямим умислом. Подібної точки зору дотримується й Д.С. Азаров [3, с. 190]. Разом із тим, принципово іншу думку має П.П. Андрушко, який зазначає, що суб'єктивна сторона несанкціонованого втручання характеризується умисним ставленням до діяння, а також умисним або необережним ставленням до настання наслідків у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу її обробки або порушення порядку маршрутизації [13, с. 45]. Схожа ситуація повторюється і при розгляді суб'єктивної сторони злочину, передбаченого ст. 362 КК. Однак у цьому питанні позиція автора щодо характеристики такого посягання як умисного збігається з положеннями, висловленими П.П. Андрушком [13] та іншими дослідниками [37, с. 31]. Водночас Д.С. Азаров уважає, що злочин, передбачений ст. 362 КК, може бути як умисним, так і необережним [3, с. 191 – 192]. При цьому аргументів, достатніх для розв'язання цього спірного питання, кримінальний закон не надає. Отже, для подальшої роботи щодо вдосконалення кримінального законодавства необхідним є чітке формулювання ознак суб'єктивної сторони у від-

повідних кримінально-правових нормах, що передбачають відповідальність за злочини у сфері використання інформаційних технологій.

Недостатньо конкретним є *формулювання ознак спеціального суб'єкта* злочину, передбаченого ст. 362 КК України (особа, яка має право доступу до комп'ютерної інформації). Цей недолік можна проілюструвати прикладом. Зловмисник перекрутив комп'ютерну інформацію, розташовану на загальнодоступному сайті в мережі Інтернет. Наприклад, в інформаційному повідомленні про науково-практичну конференцію, розміщеному на сайті певного університету, змінив дату проведення заходу. Оскільки інформація на сайті загальнодоступна, ми маємо констатувати, що зловмисник змінив комп'ютерну інформацію, до якої мав право доступу, тобто вчинив злочин, передбачений ч. 1 ст. 362 КК. Зазначимо, що так само буде кваліфікуватися й незаконна зміна цієї інформації, вчинена, наприклад, співробітником інформаційного відділу університету, оскільки він також має право доступу до інформації, що є предметом посягання. Однак суспільна небезпечність посягання, наведеного в останньому прикладі, видається більшою, оскільки співробітник інформаційного відділу наділений певними правами доступу до комп'ютерної інформації не тільки на підставі того, що вона є загальнодоступною, а й у зв'язку з посадою, яку він займає. Таким чином, наявне в законі формулювання спеціального суб'єкта злочину, передбаченого ст. 362 КК, – "особа, яка має право доступу до інформації" – не повною мірою забезпечує можливість урахування при кваліфікації підвищеної суспільної небезпечності посягання, вчиненого особою, яка має певні повноваження щодо комп'ютерної інформації, зумовлені її специфічним статусом.

Таке становище, коли кваліфікація злочину не відповідає ступеневі його суспільної небезпечності, свідчить про очевидну недосконаліть діючого механізму кримінально-правової охорони суспільних відносин власності на комп'ютерну інфо-

рмацію, зумовлену в цьому випадку неконкретністю законодавчого визначення суб'єкта злочину. Можна сказати, що в цій ситуації "дух" закону не відповідає його "букві".

З урахуванням висловлених зауважень ознаки суб'єкта так званих "інсайдерських" злочинних посягань на комп'ютерну інформацію видається доцільним конкретизувати таким чином: *особа, яка має правомірний доступ до комп'ютерних даних у зв'язку з займаною посадою або спеціальними повноваженнями.*

До числа таких осіб слід включати працівників підприємств, установ або організацій, функціональні обов'язки яких передбачають використання комп'ютерних даних, що належать роботодавцеві, для виконання завдань, які стоять перед ними (інженери-програмісти, оператори ЕОМ, адміністратори комп'ютерних мереж тощо). До таких осіб відносяться і працівники правоохоронних органів під час виконання спеціальних оперативно-розшукових заходів, пов'язаних із доступом до комп'ютерної інформації. Важливо відмітити, що ознаки спеціального суб'єкта в такій редакції статті матимуть тільки безпосередні користувачі ЕОМ, систем або комп'ютерних мереж. Допоміжний персонал (водії, охоронці, слюсарі тощо) хоча й може мати певний доступ до ЕОМ, системи або комп'ютерної мережі, але спеціальним суб'єктом цього злочину не є, через те що не має санкціонованого доступу до інформації.

Таким чином, дослідження норм, передбачених у розділі XVI КК, у контексті дотримання принципу повноти складу дозволяє зазначити, що: 1) для підвищення визначеності положень КК щодо несанкціонованого втручання (ст. 361) доцільно передбачити в окремих нормах кримінальну відповідальність за несанкціоноване втручання в роботу комп'ютерної техніки та мереж електрозв'язку; 2) потребують уточнення положення закону щодо суб'єктивної сторони досліджуваних складів злочинів, а також законодавчого визначення суб'єкту злочину, передбаченого ст. 362 КК.

4.2. Прогалини кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій та прояви її надлишковості

На окрему увагу заслуговує дослідження дотримання принципу ***відсутності прогалин та ненадлишковості заборони*** при криміналізації комп'ютерних злочинів. Передусім це стосується доцільності криміналізації незаконного збуту або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361-2). Як свідчить проведений аналіз відмежування складу цього злочину від суміжних, кримінальна відповідальність за нього може наставати в таких випадках:

1) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає державну таємницю, здійснює особа, якій ці відомості довірені не були й це не пов'язане з передачею її іноземній державі, іноземній організації або їх представникам;

2) коли розповсюдження або збут комп'ютерної інформації, зміст якої складають:

- відомості про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби;
- лікарська таємниця;
- комерційна або банківська таємниця;
- відомості про заходи безпеки щодо особи, взятої під захист;
- дані досудового слідства чи дізнання, –

здійснює особа, якій ці відомості довірені не були, тобто вона не мала спеціальних зобов'язань щодо збереження їх в таємниці;

3) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає лікарську, комерційну або банківську таємницю, здійснює особа, якій вони були довірені, але наслідків, зазначених у ст.ст. 145 чи 232 не настало;

4) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складає таємницю усиновлення (ст. 168) або приватного життя (ст. 182), але до умислу суб'єкта не включається усвідомлення та бажання чи свідоме допущення заподіяння шкоди конкретній особі або чітко визначеній групі осіб, тобто відсутні ознаки складу злочину проти конституційних прав та свобод;

5) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складають відомості з обмеженим доступом інших видів.

Щоб не перевантажувати запропоновану схему, "за дужки" ми винесли такі ознаки комп'ютерної інформації, предмета злочину, передбаченого ст. 361-2 КК, як "зібрана та захищена відповідно до чинного законодавства". Однак видається, що і без цього запропонований перелік випадків, коли можливим є застосування ст. 361-2 КК, яскраво демонструє очевидну надлишковість кримінально-правової заборони, передбаченої досліджуваною нормою. Дійсно, крім випадків шпигунства, не можна погодитися з тим, що слід уважати злочином розповсюдження відомостей, які складають певну таємницю, вчинене особою, якій вони не були довірені. Ситуація з відповідальністю за порушення лікарської, комерційної або банківської таємниці є ще більш наочною. Чи обґрунтовано вважати певні дії злочином, коли наслідки, що зумовлюють кримінальну відповідальність за них, не настали? Єдиним аргументом, який може бути використаний для обґрунтування доцільності такої відповідальності, можна вважати лише те, що кримінальна відповідальність продиктована формою цих відомостей, тим, що вони є комп'ютерною інформацією. Однак, крім того, що він спірний, цього аргументу явно недостатньо для обґрунтування кримінальної відповідальності за подібні дії. Форма інформації ні в якому разі не може обґрунтовувати підвищену суспільну небезпечність її розповсюдження або збуту.

Проте відкритим залишається питання кримінально-правової охорони інших видів інформації з обмеженим доступом. Можна сказати, що це єдина позитивна риса наявності в Кри-

мінальному кодексі такої норми, як ст. 361-2. Вона дійсно забезпечує певну охорону суспільних відносин власності на комп'ютерну інформацію з обмеженим доступом. Однак указівка на те, що предметом цього злочину є комп'ютерна інформація з обмеженим доступом, яка *захищена* відповідно чинного законодавства, унеможливлює ефективне використання норми. Наявність такої ознаки предмета означає, що злочин, передбачений ст. 361-2 КК, буде мати місце лише тоді, коли незаконно розповсюджується або збувається інформація, що обробляється із застосуванням певної системи захисту. Таким чином, проблематичним буде застосування цієї норми для кваліфікації тих випадків, коли особа збуває або розповсюджує інформацію з обмеженим доступом, яку, наприклад, було отримано з захищеної комп'ютерної мережі шляхом подолання системи захисту, тобто на момент розповсюдження інформація з обмеженим доступом уже не захищалася спеціальними технічними засобами. Зауважимо, що подібні випадки траплялися, вони стосувалися незаконного розповсюдження такого виду комп'ютерної інформації з обмеженим доступом, як електронні бази персональних даних. Наприклад, у 2003 році в продажу з'явилися бази даних російських операторів мобільного зв'язку "Мобільні ТелеСистеми" та "Бі лайн". Крім прізвищ абонентів вони містили паспортні дані, адресу місця проживання, індивідуальний номер платника податків та іншу інформацію. Зазначимо також, що ринок персональних даних – це сегмент комп'ютерної злочинності, який швидко розвивається, деякі фахівці оцінюють його в 3 мільярди доларів США на рік [312]. Але, на жаль, відзначені недоліки статті 361-2 КК унеможливлюють її застосування для протидії новому виду комп'ютерної злочинності. Для того щоб бути об'єктивними, необхідно зазначити, що персональні дані певною мірою захищені кримінальним законодавством: ст. 182 КК України передбачає відповідальність за порушення недоторканності приватного життя, однак використання цієї норми для протидії незаконним операціям з електронними базами персональних даних видається не зовсім ефективним. Ця стаття

забезпечує фрагментарний захист суспільних відносин від аналізованого посягання, адже безпосереднім об'єктом незаконних дій з електронними базами персональних даних є право власності осіб (юридичних або фізичних), які на законних підставах придбали або створили ці бази, а конституційне право на недоторканність приватного життя виступає, як видається, лише додатковим факультативним об'єктом таких діянь.

Наведених вище аргументів достатньо для того, щоб зробити висновок про виключення ст. 361-2 з Кримінального кодексу. Однак це не означає, що необхідно декриміналізувати збут або розповсюдження відомостей з обмеженим доступом. Ця проблема, як видається, не відноситься до злочинів у сфері використання інформаційних технологій. Вище ми зазначали, що форма подання інформації не є визначальним чинником суспільної небезпечності її збуту або розповсюдження. Отже, логічним буде повернення до цього питання в главі, присвяченій дослідженню кримінально-правових засобів охорони суспільних відносин щодо забезпечення доступу до інформації.

Певні прогалини в кримінально-правовій охороні суспільних відносини зумовлені вадами *конструкції об'єктивної сторони* складу злочину, передбаченого ст. 361 КК України. Як уже зазначалося, цей склад злочину є матеріальним, його об'єктивна сторона складається з діяння (несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), суспільно небезпечних наслідків (витік, втрата, підробка, блокування інформації, спотворення процесу обробки інформації та порушення порядку її маршрутизації) та причинного зв'язку між діянням і наслідками. Отже, відповідно до чинного законодавства настання вказаних наслідків не буде визнаватися злочином, якщо їм не передувало несанкціоноване втручання в роботу засобів опрацювання інформації. Наприклад, під час коли електронно-обчислювальна машина не була ввімкнена, тобто принципово неможливим було втручання в її роботу, на жорсткий диск здійснено вплив потужним електромагнітним випромінюванням, наслідком чого виявилася втрата інформації, що знаходилася на ньому.

Використання ст. 361 КК для кваліфікації цього випадку виключається, оскільки не було несанкціонованого втручання в роботу ЕОМ. Зазначимо також, що фізичне знищення або пошкодження носія, який був відокремлений від ЕОМ, АС або комп'ютерної мережі, з метою знищення інформації, яка на ньому знаходиться, знову ж таки з цієї самої причини неможливо кваліфікувати за розгляданою статтею. В останньому випадку можна говорити лише про умисне знищення чужого майна, але використання ст. 194 КК допускається лише тоді, коли в результаті знищення було заподіяно шкоду у великих розмірах. Крім того, така кваліфікація не відповідала б об'єкту посягання: шкоду заподіяно інформаційним відносинам, а діяння кваліфікується як посягання на відносини власності на річ. Без несанкціонованого втручання в роботу ЕОМ, автоматизованих систем або комп'ютерних мереж можливим є й ознайомлення з інформацією, яка в них обробляється. Наприклад, за допомогою спеціального обладнання можливо, перебуваючи на певній відстані від ЕОМ, отримувати відеосигнал, який подається на монітор, та ознайомлюватися з інформацією, яка відображається на ньому. Блокувати комп'ютерну інформацію також можливо без несанкціонованого втручання в роботу засобу її оброблення. Отже, вада конструкції об'єктивної сторони складу несанкціонованого втручання (ст. 361 КК) полягає в тому, що вона не враховує можливість заподіяння вказаних у нормі суспільно небезпечних наслідків без вчинення передбаченого в нормі діяння. Крім того, відсутність несанкціонованого втручання (діяння) не означає, що настання цих наслідків втрачає суспільну небезпечність. Як уже неодноразово відзначалося, головним чинником суспільної небезпечності комп'ютерного злочину є значущість інформації.

Таким чином, формулювання ознак злочинів у сфері використання інформаційних технологій, яке містить вказівку на діяння у вигляді несанкціонованого втручання в роботу комп'ютерної техніки, є недоцільним.

Певні прогалини чинного кримінального законодавства пов'язані також із законодавчим визначенням *суб'єкта злочину*,

передбаченого ст. 363 КК. Таким суб'єктом є особа, яка відповідає *за експлуатацію* електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. Це визначення перебуває у явній невідповідності з формами об'єктивної сторони розгляданого злочину, яка може виявлятися в порушенні *порядку захисту* інформації, *правил захисту* інформації або *правил експлуатації* комп'ютерної техніки. Слід погодитися з зауваженням Д.С. Азарова, що "не може вважатися злочином порушення правил (порядку) захисту інформації, вчинене особою, яка за забезпечення цього захисту відповідає, а за дотримання правил експлуатації техніки – ні" [236, с. 78.]. Тобто формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 363 КК, значно звужує можливості використання цієї норми, створює певні прогалини в кримінально-правовій охороні суспільних відносин від злочинних посягань у сфері використання інформаційних технологій. Ці прогалини пов'язані з кваліфікацією злочинних дій осіб, які відповідають тільки за дотримання порядку або правил захисту комп'ютерної інформації.

Наступна прогалина кримінально-правової охорони суспільних відносин у сфері забезпечення дотримання вимог експлуатації комп'ютерної техніки, порядку та правил захисту інформації пов'язана з невідповідністю норм конструктивних галузей права потребам захисту суспільних відносин у сфері використання інформаційних технологій. Як зазначалося вище, на сьогодні спеціальні вимоги встановлюються лише щодо захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Відповідно, і ст. 363 КК виступає елементом саме цього правового механізму інформаційної безпеки. Її наявність дозволяє притягати до кримінальної відповідальності осіб, які порушують вимоги захисту інформації, але головним чином сприяє, як видається, підвищенню ефективності попередження комп'ютерних злочинів у державному секторі. Стимулюючи відповідальних осіб застосовувати заходи захисту інформації, ця норма забезпечує врешті-решт значне зниження ймовірності посягання на державний інформа-

ційний ресурс. Однак статистичні дані свідчать про певну невиправданість такого підходу. Це перш за все дані Українського Антивірусного Центру: 1) у першому півріччі 2004 року втрати від вірусних атак в Україні склали 290 мільйонів гривень; 2) найбільші збитки в розрахунку на один ПК спостерігаються в середньому бізнесі, де витрати на технічний захист інформації мінімальні; 3) значно збільшилася кількість вірусних інцидентів, пов'язаних із домашніми користувачами, основна причина масового поширення вірусів у цьому сегменті – практично повна відсутність антивірусних засобів; 4) збитки від вірусних атак в Україні у першій половині 2004 року зросли на 30% у порівнянні з аналогічним періодом 2003 року [357]. Отже, можна сміливо стверджувати, що відсутність спеціального нормативного регулювання у сфері захисту недержавної інформації призводить до недостатності заходів щодо захисту такої інформації, які мають здійснюватися її власниками, та певною мірою потенційно небезпечна зростанням показників комп'ютерної злочинності. Недостатність заходів захисту недержавного інформаційного ресурсу є одним з віктимологічних факторів комп'ютерної злочинності. При цьому можливості використання ст. 363 КК для стимулювання застосування засобів інформаційної безпеки в цьому сегменті інформаційних відносин значно обмежені через відсутність норм, які б зобов'язували їх використовувати.

Цілком зрозуміло, що ефективним захист інформації буде за умови комплексного використання технічних, програмних та організаційних засобів. Очевидно також і те, що ставити власникам недержавної інформації вимоги, подібні до тих, які передбачаються наведеними нормативними документами, недоцільно, крім того, це навряд чи сприятиме розвиткові відносин інформатизації в країні. Однак проблема законодавчого стимулювання більш широкого використання засобів захисту недержавної інформації є наявною та потребує якнайшвидшого розв'язання. Отже, ще одним напрямком удосконалення національного законодавства є створення нормативної бази для розвитку системи захисту недержавної інформації, яка б

відповідала можливостям її власників і забезпечувала достатньо надійний захист відповідного сегменту національного інформаційного ресурсу. Це сприятиме попередженню комп'ютерної злочинності та забезпечить більш широкі можливості реалізації конституційного права на інформацію.

Отже, чинний механізм кримінально-правової охорони відносин у сфері використання інформаційних технологій містить прогалини, зумовлені як недосконалістю диспозиції ст. 363, так і недоліками законодавчого регулювання використання засобів захисту інформації. Мабуть, найбільш серйозним аргументом на підтвердження цього висновку є вкрай незначна практика використання ст. 363, яка входить в очевидну конфронтацію з кримінологічними характеристиками цих посягань. Як ми зазначали, фахівці з інформаційної безпеки переважну більшість комп'ютерних злочинів пов'язують саме з діяльністю спеціальних суб'єктів, осіб, що мають певні повноваження щодо інформації, яка виступає предметом посягання. Наприклад, у доповіді Global Security Report компанії Trustwave, одного з лідерів ринку апаратних та програмних продуктів для захисту інформації, зазначається, що близько 88 відсотків порушень інформаційної безпеки пов'язано з використанням недостатньо надійних криптографічних засобів або неналежного рівня безпеки у використанні програмного забезпечення сторонніх виробників [238]. Чинне законодавство містить дві норми про відповідальність таких осіб – статті 362 та 363 КК. Однак серед осіб, засуджених у 2008 році, лише 12,3% були засуджені за ст. 362, а за ст. 363 взагалі не було засуджено жодної особи [73]. Тобто практика застосування національного законодавства явно не відповідає експертним оцінкам щодо структури комп'ютерної злочинності. При цьому така невідповідність лежить далеко за межами статистичної похибки, ідеться про переважну більшість в оцінках експертів і меншість у статистичних показниках. Зрозуміло, що це зумовлюється не тільки вадами чинного законодавства, хоча останні є достатньо вагомим чинником ситуації, що склалася.

Ураховуючи означені недоліки ст. 363 КК, суб'єктом порушення правил експлуатації комп'ютерних систем, порядку чи правил захисту комп'ютерних даних пропонується визнавати особу, яка відповідає за дотримання вимог інформаційної безпеки. Зауважимо, що ключовий для дослідження термін "інформаційна безпека" ми вживаємо в цій нормі у вузькому значенні, розуміючи під нею сукупність вимог щодо забезпечення працездатності комп'ютерної техніки та іншого телекомунікаційного обладнання, організації та здійснення програмного, технічного й організаційного захисту комп'ютерних даних. Ще раз зазначимо, що для забезпечення ефективного використання цієї норми необхідним є також доповнення законодавства положеннями про обов'язок використання засобів захисту інформації у недержавному секторі.

Окремою проблемою протидії суспільно небезпечним посяганням у сфері використання комп'ютерної техніки в контексті дотримання принципу відсутності прогалин є *питання відповідальності за розповсюдження спаму* (SPAM, sending of predatory and abusive e-mail). Спам являє собою множинні повідомлення електронної пошти рекламного або порнографічного характеру, а також повідомлення іншого змісту, що використовуються, як правило, для введення в оману з метою подальшого вчинення шахрайства. До істотних ознак спаму також відносять те, що подібні листи отримувач або не замовляв, або не може відмовитися від їх отримання надалі.

Отже, розповсюдження спаму, як правило, полягає в надсиланні великій кількості адресатів повідомлень, які вони не замовляли. Суспільна небезпечність такого діяння має певну специфіку. З точки зору конкретного користувача матеріальні збитки від розповсюдження спаму незначні, вони врешті-решт зводяться до оплати Інтернет-послуг, пов'язаних з отриманням зайвої кореспонденції. Однак з точки зору провайдерів, організацій, що надають послуги доступу до Інтернету, спам є досить небезпечним явищем, оскільки його наявність створює зайве, некорисне навантаження обладнання й ускладнює роботу інформаційної системи. Ще одним показником суспільної

небезпечності спаму є втрати робочого часу працівників підприємств, установ та організацій, які використовують Інтернет у своїй роботі. Зазначимо, що за даними компанії "Ашманов і Партнери", яка є провідним виробником антиспамерського програмного забезпечення в Росії, обсяг спаму в російському поштовому інтернет-трафіку у 2004 році склав 75 – 80%, а збитки від його розповсюдження – мінімум 250 мільйонів євро [17]. За даними наукового підрозділу компанії Websense Inc., у серпні 2010 року серед усього обсягу електронної кореспонденції спам склав 82,2%, в абсолютних цифрах 3,62 мільярдів (!) листів [414]. І хоча доля національного сегменту в цьому інформаційному потоці невелика, але з великою ймовірністю можна прогнозувати, що подібні проблеми очікують українських користувачів мережі Інтернет і провайдерів у найближчому майбутньому. Чи готове українське законодавство до цього?

На жаль, на це питання неможливо відповісти позитивно. Стаття 363-1 КК України передбачає відповідальність за масове розповсюдження повідомлень електрозв'язку, однак кримінальна відповідальність у разі вчинення таких дій настає тільки тоді, коли спричинено наслідки у вигляді порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Як уже зазначалося, розповсюдження спаму, як правило, не призводить до таких наслідків. Ситуація, коли в результаті масового розповсюдження повідомлень електрозв'язку настають зазначені наслідки, є винятковою. Порушення або припинення роботи засобів опрацювання інформації слід віднести до абсолютно нетипових наслідків розповсюдження спаму. Тому приклад, який наводився в главі, присвяченій аналізу складу злочину, передбаченого ст. 363-1 КК, можливо, є єдиною ситуацією, коли ця норма "спрацьовує". Отже, маємо констатувати, що інформаційні суспільні відносини через недосконаліть статті 363-1 КК України практично не захищені від посягань, пов'язаних із розповсюдженням спаму. "Звичайне" розповсюдження спаму не можна кваліфікувати за цією нормою, оскільки воно не призводить до наслідків,

зазначених у статті 363-1 КК. Тому до недоліків чинного кримінального законодавства треба віднести і його недостатню ефективність у протидії такій майбутній інформаційній загрозі, як спам.

Наведений висновок підтверджується також зіставленням показників судової статистики та фактичних даних щодо діяльності українських спамерів. Так, згідно з інформацією Державної судової адміністрації, у 2007 – 2008 рр. суди не розглядали кримінальних справ про злочини, передбачені ст. 363-1 КК [73]. У подальшому ситуація докорінно не змінилася. Водночас, за даними міжнародної громадської організації The Spamhaus Project, серед 10 найнебезпечніших спамерів світу налічується 3 особи, діяльність яких пов'язують з Україною [424]. Крім цього, відповідно до висновків, зроблених експертами цієї організації, близько 80% світового спаму слід пов'язувати з однією сотнею встановлених спамерів, дані про них об'єднані в спеціалізованій базі даних The Register of Known Spam Operations (ROKSO). Українців у цій сотні четверо. Інакше кажучи, існує чотири особи або групи осіб, які здійснюють масові розсилки з території України у світовому масштабі [423]. Тобто Україна й українці є вельми помітними учасниками процесів, пов'язаних із розповсюдженням спаму, але ця тенденція не знаходить відображення в практиці українських судів.

Переходячи до пропозицій щодо вдосконалення чинного законодавства з питань протидії спаму, зазначимо, що далеко не всі дослідники вважають його криміналізацію доцільною. Так, Н.В. Кушакова-Костицька звертає увагу на невідповідність тяжкості злочину санкціям, які містить ст. 363-1 КК. На її думку, необхідно "ввести кримінальну відповідальність за розповсюдження інформації про алкогольні, тютюнові вироби, харчову та іншу продукцію, шкідливу для здоров'я, та інші види реклами, яка має в цілому негативний характер у сенсі психічного і фізичного здоров'я як окремих громадян так і нації в цілому" [200, с. 111 – 112]. Ці пропозиції, безсумнівно, заслуговують на розгляд, але не в контексті злочинів у сфері

використання інформаційних технологій. Вони відносяться до аналізу кримінально-правових засобів охорони суспільних відносин щодо формування інформаційного ресурсу, які ми будемо розглядати в наступній главі. Стосовно ж спаму як злочину у сфері використання інформаційних технологій позиція дослідниці очевидна: саме по собі масове розповсюдження повідомлень електрозв'язку не становить суспільної небезпечності.

Російські дослідниці І.Ю. Богдановська та Є.К. Волчинська справедливо зазначають, що діяльність з розсилання повідомлень, які адресат не запитував, збирання електронний поштових адрес, розроблення спеціалізованого програмного забезпечення, яке дозволяє приховати джерело розсилання, перетворилася на ефективний бізнес. "Цей бізнес є вигідним для виробників товарів і послуг, оскільки являє собою достатньо економічний спосіб прямого маркетингу, що охоплює величезну аудиторію за мінімальних витрат. Однак права та інтереси інших учасників правовідносин (операторів зв'язку, отримувачів повідомлень – споживачів послуг зв'язку) при цьому порушуються" [27, с. 33]. Ураховуючи таку особливість, дослідниці вважають, що доцільно обмежитися внесенням змін до законодавства про зв'язок та щодо використання персональних даних (номерів телефонів, адрес e-mail тощо). При цьому пропозиція щодо встановлення кримінальної відповідальності за розсилання спаму, на їхню думку, є "не виправданою як з точки зору суспільної небезпечності такого діяння, так і з позицій загальної лібералізації та гуманізації вітчизняного законодавства" [27, с. 34]. Разом із тим, дослідницям, як видається, вдалося сформулювати дуже перспективне в плані побудови стратегії правового регулювання спаму положення: "розповсюдження спаму – це бізнес". За результатами досліджень Асоціації прямого маркетингу та ORC International, у США завдяки спаму продається товарів на суму близько $11,7 млрд. Наприклад, у 2003 році комерційні повідомлення електронної пошти сприяли здійсненню 36% усіх покупок американців у грошовому еквіваленті [8]. Будь-який економіст скаже, що такі показ-

ники вимагають розгляду питання про спам не в контексті заборони, а з метою регулювання. Відповідно, і криміналізація спаму не може розглядатись окремо від його соціально корисної функції.

Ураховуючи зазначене, а також беручи до уваги здійснений під час дослідження аналіз одного з найбільш прогресивних у цій сфері законодавчих актів (Controlling the Assault of Non-Solicited, Pornography and Marketing Act (U.S.A. CAN-SPAM Act) [400]) та практики його застосування (додаток 4), можна зробити висновок про те, що правове регулювання масового розповсюдження повідомлень електрозв'язку слід уважати таким, що відповідає соціальному змістові та значенню явища тільки тоді, коли: 1) масове розповсюдження повідомлень електрозв'язку не розглядається однозначно як протиправна діяльність; 2) на рівні нормативно-правових актів установлюються правила здійснення подібних розсилань як певного виду господарської діяльності; 3) комплекс правових заходів з протидії негативним наслідкам масових розсилань являє собою норми, які встановлюють відповідальність за порушення таких правил; 4) диференціація цих правових заходів здійснюється за ступенем суспільної небезпечності наслідків масового розповсюдження зазначених повідомлень.

У цьому контексті розглянемо, як регулюється діяльність щодо розповсюдження спаму нормами національного законодавства. У Правилах надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України від 09.08.2005 р. № 720, під спамом розуміються незамовлені попередньо споживачами електронні повідомлення, які або є масовими, або в яких не наведено достовірних відомостей про повну назву, власну поштову чи електронну адресу замовника чи відправника цих повідомлень, або подальше отримання яких споживач не може припинити шляхом інформування про це замовника чи відправника. Правила містять норми щодо порядку надання та використання інтернет-послуг, серед яких наявні заборони замовляти, пропонувати розсилання або розсилати спам. Крім цього забороняється викорис-

товувати мережеві ідентифікатори інших осіб, фальсифікувати мережеві ідентифікатори, використовувати неіснуючі мережеві ідентифікатори.

Тобто в загальних рисах українське законодавство містить норми, подібні до розглянутого американського закону. Разом із тим, слід визнати, що на рівні матеріальних норм, які стосуються регулювання порядку надання й отримання телекомунікаційних послуг, українське законодавство є значно жорсткішим ніж американське. Якщо останнє в певних випадках дозволяє розсилання кореспонденції, яку не замовляв отримувач, то національне її однозначно забороняє. Національне законодавство об'єднує два вищеназвані підходи до регулювання спаму, установлюючи одночасну заборону двох типів: як "opt in", так і "opt out". Однак засобів забезпечення цих вимог українське законодавство не містить. Уявімо собі, що Роберт Соловей (додаток 4) розгорнув свою діяльність в Україні. До нього можна було б застосувати норми про відповідальність за шахрайство та відмивання грошей, але стосовно порушення суворих національних вимог щодо розповсюдження спаму та правової оцінки наслідків від його діяльності українська юстиція мала б розвести руками. Дійсно, ініційоване ним розсилання було б порушенням згаданих вище Правил надання та отримання телекомунікаційних послуг: повідомлення, які він надсилав, не містили достовірних відомостей про відправника, отримувачі їх не замовляли та відмовитися від них не могли. Проте відповідальність за порушення цих правил настає тільки в разі "здійснення дій, що призвели до зниження якості функціонування телекомунікаційних мереж" (ст. 148-1 КУпАП). Такі наслідки не були властиві діяльності Соловея. Навпаки, реальні небезпечні наслідки були пов'язані з тим, що через функціонування мережі в режимі масового розповсюдження повідомлень ускладнювалося користування електронною поштою. Використання ст. 363-1 КК України в цьому випадку теж було б неможливим, оскільки наслідки, що характеризували діяльність Соловея, не призводили до "порушення або припинення

роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку".

Крім цього, розгляд ст. 363-1 КК у контексті нормативних вимог до надання чи отримання телекомунікаційних послуг дозволяє встановити ще одну ваду цієї норми. Вона полягає в тому, що кримінальний закон не повністю відповідає матеріальним нормам, які встановлюють правила користування послугами направлення повідомлень. Оскільки діяння як ознака складу злочину, передбаченого цією нормою, полягає в масовому розповсюдженні повідомлень електрозв'язку, здійсненому без попередньої згоди адресатів, то масове розповсюдження замовлених повідомлень, але таких, що мають викривлені дані про відправника або не містять можливості відмовитися від подальшого їх отримання, не утворюватиме ознак злочинного діяння, хоча й заборонене Правилами отримання телекомунікаційних послуг. Тобто невідповідність матеріальних та охоронних норм призводить до неефективності правого регулювання розгляданої сфери суспільних відносин. Разом із тим, настільки суворі вимоги національного законодавства щодо здійснення масових розсилань (ідеться насамперед про заборону повідомлень, які отримувач не замовляв), хоча й не підкріплені охоронними нормами, усе ж таки мають, як видається, негативне суспільне значення. Наявність таких норм виключає можливість розвитку відповідних видів господарської діяльності, оскільки значно звужує її правове поле. Ті види комерційної діяльності, які американський законодавець намагається цивілізувати, розвинути, аби забезпечити, урешті-решт, певне підвищення рівня національної економіки, відповідно до нашого законодавства є неможливими через однозначну заборону.

Таким чином, розв'язання проблеми кримінальної відповідальності за розсилання масових телекомунікаційних повідомлень передбачає передусім установлення чітких правил здійснення подібної діяльності. Уважаємо за доцільне, щоб ці

правила були орієнтованими не тільки на електронну пошту, а й на інші види зв'язку, наприклад SMS-повідомлення. При цьому зміст нормативних вимог, на нашу думку, не повинен бути настільки жорстким, як це передбачає чинне законодавство. Нормативні приписи мають створювати стимули та надавати можливості для розвитку леґального масового розсилання повідомлень електрозв'язку, оскільки воно, як свідчить світова практика, набуває значення важливого для економіки держави каналу постачання даних до користувачів товарів і послуг. З набранням такими правилами чинності доцільно встановити кримінальну відповідальність за їх порушення.

Отже, стосовно дотримання принципу ***відсутності прогалин та ненадлишковості заборони*** при криміналізації злочинів у сфері використання комп'ютерної техніки та мереж електрозв'язку маємо зазначити таке:

1. Чинна редакція ст. 361-2 дозволяє говорити як про надлишковість сформульованої в ній заборони, так і про формування цією нормою певних прогалин у законодавстві. Надлишковість стосується криміналізації діянь, які не можна визнавати суспільно небезпечними в контексті інших норм щодо відповідальності за незаконні дії з інформацією з обмеженим доступом. Прогалини пов'язані з невдалим формулюванням ознак предмета, які значно звужують можливості норми, роблять передбачені нею кримінально-правові засоби такими, що не відповідають сучасним потребам протидії злочинам у сфері використання інформаційних технологій.

2. Конструкція об'єктивної сторони ст. 361 КК України зумовлює прогалини, що полягають у неможливості притягнення до кримінальної відповідальності осіб, які заподіюють зазначені в нормі суспільно небезпечні наслідки без вчинення передбаченого в нормі діяння.

3. Певні прогалини створює законодавче визначення суб'єкта злочину, передбаченого ст. 363 КК, яке не відповідає можливим формам об'єктивної сторони цього посягання. Також неефективність розгляданої норми зумовлена недоліками за-

конодавчого регулювання використання засобів захисту інформації.

4. Прогалини мають місце при формулюванні кримінально-правової заборони масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК). Вони полягають у тому, що відповідальність за розповсюдження спаму пов'язана з наслідками, які є абсолютно нетиповими для подібних дій, а отже, переважна більшість випадків розповсюдження спаму не підпадають під ознаки злочину, передбаченого цією нормою. Недосконалим, таким, що зменшує ефективність кримінально-правової охорони, є також матеріально-правове регулювання множинного розсилання телекомунікаційних повідомлень.

4.3. Суспільна небезпечність посягань у сфері використання інформаційних технологій як чинник їх криміналізації

Разом з наявністю прогалин, невизначеністю та відсутністю єдності у застосуванні термінології, порушеннями принципу повноти складу чинне законодавство про кримінальну відповідальність за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку характеризується також певними порушеннями принципу ***суспільної небезпечності.***

Так, до порушення принципу суспільної небезпечності слід віднести *недоліки диференціації відповідальності залежно від заподіяної шкоди*. Як ми вже зазначали, досліджувані норми містять кваліфікуючу ознаку "заподіяння значної шкоди". Згідно з приміткою до ст. 361 вона визнається такою, якщо в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян. Водночас однаковими з точки зору кваліфікації будуть, наприклад, несанкціоноване втручання, що завдало матеріальних збитків у розмірі 120 неоподатковуваних мінімумів доходів громадян, і несанкціоноване втручання, що завдало збитків у розмірі 520 неоподатковуваних мінімумів доходів гро-

мадян, або несанкціоноване втручання, що призвело до порушення роботи світлофорів у певному мікрорайоні, та несанкціоноване втручання, що призвело до порушення роботи системи радіаційної безпеки АЕС. Саме тому для подальшого вдосконалення законодавства актуальним є питання про відбиття *диференціації тяжкості заподіяної шкоди* в конструкції складів комп'ютерних злочинів.

Не можна не звернути уваги на те, що законодавець у нормах Особливої частини КК по-різному визначає шкоду, заподіювану тим чи іншим злочином: в одних випадках він говорить про істотну (значну) шкоду, а в інших – про тяжкі наслідки. При цьому аналіз цих норм дозволяє зробити висновок, що законодавець (у переважній більшості складів) пов'язує істотну шкоду саме з матеріальними збитками. Що ж стосується інших видів шкоди, то здебільшого їх характеризують як тяжкі наслідки.

Так, у ряді складів законодавець прямо вказує на це в приміткаx до статей (наприклад ст. 185 "Крадіжка"). Виходячи з аналізу об'єкта й об'єктивної сторони конкретного складу, можна також констатувати, що істотна шкода виражається саме в матеріальних збитках (наприклад ст. 222 "Шахрайство з фінансовими ресурсами", ст. 223 "Порушення порядку випуску (емісії) та обігу цінних паперів").

Що ж стосується тяжких наслідків, то це, як випливає з аналізу Особливої частини КК, більш широке поняття, яке охоплює не тільки заподіяння матеріальних збитків, про що свідчить той факт, що в ряді випадків законодавець визнає завдання істотної чи значної шкоди кваліфікуючою ознакою, а настання тяжких наслідків – особливо кваліфікуючою ознакою (наприклад ст. 424 "Перевищення військовою службовою особою влади чи службових повноважень"). Також у ряді статей (наприклад ст. 294 "Масові заворушення", ст. 414 "Порушення правил поводження зі зброєю, а також із речовинами і предметами, що становлять підвищену небезпеку для оточення") законодавець формулює досліджувану ознаку в такий спосіб:

заподіяння загибелі людей або настання інших тяжких наслідків. Це так само підтверджує висновок про те, що тяжкі наслідки – це більш широке поняття, яке містить у собі не тільки завдання матеріальних збитків.

Отже, характеристика можливих наслідків комп'ютерних злочинів дозволяє стверджувати, що доцільним, обґрунтованим і таким, що відповідає специфіці об'єкта й об'єктивної сторони, було б доповнення статей розділу XVI КК України відповідними частинами, які б крім кваліфікуючої ознаки "заподіяння значної шкоди" передбачали таку особливо кваліфікуючу ознаку, як заподіяння тяжких наслідків. При цьому в примітці до ст. 361 необхідно зазначити, що в статтях розділу XVI під значною шкодою, якщо вона полягає в завданні матеріальних збитків, слід розуміти таку шкоду, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян. У свою чергу, до тяжких наслідків, якщо вони полягають у заподіянні матеріальних збитків, належить шкода, яка у п'ятсот і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Певне зменшення ефективності кримінально-правових засобів охорони інформаційних суспільних відносин зумовлене *відсутністю* в нормах розділу спеціальної вказівки на можливість так званої *змішаної повторності*. Узагалі повторність обґрунтовано визнається ознакою, що підвищує суспільну небезпечність вчиненого, а тому враховується як обтяжуюча обставина при призначенні покарання (п. 1 ст. 67 КК), а у випадках, передбачених статтями Особливої частини, – як кваліфікуюча ознака. Така ознака міститься і в ст.ст. 361, 361-1, 361-2, 362 та 363-1 КК України.

У науці та практиці поняття повторності тлумачилося неоднозначно. Тому, безперечно, позитивним є те, що новий КК України в ч. 1 ст. 32 дав визначення цього поняття, згідно з яким повторністю злочинів визнається вчинення двох або більше злочинів, передбачених тією самою статтею або частиною статті Особливої частини КК. Відповідно до цього

комп'ютерний злочин, передбачений однією зі згаданих статей, слід уважати вчиненим повторно тільки у випадках, коли особа два або більше разів вчинила злочин, передбачений однією й тією самою статтею.

Аналізуючи загальне поняття повторності, не можна не сказати, що воно значно обмежує можливість урахування підвищеної суспільної небезпечності комп'ютерного злочину, який вчиняється не після тотожного, а після однорідного злочину. Законодавець у ч. 3 ст. 32 КК України передбачає можливість визнання повторним певного злочину за наявності змішаної повторності, тобто вчинення двох або більше злочинів, передбачених різними статтями КК, якщо таку повторність спеціально передбачено в статтях Особливої частини КК.

Отже, при подальшому вдосконаленні кримінального законодавства про комп'ютерні злочини доцільно передбачити можливість змішаної повторності. Таке доповнення дало б змогу під час кваліфікації чітко враховувати суспільну небезпечність посягання, визнавати повторними комп'ютерні злочини не тільки в разі їх вчинення після тотожного, але й після однорідного, передбаченого вищезазначеними статтями.

Проте *основним недоліком чинної системи кримінально-правових засобів охорони суспільних відносин інформаційної безпеки у сфері використання інформаційних технологій слід визнати відсутність достатніх нормативних критеріїв суспільної небезпечності посягань, передбачених ст.ст. 361 – 363-1 КК.* На початку цієї глави ми зауважили, що необхідно встановити, чи враховано визначені нами особливості соціальних потреб у кримінально-правовій охороні від посягань у сфері використання інформаційних технологій при криміналізації злочинів, які об'єднуються в розділі XVI КК України. Проведений нами аналіз складів цих злочинів, а також критеріїв відмежування їх від суміжних свідчить про те, що відповідь має бути радше неґативною.

Раніше йшлося, що суспільна небезпечність злочинів у сфері використання комп'ютерної техніки головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології.

Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це й визначає суспільну небезпечність конкретного посягання у сфері використання інформаційних технологій. Однак для настання кримінальної відповідальності за більшість злочинів, передбачених у розділі XVI КК, установлення таких характеристик суспільно небезпечних наслідків не є обов'язковим. Судячи з прийнятого законодавцем рішення, витік, втрата, підроблення, блокування інформації, порушення встановленого порядку її маршрутизації або спотворення процесу її обробки (ст. 361, 362) визнаються суспільно небезпечними самі по собі. Так само суспільно небезпечними, на думку законодавця, є просте розповсюдження або збут шкідливого програмного або технічного забезпечення (ст. 361-1), розповсюдження або збут комп'ютерної інформації з обмеженим доступом (ст. 361-2) тощо. Лише в диспозиції ч. 1 ст. 363, других частин статей 361, 361-1, 361-2 та 363-1, а також ч. 3 ст. 362 ми знаходимо законодавчі положення, адекватні визначеній специфіці суспільної небезпечності досліджуваних злочинів. Ідеться про наявність такої ознаки об'єктивної сторони складів злочинів, передбачених означеними нормами, як настання значної шкоди. Наявність цієї ознаки вимагає встановлення тих суспільних відносин, у межах яких використовуються інформаційні технології та яким заподіюється шкода внаслідок посягань, які ми називаємо "комп'ютерними" злочинами. Саме ці суспільні відносини й характеризують реальну суспільну небезпечність посягань у сфері інформаційних технологій. Знищення інформації, її спотворення чи блокування, якщо розглядати їх самостійно, а не в контексті згаданих суспільних відносин, не може вважатися суспільно небезпечним.

Неповна відповідність чинного законодавства означеній специфіці суспільної небезпечності комп'ютерних злочинів зумовлює появу певних неґативних тенденцій у практиці застосування норм про кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж та мереж елек-

трозв'язку. З метою їх установлення ми дослідили відповідну категорію кримінальних справ (додаток 5). Головний висновок дослідження полягає в тому, що практика національних судів містить рішення, у яких застосування кримінальної відповідальності до осіб, які вчиняли комп'ютерні злочини, було пов'язане з посяганнями, які дійсно є суспільно небезпечними (43,71 %); разом із тим, більше половини судових рішень досліджуваної категорії (56,29%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є досить спірним.

Для інтерпретації результатів дослідження необхідним є звернення до результатів наукових досліджень з питань ефективності кримінально-правових засобів протидії.

Загально визнаним є те, що кримінальне право являє собою систему норм, яка існуючими в ньому та використовуваними ним засобами здатна визначати й легітимізувати право державної влади та спеціально уповноважених державних органів на застосування найбільш жорсткого насильства [95, с. 6]. При цьому воно має завжди розглядатися як ultima ratio (останній засіб) у державних можливостях впливу на значні негативні події в суспільстві [325, с. 81]. Можливість збереження соціальних цінностей, які потребують захисту, без застосування кримінального покарання в принципі виключає легітимність кримінально-правової заборони.

Ключовою категорією для прийняття рішення щодо легітимізації певного кримінального закону є суспільна небезпека. Саме її ретельне дослідження в процесі нормотворчості та правозастосування дозволяє обмежити використання кримінальної юстиції дійсно необхідними випадками та уникнути формалізму, який не має матеріально-правових передумов [95, с. 112-120]. Як правильно зауважив В.К. Грищук, ефективність законодавства про кримінальну відповідальність значною мірою залежить від аргументованості й послідовності розв'язання такого питання: "Чи доцільно забороняти певне діяння людини під загрозою покарання і якою у зв'язку з цим має бути теоретико-прикладна модель норми (норм) закону про кримі-

нальну відповідальність?" [74]. Використання можливостей кримінального правосуддя у випадках, що не пов'язані з дійсно суспільно небезпечними посяганнями, А.Е. Жалінський називає "зловживанням кримінальним правом" [95, с. 112-120]. У зв'язку з цим заслуговує на увагу позиція А.А. Музики, який вводить у науковий обіг поняття "кримінально-правові ризики", які, на його думку, являють собою наслідки браку системності в правотворчості, а також непрофесійного застосування законодавства, відсутності знань про тлумачення закону і навичок у цій справі. Слід погодитися з дослідником у тому, що прорахунки законотворчої роботи на рівні правозастосовчої діяльності нерідко трансформуються в неправильну кваліфікацію певних видів суспільно небезпечних діянь, надмірно суворі або невиправдано м'які вироки, необґрунтовані рішення щодо звільнення від кримінальної відповідальності [237, с. 100 – 101].

Застосування кримінального права є завжди видатковим. Причому видатки мають не лише матеріальний характер. Вони також виявляються й у криміналізації суспільства, певних демографічних та соціально-культурних наслідках. Тому оптимальний стан кримінального права, такий, якого слід добиватися, визначається його відповідністю до реальних соціальних потреб, відповідністю соціальних видатків на його реалізацію до значимості та захищеності охоронюваних благ [95, с. 3]. Такий стан досягається в тому числі й раціональним (економічним) підходом, який передбачає верифікацію кожного рішення з позицій балансу соціальних видатків і результатів. Основною метою раціонального підходу є мінімізація соціальних витрат, оптимізація результатів дії кримінального права [95, с. 130].

Розглядаючи з цих позицій фактичний стан речей у правотворчості й правозастосуванні, А.Е. Жалінський зауважує, що сучасний стан кримінального права слід характеризувати як кризу. Така оцінка сучасному кримінальному праву дається переважно в зарубіжних наукових джерелах та стосується кримінального права зарубіжних країн, але ситуація, що скла-

лася у сфері кримінальної юстиції РФ, дозволяє дослідникові зробити аналогічний висновок і щодо російської кримінальної політики. Основним індикатором кризи є зростання злочинності при інфляції кримінальної правотворчості та зростаючих видатках суспільства.

Ознаки кризи кримінального права в роботах європейських авторів дослідник класифікує, як він зазначає, "дещо умовно", на соціальні та власне правові.

Перша група – соціальні ознаки кризи кримінального права. До них належить, зокрема, одночасне зростання кількості обвинувальних вироків і вчинюваних злочинів, що означає невідповідність соціальних витрат соціальним результатам, або, простіше, що публічна влада, здійснюючи делеговане їй право на насильство, не забезпечує при цьому безпеки суспільства. Далі, швидке зростання прямих витрат на підтримку реалізації кримінального закону, тобто на розшук, розслідування, судову діяльність, виконання вироку, а також непрямих витрат, що утворюються підвищенням трансакційних витрат суб'єктів соціальних стосунків. Усе це завдає величезної шкоди суспільству, впливаючи на його моральну свідомість, динаміку демографічних процесів, здоров'я населення, економічну ефективність.

Друга група – правові ознаки кризи. Це інфляція кримінального законодавства: невмотивоване розширення предмета кримінально-правової дії та посилення відповідальності, зниження технічного рівня кримінального законодавства, пов'язане з втратою визначеності кримінального закону та зростанням недіючих норм [95, с. 116].

"Подібні явища з більшою або меншою інтенсивністю характерні і для російського кримінального права" [95, с. 116], – зауважує дослідник. Не претендуючи на висновки стосовно національного кримінального права в цілому, маємо зазначити, що кримінально-правова протидія злочинам у сфері використання комп'ютерної техніки та мереж електрозв'язку характеризується доволі значним потенціалом подібних кризових явищ.

Ураховуючи проведене дослідження матеріалів судової практики та інтерпретуючи його в контексті парадигми раціонального використання кримінального права, навряд чи можливо прогнозувати позитивні соціальні результати застосування кримінального законодавства про "комп'ютерні" злочини. Наприклад, не можна казати, що застосування кримінального права є адекватним засобом забезпечення соціальної потреби у функціонуванні інформаційних технологій, коли більш ніж третина вироків, пов'язаних із застосуванням ст. 361 КК, являють собою засудження за несанкціоноване підключення до телевізійної або телефонної мережі. Навряд чи можна казати про ефективну протидію розповсюдженню шкідливих програм, коли 53,33 % вироків, пов'язаних із застосуванням ст. 361-1 КК, являють собою засудження за збут дисків із копіями комп'ютерних вірусів – принципово застарілу та непоширену форму розповсюдження подібної продукції в реальній дійсності. Узагалі сумнівною, особливо в системі "видатки – результат", видається ефективність застосування законодавства про кримінальну відповідальність за злочини у сфері інформаційних технологій, коли понад 50 % судових рішень пов'язані з кримінально-правовою оцінкою діянь, суспільна небезпечність яких є спірною. Додаткових аргументів для таких висновків додає й значна частина вироків, у яких покарання призначається з випробуванням (70,66%). Така ситуація свідчить про доцільність обговорення питань щодо віднесення подібних посягань до числа адміністративних проступків й активнішого залучення засобів адміністративно-правового впливу. Не може не викликати занепокоєння й наявність судових рішень, у яких за відсутності доведеної матеріальної шкоди витрати тільки на проведення експертизи становлять більше 10 000 гривень [169, 148, 165].

Ще раз зазначимо, ми не оцінюємо стан сучасної національної судової практики як кризовий. Зважаючи на доволі незначну частку відповідних вироків розглядані проблемні аспекти "не дотягують" навіть до рівня тенденції. Разом із тим, їх наявність є чітким індикатором потенційних проблем у цій сфері, свідчить про недопустимість розвитку законодавства та

практики його застосування в такому напрямку та, безсумнівно, вимагає прийняття відповідних заходів.

Важко не погодитися з А.Е. Жалінським у тому, що кримінально-правова теорія з урахуванням особливостей сучасної соціальної ситуації має розвиватися так, щоб національне кримінальне право розумілося як соціальний інструмент, котрий є жорстко підконтрольним суспільству, ураховує його реальний стан, націлений на задоволення його дійсних, а не уявних потреб і вживаний максимально раціонально.

Серед пріоритетних напрямів роботи дослідник називає проблему внутрішньогалузевих ґарантій, що перешкоджають зловживанню кримінальним правом. У зв'язку з цим він наполягає на необхідності пошуку можливостей підвищення визначеності кримінального закону та забезпечення передбачуваності його застосування. При цьому увага звертається на те, що інфляція кримінального законодавства спостерігається "особливо стосовно так званих нових злочинів (наприклад, відмивання брудних грошей, деяких спеціальних заборон шахрайства в економічній сфері тощо)". А.Е. Жалінський справедливо зазначає, що формально заборонити можна будь-який поведінковий акт і будь-який комплекс поведінкових актів. Формулювання кримінальної протиправності – справа переважно законодавчої техніки. "Складніше відповісти на питання: чому, які діяння, для чого їх треба заборонити, що, які соціальні блага треба охороняти? Якщо на ці питання отримано правильні відповіді, кримінальний закон відповідає загальному благу, якщо ні – він шкідливий, і дуже сильно… Нерідко законодавець … приймає кримінально-правову заборону, маючи на увазі дійсно непереносні, небезпечні діяння. Але матеріально, предметно дії, охоплені приписом кримінального закону, дуже відрізняються. Особливо часто виникає розрив між намірами та реальністю при прийнятті нових кримінально-правових заборон, коли не цілком є зрозумілим характер поведінки, що забороняється, і законодавець відмовляється від вказівки на його матеріальні ознаки" [95, с. 336]. Використовуючи влучне українське прислів'я: "Не так сталося, як гадало-

ся", мусимо визнати, що в подібній ситуації опинився й український законодавець, приймаючи рішення про встановлення кримінально-правових заборон у сфері використання інформаційних технологій. Не приймати їх було неможливо, оскільки темпи інформатизації свідчили про необхідність відповідних правових ґарантій. Водночас було недостатньо досліджено реальну небезпечність відповідних посягань і соціальні потреби у сфері використання інформаційних технологій.

Для характеристики подібних ситуацій доречним буде використання запропонованого А.А. Музикою поняття "кримінально-правовий ризик". Очевидно, що подолання розгляданих проблем полягає в підвищенні визначеності закону про кримінальну відповідальність. У процесі кримінальної правотворчості обов'язково повинні виявлятися й фіксуватися мовою кримінального закону ознаки реальної суспільної небезпеки. Тоді закон "програмуватиме" діяльність органів кримінальної юстиції на встановлення фактичного змісту суспільної небезпечності конкретних посягань, забезпечуватиме дієве й раціональне використання кримінально-правових засобів, саме як ultima ratio.

Таким чином, дослідження кримінальних справ, пов'язаних із застосуванням ст.ст. 361 – 362 КК України, дозволяє стверджувати про недостатню ефективність кримінально-правових засобів у сфері використання інформаційних технологій. Більшість досліджених вироків не можуть розглядатися як засіб протидії суспільно небезпечним явищам у цій сфері. При цьому непослідовність проаналізованих судових рішень не в останню чергу зумовлена прогалинами в чинному кримінальному законодавстві, відсутністю в ньому чітких, зрозумілих критеріїв суспільної небезпечності посягань у сфері використання інформаційних технологій. Маємо зазначити, що при криміналізації злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку *було порушено принцип суспільної небезпечності*. Сутність цього порушення можна сформулювати таким чи-

ном: *через відсутність у законодавчих визначеннях злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку чітких критеріїв суспільної небезпечності під кримінально-правову заборону та, відповідно, до сфери впливу кримінальної юстиції потрапляють не тільки ті діяння, які дійсно є суспільно небезпечними, але й ті, які такими не є*. Це різко негативно відбивається на ефективності кримінально-правової охорони інформаційної безпеки у сфері використання інформаційних технологій.

Для виправлення ситуації насамперед необхідно включити до диспозицій відповідних кримінально-правових норм чіткі та прозорі положення щодо критеріїв суспільної небезпечності посягань.

Звернімо увагу на те, що результати здійснених дисертаційних і монографічних досліджень з проблематики кримінальної відповідальності за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку також, на жаль, не містять пропозицій щодо законодавчого визначення специфіки їх суспільної небезпечності. Так, Н.А. Розенфельд пропонувала передбачити кримінальну відповідальність за "незаконне втручання в роботу комп'ютерних систем, що призвело до витікання, перекручення або знищення комп'ютерної інформації", а також за "умисне розповсюдження комп'ютерного вірусу або інших шкідливих комп'ютерних програм, призначених для незаконного проникнення в комп'ютерні системи і здатних спричинити перекручення або знищення комп'ютерної інформації або її носіїв". Лише кваліфікуючою ознакою як першого, так і другого посягання пропонувалося передбачити настання істотної шкоди [301, с. 195].

С.О. Орлов за результатами проведеного дисертаційного дослідження запропонував такі законодавчі визначення злочинних посягань у сфері використання комп'ютерної та телекомунікаційної техніки:

1) "незаконне втручання в роботу комп'ютерних систем чи телекомунікаційних мереж, що призвело до перекручення, пе-

рехоплення, копіювання, знищення або блокування інформації в цих системах чи мережах";

2) "створення з метою розповсюдження чи збуту, збут чи розповсюдження програмних або технічних засобів, призначених для незаконного втручання в комп'ютерні системи чи телекомунікаційні мережі";

3) "порушення правил експлуатації комп'ютерних систем чи телекомунікаційних мереж особою, що відповідає за їх експлуатацію, якщо це спричинило незаконне перекручення чи знищення комп'ютерної інформації, засобів їх захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких систем чи мереж".

Знову ж таки в частині другій статей, які мають передбачати відповідальність за ці діяння, він пропонував передбачити кваліфікуючу ознаку "заподіяння значної шкоди" [254, с. 188 – 189].

Д.С. Азаров запропонував проект закону про внесення змін і доповнень до Кримінального кодексу. Як ми зауважували раніше, для найменування досліджуваних злочинів він використовує спірний термін "Злочини у сфері комп'ютерної інформації" та пропонує відносити до них такі посягання:

1) "незаконні введення, зміна, пошкодження, знищення чи блокування комп'ютерної інформації в комп'ютерній системі чи телекомунікаційній мережі, або інший незаконний умисний вплив на процес обробки комп'ютерної інформації, що змінило результат такого оброблення";

2) "незаконні введення, зміна, пошкодження, знищення чи блокування комп'ютерної інформації у комп'ютерній системі чи телекомунікаційній мережі, або інше незаконне втручання в їх роботу, що перешкодило функціонуванню такої системи чи мережі";

3) "незаконні умисні зміна, пошкодження чи знищення комп'ютерної інформації";

4) "незаконний доступ до комп'ютерної інформації";

5) "незаконні копіювання чи перехоплення комп'ютерної інформації або інше незаконне заволодіння нею";

6) "створення шкідливих комп'ютерних програм з метою їх розповсюдження в комп'ютерних системах або телекомунікаційних мережах";

7) "умисне розповсюдження в комп'ютерних системах або телекомунікаційних мережах шкідливих комп'ютерних програм, що спричинило незаконні зміну, пошкодження, знищення, блокування інформації чи доступ до неї";

8) "незаконне умисне розповсюдження в комп'ютерних системах або телекомунікаційних мережах паролів, кодів доступу або інших даних, які призначені для отримання доступу до комп'ютерної інформації".

Так само, як і попередні дослідники, Д.С. Азаров висуває пропозицію передбачити лише кваліфікуючі ознаки, пов'язані із заподіянням шкоди у великому розмірі, особливо великому розмірі чи настанням тяжких наслідків [3, с. 259 – 263].

Вельми показовими є положення автореферату дисертації Т.В. Міхайліної. Дослідження присвячено аналізу питань кримінальної відповідальності за створення, розповсюдження або збут шкідливих програмних чи технічних засобів (ст. 361-1 КК). Авторка зазначає: "У підрозділі 1.1 "Соціально-економічні та правові передумови криміналізації створення з метою використання, розповсюдження або збуту, а також розповсюдження або збуту шкідливих програмних чи технічних засобів" аналізується історія виникнення та розвитку злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, розглядаються загальні кримінологічні ознаки злочинів цього виду, а також їх особливості в Україні" [235, с. 9]. На цьому опис результатів роботи з питань підстав криміналізації закінчується. Дослідивши таким чином соціально-економічні передумови криміналізації та, очевидно, дійшовши висновку про те, що розповсюдження шкідливих програм є суспільно небезпечним саме по собі, дослідниця запропонувала нову редакцію статті 361-1 КК. Основний склад злочину, передбаченого цією нормою, як і в решті розглянутих дисертаційних досліджень, не містить критеріїв суспільної небезпе-

чності. Разом із тим, частина друга містить кваліфікуючу ознаку "заподіяння значної шкоди", а третя – "загибель людей чи інші тяжкі наслідки" [235, с. 14 – 15].

Для формулювання нормативних визначень комп'ютерних злочинів, які б ураховували дійсну специфіку їх суспільної небезпечності, необхідно розглянути комплекс питань. Серед них головними є такі: 1) визначення видового об'єкта досліджуваних злочинів; 2) установлення системи їх безпосередніх об'єктів; 3) формулювання ознак об'єктивної сторони злочинів у сфері використання комп'ютерної техніки; 4) дослідження ознак суб'єктивної цих злочинів, які можуть свідчити про суспільну небезпечність посягання.

При цьому видається, що з урахуванням потреб у підвищенні нормативної визначеності кримінально-правових заборон у сфері використання інформаційних технологій найбільш оптимальним рішенням буде звернення до таких законодавчих конструкцій, які притаманні злочинам із похідними наслідками. Ґрунтовне дослідження цього виду злочинів здійснено Є.В. Шевченком [384]. Зупинимося на основних положеннях.

Головним критерієм, що дозволяє виділити цю групу діянь як самостійний вид одиничних злочинів, є наявність у них юридично значущих наслідків – проміжного (основного) і похідного (додаткового), що настають хронологічно (послідовно) один за одним у результаті вчиненого особою діяння. Розглядані злочини мають два безпосередні об'єкти – основний і додатковий. Додатковий об'єкт у цих деліктах завжди є обов'язковим. У зв'язку з тим, що в них мають місце як один, так і декілька додаткових об'єктів, ці діяння можуть бути як двохоб'єктними, так і поліоб'єктними. Причинний зв'язок у злочинах цього виду встановлюється окремо до кожного з наслідків: проміжного і похідного. При цьому визначальним тут є проміжний наслідок, який створює реальну загрозу настання наслідку похідного. Суб'єктивна сторона злочинів із похідними наслідками щодо діяння та проміжного наслідку характеризується тільки умисною формою вини. Стосовно похідних

наслідків суб'єктивна сторона таких злочинів має різні комбінації (поєднання) умислу та необережності: 1) об'єднання в межах одного делікту тільки умисного та необережного злочинів (умисел + необережність), тобто подвійна форму вини; 2) можливість вчинення злочину як у межах однієї – умисної форми вини (умисел + умисел), так і в межах двох різнорідних форм вини (умисел + необережність) – комбінована форма вини [384, с. 179 – 180]. Необхідно також зауважити, що можливими шляхами розвитку законодавства про кримінальну відповідальність за злочини з похідними наслідками Є.В. Шевченко вважає відповідні зміни законодавчих визначень злочинів у сфері використання інформаційних технологій [384, с. 54 – 56].

Таким чином, установивши потребу в підвищенні визначеності кримінально-правових засобів охорони інформаційної безпеки у сфері використання інформаційних ресурсів та використовуючи теоретичні положення щодо законодавчої конструкції злочинів із похідними наслідками, яка найбільше відповідає встановленій потребі, перейдемо до формулювання основних напрямів удосконалення відповідних правових норм.

Стосовно видового об'єкта маємо зауважити, що запропоноване в попередній главі визначення видається цілком обґрунтованим, таким, що достатньо чітко окреслює коло охоронюваних суспільних відносин. Разом із тим, як зазначалося раніше, певним недоліком чинного законодавства є використання переліку можливих засобів оброблення інформації. Відповідно, видовий об'єкт досліджуваних злочинів пропонується визначати як *суспільні відносини у сфері використання інформаційних технологій*. Застосований термін має чітке законодавче визначення. Закон України "Про національну програму інформатизації" від 4 лютого 1998 року визначає інформаційну технологію як цілеспрямовану організовану сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування. От-

же, зміст суспільних відносин, які пропонується визнавати видовим об'єктом, полягає у здійсненні інформаційних процесів, організованих з використанням сучасних засобів автоматизованої обробки інформації, для задоволення інформаційної потреби громадян, суспільства або держави. Важливим моментом характеристики видового об'єкта злочинів у сфері використання інформаційних технологій є визначення його місця в системі родового об'єкта – відносин, що становлять інформаційну безпеку України. Як ми зазначали, інформаційна безпека являє собою систему відносин щодо забезпечення реалізації інформаційної потреби. Цю систему складають відносини щодо надання доступу до інформаційних ресурсів, відносини щодо формування інформаційних ресурсів та відносини у сфері використання інформаційних технологій. Останні забезпечують можливість, швидкість, оперативність тощо перших двох. Це відбивається на механізмі заподіяння шкоди інформаційній безпеці посяганнями у сфері використання інформаційних технологій. Він полягає в тому, що зменшення або виключення можливості реалізації інформаційної потреби настає через неможливість формувати інформаційний ресурс або забезпечувати доступ до нього внаслідок посягань у сфері інформаційних технологій.

Зважаючи на зроблені вище термінологічні уточнення та пропозиції щодо усунення прогалин у забезпеченні кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій, до системи безпосередніх об'єктів досліджуваних злочинів пропонується включити: 1) суспільні відносини власності на комп'ютерні дані; 2) суспільні відносини щодо користування послугами електронної пошти; 3) суспільні відносини щодо забезпечення працездатності комп'ютерних систем та інших технічних засобів інформаційних технологій, організації та здійснення програмного, технічного й організаційного захисту комп'ютерних даних; 4) суспільні відносини надання та отримання телекомунікаційних послуг.

Зміст перших трьох видів суспільних відносин можна легко встановити з урахуванням висловлених раніше положень щодо права власності на комп'ютерну інформацію, а також соціальної зумовленості кримінальної відповідальності за порушення вимог інформаційної безпеки (у вузькому розумінні) та здійснення масових розсилань повідомлень електронної пошти. При цьому необхідність захисту суспільних відносин власності на комп'ютерні дані зумовлена широким використанням комп'ютерних систем для здійснення повноважень володіння, користування або розпоряджання цими даними. Норма про відповідальність за порушення вимог інформаційної безпеки необхідна як стимул дотримання правил застосування спеціальних заходів захисту комп'ютерних даних та, відповідно, підвищення ефективності попередження комп'ютерних злочинів. У свою чергу, відповідальність за порушення правил здійснення масових розсилань повідомлень електронної пошти зумовлена необхідністю протидії негативним соціальним проявам розповсюдження спаму.

Останній запропонований безпосередній об'єкт охоплює ті відносини у сфері використання інформаційних технологій, предметом яких виступають не комп'ютерні дані, а інші види інформації, передавання або отримання якої здійснюється з використанням телекомунікаційних мереж (телефонний стаціонарний або мобільний зв'язок, радіомовлення, ефірне чи кабельне телебачення тощо). Отже, як і в чинному законодавстві, ми використовуємо обмежувальне тлумачення терміна "телекомунікаційна мережа (мережа електрозв'язку)", до якого в контексті формулювання ознак складів злочинів у сфері використання інформаційних технологій ми не відносимо комп'ютерні мережі.

При цьому для нормативного відбиття специфіки суспільної небезпечності досліджуваних злочинів необхідно в досліджуваних складах передбачити систему додаткових обов'язкових об'єктів, які б відображали реальну суспільну небезпечність посягань у сфері використання інформаційних технологій. Ще раз зазначимо, що шкода, яка завдається суспільним

відносинам, котрі складають запропоновану сукупність основних безпосередніх об'єктів, не завжди є суспільно небезпечною. Аналіз соціологічних досліджень, законодавства та практики його застосування свідчить про необхідність визнавати суспільно небезпечними лише ті посягання у сфері інформаційних технологій, які завдають істотної шкоди суспільним відносинам, у межах яких використовувалась інформація, що є предметом посягання.

Як видається, про суспільну небезпечність посягань у сфері використання інформаційних технологій може свідчити заподіяння шкоди суспільним відносинам у сфері: реалізації прав, свобод або законних інтересів окремих фізичних осіб; реалізації державних чи громадських інтересів; нормальної діяльності юридичних осіб (установ, підприємств, організацій). Саме ці суспільні відносини і мають складати систему додаткових обов'язкових об'єктів досліджуваних злочинів.

Про необхідність передбачення як додаткового об'єкта суспільних відносин у сфері реалізації прав, свобод і законних інтересів свідчить визначення права на інформацію, що дається у відповідному законі [103]: "можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів". Закон абсолютно справедливо визнає суспільно значущою, такою, що потребує нормативного регулювання, не просто будь-яку діяльність щодо інформації, а діяльність у контексті реалізації прав, свобод і законних інтересів. Відповідно суспільно небезпечним слід уважати не просте, наприклад, знищення або перекручення інформації, а лише таке, що перешкоджає реалізації прав, свобод і законних інтересів.

При цьому до суспільних відносин у сфері реалізації державних чи громадських інтересів належить у тому числі й забезпечення громадського порядку та безпеки. Ці види суспільних відносин потребують включення до системи додаткових об'єктів досліджуваних злочинів через очевидну небезпеку, яку створює поширення інформаційних технологій для громадського порядку та безпеки. Велика кількість абонентів со-

ціальних мереж, спеціалізованих сайтів для ведення блогів, інших популярних мережевих служб, поширеність автоматизованих систем керування дорожнім або повітряним рухом, включення комп'ютерного обладнання до систем виробничої безпеки й контролю якості продукції можуть украй негативно вплинути на громадський порядок або безпеку через знищення або модифікацію комп'ютерної інформації.

Урешті-решт, відносини у сфері забезпечення нормальної діяльності підприємств, установ, організацій мають бути віднесені до додаткових безпосередніх об'єктів з огляду на те, що процеси управління будь-якою подібною структурою сьогодні, як ми зазначали в підглаві 1.2, потребують постійного збирання й аналізу інформації. Комп'ютерні мережі набувають значення "нервової системи" сучасних підприємств, збої у їх роботі можуть спричинити значні наслідки.

Зауважимо, що три останні види суспільних відносин, безперечно, входять до змісту першого. Однак видається доцільним їх виокремлювати для того, щоби більш чітко охарактеризувати суспільну небезпечність досліджуваних посягань і, зрештою, надати правозастосовчим органам інструментарій для встановлення суспільної небезпечності злочинів у сфері використання інформаційних технологій.

Перш ніж перейти до специфіки об'єктивної сторони досліджуваних злочинів, розглянемо, як вирішується завдання нормативного відображення означеної специфіки суспільної небезпечності комп'ютерних злочинів у кримінальному законодавстві зарубіжних країн. Так, Кримінальний кодекс Польщі використовує спеціальні ознаки предмета посягання. Він містить норми про відповідальність за незаконні дії лише відносно "запису інформації, що має істотне значення", а також "запису на комп'ютерному носії інформації, який має особливе значення для обороноздатності держави, безпеки зв'язку, функціонування урядової адміністрації або іншого державного органу чи адміністрації самоврядування" [345, с. 182 – 183]. Ознаки предмета посягання використовує й КК ФРН, відповідно до якого кримінальна відповідальність за зміну комп'ютер-

них даних настає лише тоді, коли вони спеціально захищені від несанкціонованого доступу (параграф 303a). У свою чергу порушення опрацювання даних (параграф 303b) отримує кримінально-правову оцінку лише тоді, коли ці дані "мають істотне значення для чужого підприємства, чужої фірми або державного органу" [350, с. 454]. Кримінальні кодекси Данії та Голландії містять спеціальні вимоги до комп'ютерних систем опрацювання даних. Так, за КК Данії (параграф 193) відповідальність за "серйозні збої" у роботі систем опрацювання даних настає тільки в тому випадку, коли такі системи використовуються публічно [341, с. 162]. Подібну норму містить і КК Голландії (ст. 351), який передбачає відповідальність за псування комп'ютерних пристроїв або інші незаконні дії щодо них, якщо вони призначені для використання населенням чи для цілей національної оборони [340, с. 421 – 422]. КК Бельгії використовує ознаки суб'єктивної сторони. Стаття 550ter цього кодексу встановлює відповідальність за введення в інформаційну систему, зміну чи знищення даних, а також зміну будь-яким технологічним шляхом можливого використання даних в інформаційній системі лише в тому разі, коли вони здійснені з метою заподіяння шкоди [339, с. 344]. Австралійський кримінальний кодекс використовує як об'єктивні, так і суб'єктивні ознаки. Він пов'язує відповідальність за посягання у сфері використання інформаційних технологій з: наявністю умислу на вчинення іншого злочину (пункт (d) частини (1) статті 477.1 та пункт (c) частини (4) статті 477.1); приналежністю даних чи комп'ютерних пристроїв, у яких вони обробляються, Австралійському Союзу ((i), (ii), (iv), (v) (1) (d) 477.2); використанням при вчиненні злочину телекомунікаційних послуг, або заподіянням шкоди їх якості внаслідок його вчинення ((iii) (1) (d) 477.2) [337, с. 325 – 331]. Однак найбільш вдалим видається підхід, відповідно до якого специфічна суспільна небезпечність злочинів у сфері використання інформаційних технологій визначається шляхом установлення кримінальної відповідальності тільки за ті порушення в розгляданій сфері, котрими заподіяно шкоду відносинам, для інтенсифікації яких використо-

вується обчислювальна техніка. Так, КК Японії передбачає кримінальну відповідальність за незаконні дії, пов'язані з порушенням функціонування комп'ютерів, введенням неправдивої інформації в автоматизовані системи, знищенням її тощо, тільки тоді, коли ці дії "перешкоджають виконанню професійної діяльності" (ст. 234-II) або використовуються для протиправного отримання вигоди (ст. 246-II) [352, с. 141 – 142, 146 – 147]. Відповідно до КК Австрії відповідальність за зміну, стирання або приведення інформації в непридатний для використання стан іншим шляхом настає тоді, коли подібними діями "заподіяно шкоду іншій людині" (параграф 126а) [338, с. 176]. Відповідальність за зміну комп'ютерної інформації чи введення свідомо неправдивої інформації за відсутності ознак злочину проти власності КК Республіки Білорусь пов'язує лише з настанням істотної шкоди (ст. 350) [344].

Останній спосіб законодавчого відображення суспільної небезпечності досліджуваних злочинів є перспективним ще й тому, що використання ознак предмета та специфічного призначення комп'ютерної техніки допускає можливість віднесення до категорії злочинів діянь, які не є суспільно небезпечними. Наприклад, цілком реальною видається ситуація, коли знищення інформації, яка "має важливе значення для підприємства" або "особливо захищена спеціальними засобами", не спричинило істотних наслідків. Разом із тим, цілком вдалими слід визнати законодавчі рішення, що ґрунтуються на формулюванні специфічних ознак наслідків, способу та мети вчинення злочину.

Таким чином, послідовною, такою, що відповідає означеній специфіці безпосереднього об'єкта, а отже, й суспільній небезпечності досліджуваних злочинів, буде пропозиція визнавати злочини у сфері використання інформаційних технологій такими, які за особливостями конструкції об'єктивної сторони відносяться до злочинів з матеріальним складом. Структура об'єктивної сторони цих злочинів повинна включати як основні наслідки – різні форми порушення запропонованих безпосередніх об'єктів, так і похідні наслідки – істотне

порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, державних чи громадських інтересів, діяльності юридичної особи. Лише за наявності сукупності таких наслідків вчинене посягання у сфері використання інформаційних технологій слід вважати злочином.

Розглянемо, які основні наслідки необхідно передбачити в нормах, що встановлюють відповідальність за порушення права власності на комп'ютерні дані. За чинним законодавством до них належать: витік, втрата (знищення), підробка (зміна), блокування, копіювання, перехоплення, збут або розповсюдження інформації з обмеженим доступом, спотворення процесу обробки, порушення встановленого порядку маршрутизації. Подібні переліки можливих порушень права власності на комп'ютерну інформацію містить також і більшість кримінальних кодексів зарубіжних країн. Так, польський законодавець передбачає відповідальність за знищення, пошкодження, видалення, зміну даних, істотне ускладнення ознайомлення з даними уповноваженої особи чи позбавлення можливості такого ознайомлення іншим способом, а також порушення або унеможливлення автоматизованого збору або передачі даних [345, с. 182-183]. КК Австрії зараховує до розгляданих порушень зміну, стирання або приведення даних у непридатний для використання стан іншим шляхом (параграф 126а) [338, с. 176]. Подібні форми порушення власності на комп'ютерну інформацію містить і КК Голландії (ст. 350a, 350b), який крім цього передбачає відповідальність за блокування. [340, с. 420 – 421]. КК Республіки Білорусь містить таку систему досліджуваних форм: зміна, внесення свідомо неправдивих відомостей, знищення, блокування, приведення у стан, який виключає використання за призначенням, копіювання чи інше заволодіння [344].

Таким чином, "загальновизнаними" слід уважати такі види порушення права власності на комп'ютерну інформацію, як: знищення, зміна, блокування, порушення порядку маршрутизації та спотворення процесу обробки. Отже, доцільність криміналізації цих форм порушення права власності на комп'ютер-

ні дані в контексті злочинів у сфері використання інформаційних технологій не викликає сумнівів.

Неоднозначно кримінальні кодекси зарубіжних країн ставляться до криміналізації витоку, копіювання, перехоплення даних, а також введення недостовірних даних.

Почнемо з останньої форми. Видається, що вона являє собою певний вид такого порушення, як зміна даних. Питання в тому, що терміни "зміна", "підроблення", "перекручення", "спотворення", які використовуються для опису форми порушення права власності на дані, що полягає в несанкціонованій зміні їх змісту, тлумачаться зазвичай у вузькому розумінні, тобто як певна зміна існуючих даних, яка не охоплює їх зміни шляхом внесення нових. На нашу думку, проблема має в певному розумінні лінгвістичний характер, тобто використовувані терміни несуть таке змістове навантаження, що обмежує дійсний зміст форми порушення права власності на дані, для визначення якої застосовуються ці терміни. У зв'язку з цим заслуговує на увагу досвід австралійського кримінального законодавства, яке використовує термін "модифікація даних, що містяться в комп'ютері" та визнає його як "(a) зміну або знищення цих даних; або (b) доповнення цих даних" (1) 476.1 [337, с. 318 – 319]. Термін, що охоплює як зміну, так і доповнення комп'ютерних даних, наявний і в національному законодавстві. Ідеться про порушення цілісності інформації в системі, що визначається Законом України "Про захист інформації в інформаційно-телекомунікаційних системах" як "несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст". Такий термін доцільно використати при подальшому вдосконаленні національного кримінального законодавства для позначення відповідної форми порушення права власності на комп'ютерні дані.

Наступне питання – криміналізація дій, які призводять до витоку інформації. Уважаємо, що таке суспільно небезпечне діяння, як отримання особою інформації, яка не призначена для неї (у термінах вітчизняного законодавства дії, що призводять до витоку інформації), недоцільно пов'язувати тільки з

інформацією у формі комп'ютерних даних. Ці дії також можливі щодо інформації, яка передається в мережах телефонного, радіозв'язку тощо. Суспільна небезпечність таких посягань зумовлена значенням, яке має інформація. Форма представлення інформації може розглядатися в цьому випадку як кваліфікуюча, але не конституююча ознака складу злочину. Тому дії, які призводять до витоку інформації, видається доцільним розглядати не як злочин у сфері використання інформаційних технологій, а як посягання на відносини щодо забезпечення доступу до інформаційних ресурсів. Подібне законодавче рішення містить, наприклад, КК Польщі, стаття 267 якого передбачає кримінальну відповідальність за отримання інформації, не призначеної для суб'єкта посягання, шляхом відкриття запечатаного листа, підключення до каналу передачі інформації, пошкодження електронного, магнітного або іншого спеціального засобу, що забезпечує її безпеку [345, с. 181]. Як можна побачити, польський законодавець не виокремлює в спеціальну норму відповідальність за дії, що призвели до витоку саме комп'ютерної інформації. Існує також інший приклад. Так, КК ФРН у параграфі 202a "Розвідування відомостей" установлює відповідальність за протиправне отримання відомостей, які не призначені для суб'єкта посягання та які особливо захищені від незаконного доступу. При цьому частина друга розгляданого параграфу визначає, що під цими відомостями слід розуміти тільки ті відомості, які являють собою комп'ютерну інформацію, "збираються або передаються електронним, магнітним або іншим способом, який безпосередньо не сприймається" [350, с. 359]. Однак КК ФРН розглядає цей злочин не як посягання у сфері інформаційних технологій, а як одне з порушень недоторканності й таємниці приватного життя (розділ XIV Особливої частини) разом із такими посяганнями, як порушення таємниці листування (параграф 202) і таємниці приватного життя (параграф 203). Отже, наведений приклад знову ж таки підтверджує тезу про недоцільність розгляду відповідальності за витік інформації в контексті злочинів у сфері інформаційних технологій. Подібне рішення міс-

тить і КК Австрії, який відносить незаконне отримання комп'ютерних даних, що не призначені для суб'єкта посягання (параграф 118а), до розділу V Особливої частини "Порушення, що посягають на приватну сферу та на розголошення певної професійної таємниці" [338, с. 164 – 165]. Зазначимо також, що дії, які призводять до копіювання або перехоплення комп'ютерної інформації, можуть мати ознаки суспільної небезпечності тільки тоді, коли здійснюються щодо інформації з обмеженим доступом та призводять до її витоку. Отже відповідальність за витік інформації доцільно розглядати в комплексі заходів кримінально-правового забезпечення охорони суспільних відносин щодо доступу до інформації. При цьому дії, що призводять до витоку інформації у вигляді комп'ютерних даних, а також копіювання або перехоплення таких даних слід розглядати як кваліфікуючі ознаки незаконного ознайомлення особи з інформацією. Оскільки зазначене посягання є одним із видів порушення відносин щодо забезпечення доступу до інформаційних ресурсів, то до питання кримінальної відповідальності за витік, копіювання та перехоплення комп'ютерних даних ми повернемось у відповідній главі.

Питання щодо визначення форм порушення наступних безпосередніх об'єктів злочинів у сфері використання інформаційних технологій, а отже, і відповідних основних наслідків вирішується значно простіше. Так, порушенням суспільних відносини щодо забезпечення працездатності комп'ютерних систем та інших технічних засобів інформаційних технологій, організації та здійснення програмного, технічного й організаційного захисту комп'ютерних даних треба вважати незастосування або неналежне використання засобів захисту комп'ютерних даних. У свою чергу, основним наслідком при порушенні суспільних відносини щодо користування послугами електронної пошти, як ми зазначали раніше, слід визнавати істотне ускладнення або унеможливлення протягом певного часу користуватися послугами електронних повідомлень, що зазвичай виявляється в ускладненні або унеможливленні відправлення чи отримання електронних повідомлень.

Нарешті, основними наслідками посягань на суспільні відносини щодо надання й отримання телекомунікаційних послуг слід уважати ускладнення або унеможливлення їх отримання або незаконне отримання. Наприклад, унаслідок дій зловмисника особа не може користуватися телефонним зв'язком, або зв'язок значно ускладнений, або, навпаки, особа отримує якісні телекомунікаційні послуги, але не має на це права.

Як зазначалося вище, загальною умовою віднесення перелічених форм порушення визначених безпосередніх об'єктів до злочинів пропонується визнавати настання похідних наслідків у вигляді: 1) істотного порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб; 2) істотного порушення реалізації державних чи громадських інтересів; 3) істотного порушення діяльності юридичних осіб.

Формулювання "*шкода реалізації прав, свобод і законних інтересів*" є, зрозуміло, найбільш широким визначенням можливих наслідків будь-якого посягання. Разом із тим, його включення до нормативного визначення злочинів у сфері використання інформаційних технологій є необхідним. Воно забезпечить обов'язковість розв'язання в кожному конкретному випадку питання про дійсну суспільну небезпечність певного посягання та, відповідно, вимагатиме з'ясування доцільності використання засобів кримінальною юстиції. Такий підхід до конструювання законодавчого визначення досліджуваних злочинів виправданий двома головними чинниками. По-перше, відсутністю чітких критеріїв суспільної небезпечності посягань у сфері використання інформаційних технологій через обмеженість судової практики та постійне збільшення потенційних загроз, зумовлене розширенням сфери застосування комп'ютерної техніки. По-друге, установленою нами необхідністю підвищення ефективності кримінально-правової протидії досліджуваним злочинам, яка досягається насамперед виключенням зі сфери дії закону про кримінальну відповідальність посягань, що не характеризуються суспільною небезпечністю. Отже, до порушення реалізації прав, свобод і законних інтересів окре-

мих фізичних осіб будемо зараховувати такі можливі суспільно небезпечні наслідки незаконного знищення, спотворення або блокування комп'ютерної інформації, як заподіяння матеріальної шкоди, блокування персонального акаунту, електронної пошти чи засобів адміністрування сайту тощо.

До *істотного порушення реалізації державних чи громадських інтересів* слід відносити ускладнення діяльності органів державної влади чи місцевого самоврядування, заподіяння через це матеріальної шкоди, порушення громадського порядку або громадської безпеки тощо. Так, до порушень громадського порядку пропонується відносити такі наслідки незаконного впливу на комп'ютерну інформацію, що характеризуються істотним порушенням норм моралі, правил спілкування та співжиття, традиційної системи правил, які регулюють стосунки між людьми у сфері суспільного, політичного, приватного життя та побуту [271, с. 22 – 23]. Достатньо показовим прикладом посягання у сфері використання інформаційних технологій, яке слід визнавати суспільно небезпечним у зв'язку із заподіянням шкоди громадському порядку, є випадок, що мав місце 2008 року в Москві. Гучний інцидент стався в районі в'їзду до Серпуховського тунелю на Садовому кільці. На екрані розміром 6х9 метрів рекламу пластикових вікон несподівано змінив ролик порнографічного змісту. На дорозі одразу утворилася "пробка" [367]. Прикладом незаконних дій з комп'ютерною інформацією, що призвели до порушення громадського порядку, можна вважати і блокування або спотворення даних, представлених на офіційних інтернет-сторінках політичних сил або діячів. Так, у вересні 2010 року повідомлялося про те, що офіційні сайти членів уряду Туреччини протягом кількох днів піддавалися DDoS-атаці, а інформація, викладена на них, була недоступна користувачам мережі. Такі дії мали місце стосовно офіційних сайтів віце-прем'єра країни Бюлента Аринджа, а також глави МВС Бешира Аталая. Після атаки до останнього надійшло повідомлення, яке свідчило про політичну мотивацію дій зловмисників [47]. У січні 2011 року повідомля-

лося про розміщення на сторінці Ніколя Саркозі у Facebook інформації про його відмову від участі в президентських виборах 2012 року. Президентові Франції довелося давати поспішне спростування цієї інформації [370]. В іншій соціальній мережі – Twitter – було зафіксовано несанкціоновану зміну офіційного акаунту КНДР. Зловмисники розмістили на ньому заклики до скидання правлячої партії Ким Чен Іра, а також звинувачення правлячої партії країни в тому, що її політика ґрунтується на особистій наживі та спрямована на розроблення ядерної зброї [371]. Про потенційні можливості використання сучасних інформаційних технологій з метою порушення громадського порядку може певною мірою свідчити і той факт, що учасники подій кінця 2010 – початку 2011 року в Тунісі та Єгипті використовували для координації своїх дій і залучення нових учасників акцій протесту загальнодоступні соціальні мережі Twitter та Facebook [42].

А порушенням громадської безпеки, зумовленим незаконними діями з комп'ютерною інформацією, пропонується вважати заподіяння шкоди або створення небезпеки її заподіяння, спричиненої втручанням у роботу автоматизованих систем управління та контролю за джерелами підвищеної небезпеки, безпекою руху, протипожежною, санітарною, технічною безпекою на підприємствах, будівництві, у науково-дослідних закладах тощо [269, с. 504]. До прикладів подібних наслідків можна віднести порушення працездатності сайту ВМС Великобританії. У листопаді 2010 року представник британського військового флоту під час прес-конференції визнав спробу невідомих осіб заподіяти шкоду працездатності цього інформаційного ресурсу [306].

Зазначимо, що в деяких країнах порушення у сфері використання інформаційних технологій розглядаються навіть у контексті загроз національній безпеці. Так, головними загрозами Стратегія національної безпеки Великобританії називає тероризм, кібернетичні атаки, міжнародні військові кризи, масштабні надзвичайні події та природні катаклізми [391]. Подібну оцінку злочинність у сфері використання інформа-

ційних технологій починає отримувати і в нашій країні. Виходячи з комплексного аналізу викликів і загроз безпеці країни у 2011 році, Рада національної безпеки і оборони України акцентувала увагу на необхідності створення єдиної загальнодержавної системи протидії кіберзлочинності [355]. Зауважимо також, що масштабність наслідків таких подій 2010 року, як початок роботи Wikileaks та розповсюдження шкідливого програмного забезпечення Stuxnet (про сутність наслідків ітиметься далі), дозволила експерту фірми Sophos Грэму Клюлі зробити висновок про "початок нової епохи кіберзлочинності". Якщо в "першу епоху шкідливі програми створювалися в основному аматорами на персональних комп'ютерах, а в другу ними зайнялися професійні злочинці, то зараз кіберзлочинність набуває геополітичного значення" [421].

До порушення *нормальної діяльності підприємств, установ чи організацій* пропонується зараховувати істотні ускладнення в здійсненні ними статутної або нормативно передбаченої діяльності, викликані порушенням роботи використовуваних у цій діяльності інформаційних технологій. Приклади подібних наслідків ми наводили раніше. Ідеться про наявні в національній судовій практиці рішення, пов'язані з кримінально-правовою кваліфікацією дій осіб, які: істотно ускладнювали роботу працівників регіональної податкової адміністрації з електронною звітністю платників податків [155, 156]; створювали перешкоди в діяльності торговельної мережі шляхом знищення бази даних товарів і, як наслідок, унеможливили роботи касових апаратів [160]; з метою поновлення на роботі (шляхом зміни розташування баз даних на корпоративному сервері) унеможливлювали діяльність планово-організаційних підрозділів гірничо-видобувного підприємства [150]. Як приклад порушення діяльності підприємств, установ чи організацій можна також навести вихід з ладу внаслідок хакерської атаки процесингової системи "Assist", головним клієнтом якої є "Аерофлот" (липень 2010 року). Це призвело до істотного обмеження продажу квитків і, відповідно, певних збитків [1]. На окрему увагу в контексті розгляду можливостей заподіяння шкоди

діяльності підприємств, установ чи організацій шляхом порушення роботи використовуваних ними інформаційних технологій заслуговує розгляд повідомлень щодо шкідливої програми Stuxnet. Фахівці вважають її першою в "лінійці" засобів, призначених спеціально для промислових диверсій. За оцінками експертів, ця програма дозволяє не просто блокувати, знищувати чи копіювати комп'ютерну інформацію, Stuxnet розрахована на порушення роботи виробництв, де комп'ютерна техніка використовується для керування обладнанням [412]. Із впливом цього програмного забезпечення пов'язують відкладення пуску Бушерської АЕС та призупинення роботи уранозбагачувальної фабрики в Натанзі (Іран) [127], а також чисельні порушення виробничих процесів на підприємствах КНР [128].

Зауважимо, що можливі комбінації вторинних наслідків. Наприклад, порушення автоматизованих систем безпеки та керування на Бушерський АЕС, яке відбулося внаслідок використання шкідливої програми Stuxnet, слід розглядати не тільки як порушення нормальної роботи підприємства, але і як порушення громадської безпеки.

Необхідно також зазначити, що проведене дослідження практики застосування ст.ст. 361 – 362 КК України свідчить про те, що значна частина посягань у сфері використання інформаційних технологій здійснювалася з метою скоєння в подальшому інших злочинів або приховування вчинених (38,32 %). Подібна тенденція спостерігається й при оцінці даних про результати роботи спеціалізованих підрозділів правоохоронних органів країн СНД. Так, співробітники Управління "К" МВС Росії зазначали, що у 2010 році серед протиправних дій у сфері інформаційних технологій за розміром збитків лідирують неправомірний доступ до комп'ютерної інформації, а також створення, використання та поширення шкідливих програм. На їх частку припадає більше 60 відсотків усіх інцидентів. При цьому окрема увага зверталася на те, що заволодіння кодами і паролями, блокування комп'ютерних систем у переважній більшості випадків служать свого роду "ключем до скоєння ін-

ших злочинів", у тому числі шахрайства [359]. За повідомленням одного з керівників спеціалізованого управління МВС Білорусі І. Пармона, 93 % усіх злочинів у сфері високих технологій в країні складають розкрадання шляхом використання комп'ютерних технологій [41]. Ця специфіка обґрунтовує необхідність такого зауваження: у тих випадках, коли посягання у сфері використання інформаційних технологій здійснюються з метою подальшого скоєння інших злочинів або приховування вже скоєних, віднесення матеріальної шкоди, заподіяної в ході вчинення цих ("некомп'ютерних") посягань, до наслідків злочинів у сфері використання інформаційних технологій є некоректним. Якщо, наприклад, шляхом порушення цілісності комп'ютерних даних було вчинено незаконне заволодіння майном фізичної особи, неправильно відносити заподіяну шкоду як до наслідків злочину проти власності, так і до наслідків "комп'ютерного" злочину. Подібна кваліфікація була б порушенням аксіоматичних правил кримінально-правової кваліфікації. Проте сказане не означає, що в подібних випадках слід говорити про відсутність ознак злочину у сфері використання інформаційних технологій. Сам факт вчинення певного "некомп'ютерного" злочину шляхом незаконних дій з комп'ютерними даними обґрунтовано, залежно від обставин справи, розглядати як істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи.

Законодавче оформлення визначень запропонованих похідних наслідків вимагає розгляду питання щодо використання оцінних понять у текстах законів про кримінальну відповідальність. Більшість дослідників звертає увагу на необхідність формулювання спеціальних законодавчих визначень до кожного розділу Особливої частини, що містить подібні поняття. Так, Є.В. Шевченко зазначає: "Більш доцільним на початку розділу, в якому згруповані предметні делікти з похідними наслідками техногенного характеру, помістити спеціальну норму з характеристикою шкоди, що охоплюється поняттям «тяжких наслідків» і, таким чином, прийти до єдиної схеми в їх ви-

кладенні" [384, с. 105]. Подібну позицію висловлює також Д.О. Балобанова [19, с. 9]. О.М. Миколенко до основних напрямків удосконалення кримінального законодавства щодо застосування оцінних понять, які використовуються при законодавчому закріпленні суспільно небезпечних наслідків, зараховує: 1) передбачення в кожному розділі Особливої частини КК самостійної статті, яка б містила законодавче визначення всіх оцінних понять, що використовуються в цьому розділі; 2) наповнення цих оцінних понять самостійним змістом, який випливає з особливостей об'єкта посягання [232, с. 10]. Застосовуючи ці теоретичні положення для розв'язання завдання побудови законодавчого формулювання кримінально-правових засобів охорони інформаційної безпеки у сфері використання інформаційних технологій, зазначимо таке. По-перше, на сьогодні через обмеженість судової практики, постійне оновлення суспільних відносин, пов'язаних із застосуванням інформаційних технологій, та розширення сфери їх використання достатньо важко сформулювати вичерпне визначення оцінних понять, які необхідно використати в диспозиціях відповідних норм ("істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб", "істотне порушення державних чи громадських інтересів", "істотне порушення діяльності юридичної особи"). Разом із тим, по-друге, видається можливим сформулювати певні критерії, які можуть бути використані в тих випадках, коли похідні наслідки полягають у заподіянні матеріальної шкоди. Ці критерії доцільно побудувати залежно від того, кому заподіяно шкоду та які за характером збитки слід ураховувати при кримінально-правовій оцінці діяння. Зазначимо й те, що досить часто шкода, завдана злочином у сфері використання інформаційних технологій, може складатися з великої кількості незначних збитків, заподіяних певній кількості різних осіб. Ця обставина не тільки потребує нормативного визначення, але й актуалізує питання розгляду досліджуваних посягань у контексті продовжуваних злочинів. Таким чином, пропонуються такі визначення:

- істотним порушенням реалізації прав, свобод або законних інтересів окремих фізичних осіб, якщо воно полягає в заподіянні матеріальних збитків, уважається: а) шкода фізичній особі, заподіяна через обмеження або виключення можливості реалізації нею своїх прав, свобод чи законних інтересів, яка у два або більше разів перевищує неоподатковуваний мінімум доходів громадян; б) сукупна шкода двом або більше фізичним особам, заподіяна протягом одного місяця через обмеження або виключення можливості реалізації ними своїх прав, свобод чи законних інтересів, яка в п'ять або більше разів перевищує неоподатковуваний мінімум доходів громадян;

- істотним порушенням реалізації державних чи громадських інтересів, якщо воно полягає в заподіянні матеріальних збитків, уважається шкода, заподіяна через обмеження або виключення можливості реалізації державних чи громадських інтересів, яка у двадцять або більше разів перевищує неоподатковуваний мінімум доходів громадян;

- істотним порушення діяльності юридичної особи, якщо воно полягає в заподіянні матеріальних збитків, уважається шкода, що складається з витрат, яких зазнає юридична особа у зв'язку з порушенням її діяльності, а також витрат, які вона мусять зробити для відновлення своєї діяльності, яка в п'ятнадцять або більше разів перевищує неоподатковуваний мінімум доходів громадян.

Законодавче відбиття суспільної небезпечності посягань у сфері використання інформаційних технологій доцільно забезпечувати не тільки шляхом нормативного визначення можливих похідних наслідків цих злочинів. Доречним уявляється також формулювання специфічних суб'єктивних ознак. Необхідність уточнення законодавчих визначень у питанні формулювання суб'єктивних ознак було аргументовано під час розгляду принципу повноти складу. Разом із тим, законодавче уточнення суб'єктивного ставлення до похідних наслідків так само видається достатньо ефективним засобом підвищення визначеності норм кримінального закону в питанні суспільної небезпечності посягань. З урахуванням доведеної на початку

підглави необхідності законодавчої диференціації відповідальності залежно від шкоди, заподіяної комп'ютерним злочином, маємо зробити висновок, що пропонується передбачити три види похідних наслідків залежно від ступеня суспільної небезпечності: 1) основні похідні наслідки – істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи; 2) заподіяння значної шкоди; 3) заподіяння тяжких наслідків. Ураховуючи наведені раніше та доведені Є.В. Шевченком положення щодо можливих комбінацій умислу та необережності в складах злочинів з похідними наслідками [384, с. 179 – 180], для побудови системи законодавчої диференціації суспільної небезпечності посягань на відносини інформаційної безпеки у сфері використання інформаційних технологій залежно від суб'єктивного ставлення до похідних наслідків пропонуємо: 1) в окремих статтях передбачити кримінальну відповідальність за посягання на інформаційну безпеку, пов'язані з умисним або необережним ставленням до похідних наслідків; 2) у статтях, які передбачають умисне ставлення до похідних наслідків, на рівні основних складів передбачити відповідальність за істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, державних чи громадських інтересів, діяльності юридичної особи, на рівні кваліфікованих – за заподіяння значної шкоди, на рівні особливо кваліфікованих – за заподіяння тяжких наслідків; 3) у статтях, які передбачають необережне ставлення до похідних наслідків, на рівні основних складів передбачити відповідальність за заподіяння значної шкоди, на рівні кваліфікованих – за заподіяння тяжких наслідків.

Окремого розгляду потребує доцільність криміналізації створення, розповсюдження або збуту шкідливих програмних чи технічних засобів, діянь, що, як зазначалося раніше, створюють загрозу заподіяння шкоди відносинам власності на комп'ютерні дані. Зважаючи на висловлені положення щодо нормативного врахування специфіки суспільної небезпечності досліджуваних злочинів, криміналізація подібних діянь як са-

мостійних посягань видається недоцільною. У зв'язку з цим заслуговує на увагу розв'язання цієї проблеми в КК Австралії. Стаття 478.3 передбачає відповідальність за володіння даними (комп'ютерною інформацією чи комп'ютерними програмами) або здійснення контролю стосовно них, якщо суб'єкт переслідує мету їх подальшого використання при вчиненні комп'ютерних злочинів. У свою чергу, статтею 478.4 установлюється відповідальність за створення, пересилання чи отримання даних, якщо умислом особи охоплюється їх подальше використання при вчиненні злочинів, передбачених розділом 477 КК Австралії "Серйозні комп'ютерні злочини" [337, с. 334 – 335]. Фактично ці норми КК Австралії містять визначення спеціальних форм попередньої злочинної діяльності у сфері використання інформаційних технологій. Відповідальність за такі дії на підставі норм чинного національного законодавства може наставати без застосування ст. 361-1, а в межах відповідальності за злочини, для вчинення яких особа збиралася використовувати шкідливе забезпечення, із застосуванням ст. 14 або ст. 15 КК України. Разом із тим, використання спеціалізованих програмних чи технічних засобів значно підвищує рівень суспільної небезпечності комп'ютерного злочину, оскільки дозволяє заподіяти значно більшу шкоду, свідчить про сталість антисоціальної установки суб'єкта посягання, наявність у нього спеціальних знань у сфері використання інформаційних технологій. Через це обґрунтованою видається пропозиція щодо криміналізації незаконних дій із шкідливими програмними чи технічними засобами як кваліфікуючої ознаки посягань на відносини власності на комп'ютерні дані.

Слушність цієї пропозиції підтверджується й дослідженням тенденцій розвитку шкідливого програмного забезпечення. Як свідчать спеціалізовані дослідження, небезпеку становить не розповсюдження шкідливого забезпечення саме по собі, а подальші порушення інформаційних відносин з використанням цих програм, які зазвичай переслідують мету вчинення інших злочинів. Так, згідно з висновками компанії "Доктор Веб" у 2010 році спостерігався розвиток двох специфічних ви-

дів шкідливого програмного забезпечення: буткітів та шифрувальників. У листопаді 2010 року набула поширення шкідлива програма буткіт Trojan.MBRlock.1. Після установки вона розміщується в головному завантажувальному записі жорсткого диска та блокує можливість запуску системи. Як наслідок, на екран виводяться вимоги зловмисників заплатити за розблокування системи $100. У повідомленні також ідеться про те, що вміст усіх дисків комп'ютера нібито зашифрований. І хоча це не відповідає дійсності, система все одно не починає завантажуватися. При введенні правильного пароля відновлюється початковий стан завантажувальної ділянки диска, а встановлена операційна система завантажується у звичайному режимі. За подібною схемою працюють і шкідливі програми, які належать до типу шифрувальників. Наприклад, Trojan.Encoder.88 шифрує документи користувача багатьох популярних форматів (тексти, схеми, презентації, електронні таблиці, бази даних тощо) з використанням такого алгоритму, який істотно ускладнює розшифрування. Так, щоби повністю перебрати всі можливі ключі розшифрування в пошуках того, який потрібен для відновлення файлів тільки на одному зараженому комп'ютері, знадобиться таке число операцій, яке можна записати як одиницю з 77 нулями. При цьому для кожного комп'ютера генерується свій унікальний ключ шифрування [205].

Зрозуміло, що і чинна редакція ст. 361-1 КК дозволить визнати злочинними дії осіб, які розповсюджують подібні програми. Але через відсутність чітких критеріїв суспільної небезпечності наявність цієї норми, як ми мали можливість побачити, призводить до поширення сфери кримінально-правового впливу на діяння, які не можна вважати суспільно небезпечними, і, урешті-решт, зменшує ефективність кримінальної юстиції. Набагато доречнішим було б розглядати ці діяння в контексті зроблених пропозицій як блокування комп'ютерної інформації, що призвело до істотного порушення прав фізичної особи, з використанням шкідливої програми. Тим паче, що така кваліфікація більшою мірою відповідала б реальній дійсності, а кримінально-правова заборона, сформульована в та-

кий спосіб, мала б ще одну незаперечну перевагу: "програмувала" б діяльність правоохоронних і судових органів на встановлення фактів, які свідчать про реальну суспільну небезпечність відповідних посягань.

Доцільність висловлених пропозицій підтверджується також іншою тенденцією розвитку посягань у сфері використання інформаційних технологій. Уже близько десяти років фахівці з технічного захисту інформації фіксують загрози, пов'язані зі створенням і використанням так званих ботнетів. Ботнет (англ. *robot*, *network*) – це мережа комп'ютерів, на які встановлено шкідливу програму, що дозволяє зловмисникам дистанційно керувати такими машинами (кожною окремо або мережею взагалі) без відома користувача [118]. Достатньо поширеним механізмом створення подібних мереж є використання шкідливого програмного забезпечення, замаскованого під матеріали, які з великою часткою ймовірності будуть популярні серед користувачів Інтернету. Так, у січні 2011 року фахівці з комп'ютерної безпеки виявили в Інтернеті шкідливу програму, яка маскується під посібник "Справжня Камасутра". Файл з троянським вірусом видає себе за презентацію для Microsoft PowerPoint. Після його відкриття на екрані запускається слайд-шоу з 13 слайдів, водночас відбувається зараження комп'ютера. Заражений комп'ютер може в подальшому використовуватися для DDoS-атак, розсилання спаму та інших цілей. Раніше хакери видавали шкідливе програмне забезпечення за оновлення для браузерів, ігрові програми та навіть за запрошення на церемонію вручення Нобелівської премії [372].

Зловмисники, які використовують такі технології, періодично затримуються правоохоронцями. Наприклад, у жовтні 2010 року повідомлялося про арешт громадянина Росії Геворка Аванесова, який розшукувався по лінії Інтерполу правоохоронними органами Голландії за звинуваченням у вчиненні злочинів, пов'язаних з використанням інформаційних технологій, діяльністю у складі злочинних угруповань, відмиванням грошей. Передбачалося, що він є координатором ботнету. Створення бот-мережі відбувалося шляхом зараження комп'ю-

терів спеціальним шкідливим програмним забезпеченням. За даними голландського Інституту розслідувань, до створеної ним мережі входило понад 20 млн. комп'ютерів. Зазначалося, що вона використовувалася переважно для блокування різних ресурсів (DDoS-атаки), розсилання спаму, а також заволодіння банківськими реквізитами користувачів систем онлайн-банкінгу [16].

Відповідно до викладених пропозицій подібні дії отримують кваліфікацію, яка цілком відповідає їх сутності та відображає суспільну небезпечність: спотворення процесу обробки комп'ютерної інформації (виконання системою операцій, які не передбачені технічними характеристиками встановленого користувачем програмного забезпечення), що спричинило істотне порушення прав окремих фізичних осіб та діяльності юридичних осіб, вчинене з використанням шкідливих програм. А діяльність зі створення й використання ботнету, за чинним законодавством, необхідно кваліфікувати як розповсюдження шкідливої програми (ст. 361-1 КК) та несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до спотворення процесу обробки інформації (ст. 361 КК). Неважко побачити, що навіть на лінгвістичному рівні кваліфікація за чинним законодавством далека від фіксації дійсно важливих і значущих аспектів вчиненого. Сутність небезпеки ботнетів полягає у їх призначенні та меті, із якою вони створюються й використовуються, але чинне кримінальне законодавство залишає її поза межами сукупності ознак, які необхідно встановлювати при кваліфікації. Такі законодавчі положення призводять до ситуації, коли для притягнення до кримінальної відповідальності достатньо поверхового дослідження вчиненого (наприклад, установлення лише факту розповсюдження шкідливої програми). Зрозуміло, що це не сприяє підвищенню ефективності функціонування системи кримінальної юстиції у сфері протидії досліджуваним злочинам.

Наявність кримінально-правової заборони простого розповсюдження або збуту шкідливих програмних засобів є також недоцільною, якщо враховувати значне поширення подібного

явища. У контексті висловлених у підглаві 1.3 методологічних засад дослідження подібна криміналізація є порушенням принципу відносної поширеності діяння. Знайти й завантажити на власний комп'ютер для подальшого використання певну шкідливу програму можна достатньо легко. Так само не важко придбати її на спеціалізованому ринку. У таких умовах установлення кримінальної відповідальності за розповсюдження або збут шкідливих програмних чи технічних засобів є типовим прикладом інфляції закону про кримінальну відповідальність. Він передбачає норми, що принципово не можуть бути забезпечені державними ґарантіями діяльності правоохоронних і судових органів. Таке становище крім створення умов для зловживання кримінальним правом, чинить неґативний вплив і на правову свідомість, оскільки передбачає можливість демонстрації членам суспільства масових порушень принципу невідворотності покарання. Як правильно зазначає Є.Л. Стрельцов, "криміналізація певного діяння має обов'язково враховувати кількість проявів неґативного явища, тобто чи буде в змозі держава реально реалізовувати основний принцип кримінальної відповідальності – її невідворотність. Недотримання цього призведе до декларативності кримінального права, посилення правового нігілізму та може створити небезпеку вкрай низької загальної оцінки населенням реальних можливостей держави" [325, с. 81].

Таким чином, висловлені пропозиції дозволять ефективно вирішити завдання формулювання нормативних визначень злочинів у сфері використання інформаційних технологій. Отримані законодавчі положення враховуватимуть дійсну суспільну небезпечність посягань та чітко обмежуватимуть відповідну сферу кримінально-правового впливу, чим у свою чергу створять умови для підвищення ефективності протидії досліджуваним злочинам. Водночас наведені пропозиції щодо законодавчого врахування чинників суспільної небезпечності злочинів у сфері використання інформаційних технологій дозволять на новому рівні підійти до розв'язання проблеми приведення норм адміністративного та кримінального законодав-

ства до змістової та термінологічної відповідності. Для цього видається доцільним сформулювати такі законодавчі визначення адміністративних проступків і злочинів у сфері використання інформаційних технологій, які б дозволяли відмежовувати одні правопорушення від інших за ознакою настання суспільно небезпечних наслідків. Причому наслідків не у сфері використання комп'ютерної техніки, як це має місце в чинному законодавстві, а наслідків як істотної шкоди тим суспільним відносинам, для інтенсифікації яких використовуються інформаційні технології. Як ми доводили раніше, саме такі наслідки зумовлюють суспільну небезпечність досліджуваних злочинів та, відповідно, є найбільш чітким критерієм для встановлення меж адміністративно-правового та кримінально-правового впливу на суспільні відносини. Наприклад, якщо кримінальна відповідальність за блокування комп'ютерної інформації буде пов'язана із заподіянням істотної шкоди суспільним відносинам щодо реалізації прав і свобод громадян, забезпеченням громадського порядку, громадської безпеки, нормального функціонування підприємств, установ чи організацій, та дії, подібні до описаних вище "крадіжок машинного часу", отримуватимуть правову оцінку, адекватну їх суспільній небезпечності. Так, цілком обґрунтованим видається притягнення до кримінальної відповідальності у випадку, коли блокування комп'ютерної інформації, викликане несанкціонованим доступом до Інтернету за рахунок потерпілої особи, завдає істотної шкоди діяльності певної організації, установи чи підприємства. Водночас, якщо подібні дії не заподіяли шкоди відносинам, котрі пропонується визначати як обов'язковий додатковий об'єкт досліджуваних злочинів, уважаємо цілком достатнім застосування лише адміністративно-правових заходів. Так само і кримінальна відповідальність за порушення, пов'язані з масовим розсиланням повідомлень електронної пошти, буде доцільною лише тоді, коли це завдало істотної шкоди правам і свободам людини й громадянина, забезпеченню громадського порядку або громадської безпеки, нормальній діяльності установ, підприємств, організацій. У тих випад-

ках, коли подібні наслідки не настали, мова може йти про наявність відповідних адміністративних правопорушень.

Важливим аспектом дослідження криміналізації суспільно небезпечних діянь у сфері використання інформаційних технологій є також питання обґрунтованих розмірів санкцій. На нашу думку, Б.Г. Розовський запропонував чіткий і результативний метод розв'язання цієї проблеми: необхідно співвіднести запропоновані санкції із санкціями за ті посягання, суспільна небезпечність яких не є дискусійною і може слугувати своєрідним орієнтиром. Зазвичай до таких посягань відносяться так звані "традиційні" злочини. Оскільки уявлення про їх суспільну небезпечність та, відповідно, обґрунтованість санкцій пройшли верифікацію багаторічною практикою застосування, їх використання для відносних оцінок санкцій за "нові" злочинні посягання є обґрунтованим.

Насамперед зазначимо, що санкції статей розділу XVI не можна вважати узгодженими між собою. Про це свідчить очевидний дисбаланс визначених законодавцем можливих меж покарання за злочини, передбачені ч. 1 ст. 361 та ч. 1 ст. 362 КК. На думку законодавця, зміна, знищення або блокування комп'ютерної інформації, вчинені особою, яка має право доступу до неї, характеризуються меншою суспільною небезпечністю, ніж заподіяння тих самих наслідків, але загальним суб'єктом. І якщо цю ситуацію ще можна вважати технічною помилкою, то аналіз санкцій досліджуваного розділу в контексті інших норм Особливої частини КК красномовно свідчить про очевидні недоліки чинного законодавства. Так, знищення, зміна, блокування, витік, спотворення процесу обробки або порушення порядку маршрутизації комп'ютерної інформації чи інформації, що передається в мережах електрозв'язку, за відсутності настання інших наслідків (ч. 1 ст. 361 КК) характеризуються, виходячи зі співставлення санкцій, майже такою самою суспільною небезпечністю, як: публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (ч. 2 ст. 109); умисне

вбивство, вчинене при перевищенні меж необхідної оборони, а також у разі перевищення заходів, необхідних для затримання злочинця (ст. 118); умисне середньої тяжкості тілесне ушкодження (ст. 122); зайняття лікувальною діяльністю без спеціального дозволу, здійснюване особою, яка не має належної медичної освіти, якщо це спричинило тяжкі наслідки для хворого (ст. 138); проста крадіжка (ч. 1 ст. 185); шахрайство, що завдало значної шкоди (ч. 2 ст. 190); недбале зберігання вогнепальної зброї або бойових припасів, якщо це спричинило загибель людей або інші тяжкі наслідки (ст. 264); втрата документів, що містять державну таємницю (ч.1 ст. 329), тощо. Крім того, використовуючи цей метод, маємо констатувати, що просте несанкціоноване втручання в роботу комп'ютерної техніки чи мереж електрозв'язку (ч. 1 ст. 361) є більш суспільно небезпечним, ніж умисне знищення чи пошкодження чужого майна, що заподіяло шкоду у великих розмірах (ч. 1 ст. 194), або, наприклад, порушення правил безпеки дорожнього руху чи експлуатації транспорту особою, яка керує транспортним засобом, що спричинило потерпілому середньої тяжкості тілесне ушкодження (ч. 1 ст. 286). Подібні зауваження через достатньо близький зміст санкцій ст.ст. 361 – 363-1 можна зробити за кожним злочином у сфері використання комп'ютерної техніки та мереж електрозв'язку.

Додавши до сказаного наведені результати аналізу судових рішень, доходимо до абсурдних, але обґрунтованих з точки зору законодавства висновків про те, що, наприклад, підключення до мереж кабельного телебачення є таким, яке за рівнем суспільної небезпечності можна порівняти з заподіянням середньої тяжкості тілесних ушкоджень або заподіянням тяжкої шкоди здоров'ю через недбале зберігання вогнепальної зброї. Це є ще одним аргументом на користь включення до законодавчих визначень "комп'ютерних" злочинів зазначених критеріїв суспільної небезпечності посягань.

Стосовно розмірів санкцій і видів покарань зауважимо також, що обґрунтованим видається збільшення нижньої та верхньої меж можливого штрафу як основного покарання за про-

сте порушення правил здійснення масових розсилань електронних повідомлень, а також передбачення штрафу як обов'язкового додаткового покарання за кваліфіковані види таких порушень. Ця пропозиція зумовлена описаними раніше сутнісними ознаками масового розповсюдження повідомлень електрозв'язку, що дозволяють характеризувати діяльність спамерів як певний вид господарської діяльності. Отже, передбачення значних штрафів є найбільш ефективним способом попередження подібних злочинів і перетворення їх таким чином на економічно неприбуткові.

Наприкінці дослідження положень розділу XVI КК України з позицій дотримання принципу криміналізації суспільно небезпечних діянь слід зазначити ще одну особливість відносин у сфері використання інформаційних технологій, яку закон про кримінальну відповідальність повинен обов'язково враховувати. Ідеться про те, що ці відносини розвиваються дуже стрімко, а технології вчинення комп'ютерних злочинів змінюються майже щодня. Зрозуміло, що не кожна подібна зміна має знаходити відображення в статтях КК. Однак уважаємо за необхідне нормативно закріпити вимогу періодичного аналізу тенденцій досліджуваної групи злочинів, чинників їх суспільної небезпечності, соціальних потреб відповідних кримінально-правових заборон та ефективності їх застосування.

4.4. Кримінально-правові засоби протидії злочинам у сфері використання інформаційних технологій у контексті дотримання принципу міжнародно-правової необхідності та допустимості криміналізації

Одним із найважливіших питань у сфері законодавчого забезпечення протидії цим злочинам є, безсумнівно, гармонізація національного законодавства з положеннями норм між-

народного права з питань комп'ютерних злочинів. Розвиток сучасних систем телекомунікації та комп'ютерних мереж призвів до такої ситуації, коли протидія цим злочинам не може бути достатньо ефективною, якщо вона здійснюється в межах однієї країни [135, с. 57, 255]. Так званий кіберпростір не має державних кордонів. Наприклад, особа, котра вчиняє несанкціонований доступ до комп'ютерної інформації, необов'язково має перебувати в тій країні, де фізично розташований носій цієї інформації. Автор комп'ютерного вірусу може розмістити його на популярному сайті в мережі Інтернет, що призведе до його розповсюдження у великій кількості країн. Усе це вимагає узгодження національних кримінальних законодавств та створення єдиного правового простору для забезпечення ефективного захисту від злочинних посягань, пов'язаних з використанням комп'ютерної техніки.

Одним з основних міжнародних нормативних документів у цій сфері є Конвенція про кіберзлочинність, прийнята в рамках Ради Європи 23 листопада 2001 року (підписана Україною 23.11.2001, а ратифікована 07.09.2005), з Додатковим протоколом, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи. Автором досліджувалося питання відповідності чинного кримінального законодавства до цих нормативно-правових актів [121; 119]. Зупинимося лише на головному висновку: порівняльний аналіз Конвенції та КК України дає можливість установити, що більшість діянь, передбачених у Конвенції, визнаються злочинами в українському законодавстві. До таких діянь належать: нелегальне перехоплення (ст.ст. 163, 361, 362 КК); втручання в дані (ст.ст. 361, 362 КК); втручання в систему (ст. 361 КК); злочини, пов'язані з дитячою порнографією (ст. 301 КК); підробка, пов'язана з комп'ютерами (ст.ст. 358, 366 КК); шахрайство, пов'язане з комп'ютерами (ч. 3 ст. 190 КК). Діяння, передбачені Додатковим протоколом до Конвенції, охоплюються ст. 161 КК, яка встановлює відповідальність за порушення рівноправності громадян залежно від їх расової, націо-

нальної належності або ставлення до релігії, та загальними нормами Особливої частини КК України, що передбачають злочини проти свободи совісті (ст. 178 – 181 КК).

Водночас національне кримінальне законодавство, на відміну від Конвенції, не передбачає відповідальності за таке діяння, як навмисний доступ до цілої комп'ютерної системи або її частини без права на це.

Відповідно до Конвенції (ст. 2) *незаконний доступ* уважається закінченим з моменту вчинення діяння, тобто є формальним складом злочину та полягає в навмисному доступі до цілої комп'ютерної системи або її частини без права на це. Конвенцією також передбачено можливість криміналізації тільки незаконного доступу, вчиненого шляхом порушення заходів безпеки. Як видається, таке діяння вже є суспільно небезпечним і піддається криміналізації. Найбільш значущими чинниками його суспільної небезпечності виступають такі: по-перше, для подолання заходів інформаційної безпеки, технічного або програмного характеру необхідні спеціальні знання, специфічні навики, що свідчить про підвищену суспільну небезпечність суб'єкта цього злочину, а по-друге, шкода полягає в істотних матеріальних збитках, зумовлених необхідністю відновлення або заміни системи захисту (за даними фахівців з інформаційної безпеки, створення системи безпеки комп'ютерної інформації для великої фінансової установи коштує близько 15 мільйонів доларів США) [298, с. 44].

Слід зауважити, що в ряді країн несанкціонований доступ передбачається як самостійний склад злочину [419]. Німеччина – стаття 202a КК; Італія – стаття 615b КК; Нідерланди – стаття 138a КК; Швейцарія – стаття 143bis КК; Республіка Білорусь – стаття 349 КК. Незважаючи на відмінності у визначеннях, більшість цих норм містить ознаку, що відбиває не тільки правову специфіку, але й підвищену суспільну небезпечність несанкціонованого доступу. Такою ознакою *є наявність спеціальних засобів захисту комп'ютерної інформації, до якої здійснюється доступ*.

Захист комп'ютерних даних забезпечується різними засобами:

- організаційними;
- технічними;
- програмними.

Організаційні засоби інформаційної безпеки полягають у відповідній роботі з персоналом, який працює з електронно-обчислювальними машинами, системами чи комп'ютерними мережами (добір, постійна перевірка, інструктажі), забезпеченні режиму таємності при функціонуванні комп'ютерних систем і фізичній охороні об'єктів, де опрацьовується, зберігається чи передається комп'ютерна інформація [298, с. 38 – 40.].

До технічних засобів захисту комп'ютерної інформації належать різноманітні пристрої, спеціально призначені для забезпечення цілісності, конфіденційності та доступності комп'ютерної інформації: джерела безперервного живлення апаратури, пристрої стабілізації напруги, мережні фільтри; засоби екранування апаратури, дротових ліній зв'язку та приміщень, у яких знаходиться комп'ютерна техніка; пристрої визначення та фіксації номера абонента, який отримує доступ до електронно-обчислювальної машини, системи чи комп'ютерної мережі, та інші пристрої, що забезпечують безпеку функціонування комп'ютерної техніки [298, с. 40 – 41].

Програмні засоби захисту комп'ютерної інформації являють собою комп'ютерні програми, які розроблені та використовуються спеціально для забезпечення безпеки процесів зберігання, передавання й опрацювання комп'ютерної інформації в електронно-обчислювальній машині, системі чи комп'ютерній мережі.

Необхідно також зауважити, що несанкціонований доступ відбувається не тільки тоді, коли злочинець безпосередньо долає певний технічний чи програмний засіб захисту комп'ютерної інформації. Діяння матиме ознаки несанкціонованого доступу й у випадку, коли власник інформації використовує певну систему захисту, але злочинець отримує доступ до комп'ютерної інформації, не долаючи засоби захисту, а обходячи їх. Напри-

клад, до каналів витоку комп'ютерної інформації відносяться електричні канали, типовим середовищем для яких є стандартна електромережа [213]. Під час роботи електронно-обчислювальні машини створюють наводки в електричній мережі, аналіз яких дозволяє здійснити несанкціонований доступ до комп'ютерної інформації. Припустимо, що власник комп'ютерної інформації встановив засоби екранування обладнання (технічний засіб захисту комп'ютерної інформації) та систему автентифікації користувачів (програмний засіб), але злочинець, не порушуючи цих засобів, отримує несанкціонований доступ через електричні канали витоку комп'ютерної інформації. У діях такої особи наявні ознаки несанкціонованого доступу до комп'ютерної інформації.

З урахуванням вищевикладеного незаконний доступ можна було б визначити так: *одержання винним можливості ознайомлюватися, знищувати, перекручувати або блокувати комп'ютерні дані, що мають специфічні організаційні, технічні або програмні засоби захисту*. Зауважимо, що як і розповсюдження або збут шкідливих програмних засобів, незаконний доступ не може вважатися таким посяганням, що має самостійну суспільну небезпечність. Це з очевидністю випливає з наведених вище положень щодо формулювання законодавчих визначень комп'ютерних злочинів з урахуванням вимоги їх відповідності специфіці суспільної небезпечності цих посягань. Тому пропонується криміналізувати його як кваліфікуючу ознаку злочинів проти власності на комп'ютерні дані.

Досліджуючи Конвенцію, ми маємо також зазначити, що національне кримінальне законодавство прямо не передбачає відповідальності за такі дії, як:

1) навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5 Конвенції;

2) володіння пристроями, включаючи комп'ютерні програми, створені або адаптовані насамперед з метою вчинення будь-якого зі злочинів, перелічених у статтях 2 – 5 Конвенції, або комп'ютерними паролями, кодами доступу або подібними даними, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5 Конвенції, з наміром використання зазначених предметів для вчинення будь-якого зі злочинів, перерахованих у статтях 2 – 5.

Однак видається, що кримінальне законодавство містить достатньо засобів кримінально-правової охорони від посягань, що вчиняються у співучасті, а також засобів протидії попередній злочинній діяльності. Так, ураховуючи визначення Конвенції, конститутивною ознакою яких є мета подальшого вчинення злочинів, навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних являють собою пособництво у вчиненні відповідних злочинів. У свою чергу, володіння шкідливими засобами з метою подальшого вчинення злочинів необхідно, відповідно до національного законодавства, уважати готуванням. Як ми бачили з наведених вище визначень, Конвенція пропонує встановлювати кримінальну відповідальність не просто за володіння, розповсюдження або придбання шкідливих програмних чи технічних засобів, кодів доступу чи іншої подібної інформації, а лише в тому випадку, коли ці дії вчиняються з метою подальшого скоєння комп'ютерних злочинів. Таким чином, Конвенція, на нашу думку, містить достатньо вдале формулювання, що чітко відображає суспільну небезпечність діянь, пов'язаних зі шкідливими програмними чи технічними даними.

Значний інтерес становить також дослідження Закону України "Про ратифікацію Конвенції про кіберзлочинність" від 7 вересня 2005 року. Як видається, у цьому законі також містяться недоліки, пов'язані з неадекватним відображенням ре-

ального змісту суспільної небезпечності досліджуваних посягань. Так, Конвенція формулює типові ознаки складів комп'ютерних злочинів та пропонує механізм так званих застережень, який дозволяє максимально враховувати особливості національного розуміння понять "злочин" та "суспільна небезпечність" на рівні законодавств окремих держав. Україна використовує цей механізм для того, щоб відмовитися від криміналізації:

1) виготовлення, придбання для використання, надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створені або адаптовані насамперед із метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 Конвенції;

2) виготовлення і придбання для використання комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2 –5 Конвенції;

3) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації.

На цьому перелік застережень закінчується. І це фактично призводить до того, що Україна бере на себе зобов'язання визнавати злочинами діяння, які не можна вважати суспільно небезпечними в контексті національного правового поля. Наприклад, у пункті 1 статті 4 Конвенції пропонується встановлювати відповідальність за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. Україною ця норма ратифікована без застережень. Вище ми наводили аргументи недоцільності визнання злочином незаконних дій з інформацією без зазначення наслідків подібних дій для суспільних відносин, у межах яких використовується інформація, що є предметом посягання. Тому доцільніше було б ратифіковувати цю норму із застереженням, яке в п. 2 ст. 4 Конвенції сформульовано таким чином: "Сторона може залишити за собою право вимагати, щоб

поведінка, описана в пункті 1, завдавала серйозну шкоду". Ратифікація цієї норми з таким застереженням означала б, що Україна зобов'язується криміналізувати лише ті незаконні дії з інформацією, які завдають "серйозної шкоди". Таке рішення більшою мірою відповідало б визначеній вище специфіці суспільної небезпечності комп'ютерних злочинів.

Подібні зауваження стосуються й невикористання Україною можливостей ратифікації із застереженнями, що містяться в ст.ст. 2, 3, 7 Конвенції. Так, криміналізація незаконного доступу (ст. 2) можлива із застереженням, що стосується мети подібних дій. У документі зазначається, що сторона може вимагати, щоб таке правопорушення було вчинено з недобросовісною метою. Отже, доречніше було б приєднатися до цієї частини Конвенції саме з таким застереженням, яке пропонується, але Україною не використане. Застереження щодо мети наявні і в нормах Конвенції щодо кримінальної відповідальності за нелегальне перехоплення (ст. 3) та підробку, пов'язану з комп'ютерами (ст. 7). Їх використання є необхідним для приведення зобов'язань, узятих на себе Україною у сфері гармонізації кримінального законодавства, у відповідність до реальних потреб суспільства та національних особливостей кримінальної правотворчості. Ситуацію, що склалася, можна назвати, використовуючи термінологічний апарат дослідження А.Е. Жалинського [95, с. 216], порушенням національного кримінально-правового суверенітету. Слід погодитися з В.М. Литвином, який стверджував, що "копіювання нормативних розробок інших держав без відповідної адаптації нерідко привносить у нашу правову систему норми і принципи, нехарактерні для неї" [наводиться за 382, с. 36]. У цьому контексті заслуговує на увагу і пропозиція В.Д. Швеця щодо законодавчої заборони ухвалення законів про ратифікацію міжнародно-правових актів стосовно злочинної поведінки без аналізу питань кваліфікації визначених у цих актах діянь за чинним КК України [382, с. 38].

Окремо зауважимо, що наукові дослідження питань імплементації положень Конвенції характеризуються іншими резуль-

татами. Як можна судити з автореферату дисертації М.В. Плугатиря за темою "Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації", питання зміни обсягу зобов'язань, що виникли при ратифікації Конвенції, та можливостей використання системи застережень не розглядалися. Більше того, автор наполягає на криміналізації несанкціонованого втручання як формального складу злочину, указуючи на те, що "настання наслідків має бути визначене як кваліфікований склад несанкціонованого втручання" [270, с. 12], а також зазначає, що "несанкціоноване перехоплення або копіювання, передбачене у ч. 2 ст. 362 КК України, слід визначити як злочин з формальним складом" [270, с. 12]. Такі висновки знову ж таки повертають нас до питання інфляції закону про кримінальну відповідальність та необхідності врахування дійсної суспільної небезпечності посягань при формулюванні законотворчих пропозицій.

Таким чином, стосовно відповідності національного кримінального законодавства про злочини у сфері використання інформаційних технологій принципу міжнародно-правової необхідності та допустимості криміналізації маємо констатувати таке: 1) у цілому національне законодавство відповідає ратифікованим міжнародним нормативно-правовим актам, а виняток становить лише некриміналізований чинним законодавством незаконний доступ; 2) має місце надлишкова ратифікація, яка зобов'язує на рівні національного законодавства визнавати злочинами діяння, які не характеризуються суспільною небезпекністю; 3) подальша робота щодо вдосконалення чинного законодавства потребує внесення нових застережень до Закону України "Про ратифікацію Конвенції про кіберзлочинність". Внесення таких застережень дозволить забезпечити виконання принципу міжнародно-правової необхідності та допустимості криміналізації при внесенні до КК змін, доцільність яких було обґрунтовано в цій главі (додаток 10).

Висновки до четвертої глави

Здійснений аналіз засобів кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій дає змогу зробити такі висновки:

1. Ключовою позицією в побудові механізму кримінально-правової охорони суспільних відносин у сфері використання комп'ютерної техніки та мереж електрозв'язку є сутність суспільної небезпечності відповідних посягань. Вона не є самостійною й визначається головним чином соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це й визначає суспільну небезпечність конкретного посягання у сфері використання інформаційних технологій.

2. Чинне законодавство про кримінальну відповідальність передбачає певну систему кримінально-правових засобів охорони суспільних відносин у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку. Разом із тим, аналіз відповідних норм КК свідчить про те, що зазначену специфіку суспільної небезпечності враховано не повною мірою. Також спостерігається порушення низки принципів криміналізації.

3. При криміналізації злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку було порушено принцип суспільної небезпечності: через відсутність у законодавчих визначеннях злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку чітких критеріїв суспільної небезпечності під кримінально-правову заборону та, відповідно, до сфери впливу кримінальної юстиції потрапляють не тільки діяння, що дійсно є суспільно небезпечними, але й діяння, які такими не є. Це різко негативно відбивається на ефективності кримінально-правової охо-

рони інформаційної безпеки у сфері використання інформаційних технологій.

4. Певне зменшення ефективності кримінально-правових засобів охорони інформаційних суспільних відносин зумовлене *недоліками диференціації відповідальності залежно від заподіяної шкоди* та *відсутністю* в нормах досліджуваного розділу спеціальної вказівки на можливість так званої *змішаної повторності*.

5. Порушено принцип визначеності та єдності термінології. У ст.ст. 361 – 363-1 при формулюванні ознак злочинних діянь використовується термінологія, що відрізняється від тієї, яка застосовується при формулюванні ознак суміжних адміністративних правопорушень. *Відсутність єдності* термінології значно зменшує ефективність відповідних норм як кримінального, так і адміністративного законодавства. Норми розділу XVI містять терміни, що *неоднаково визначаються* як на рівні законодавства, так і на рівні наукового тлумачення, що звужує можливості його використання для охорони відповідних суспільних відносин. Використання в диспозиціях розгляданих норм переліку технічних засобів оброблення інформації створює небезпеку "технологічної залежності" законодавства.

6. Чинна редакція ст. 361-2 дозволяє говорити як про надлишковість заборони, що в ній сформульована, так і про формування цією нормою певних прогалин у законодавстві. Надлишковість стосується криміналізації діянь, які не можна визнавати суспільно небезпечними в контексті інших норм щодо відповідальності за незаконні дії з інформацією з обмеженим доступом. Прогалини пов'язані з невдалим формулюванням ознак предмета, які значно звужують можливості норми, роблять кримінально-правові засоби, передбачені нею, такими, що не відповідають сучасним потребам протидії злочинам у сфері використання інформаційних технологій.

7. Конструкція об'єктивної сторони ст. 361 КК України зумовлює прогалини, що полягають у неможливості притягнення до кримінальної відповідальності осіб, які спричиняють зазначені в нормі суспільно небезпечні наслідки без вчинення передбаченого в нормі діяння.

8. Певні прогалини створює законодавче визначення суб'єкта злочину, передбаченого ст. 363 КК, яке не відповідає можливим формам об'єктивної сторони посягання. Також неефективність цієї норми зумовлюється недоліками законодавчого регулювання використання засобів захисту інформації.

9. Прогалини мають місце при формулюванні кримінально-правової заборони масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК). Вони полягають у тому, що відповідальність за розповсюдження спаму пов'язана з наслідками, які є абсолютно нетиповими для подібних дій, а отже, переважна більшість випадків розповсюдження спаму не підпадає під ознаки злочину, передбаченого цією нормою. Недосконалим, таким, що зменшує ефективність кримінально-правової охорони, є також матеріально-правове регулювання множинного розсилання телекомунікаційних повідомлень.

10. Установлено порушення принципу повноти складу. Воно полягає як у формулюванні занадто громіздких законодавчих визначень, що ускладнюють установлення змісту ознак конкретних складів злочинів (ст. 361 КК передбачає відповідальність за два абсолютно самостійні склади злочинів), так і в недостатній визначеності складів конкретних комп'ютерних злочинів у диспозиціях відповідних кримінально-правових норм (відсутність чітких положень щодо змісту суб'єктивної сторони злочинів, передбачених ст.ст. 361 – 363-1 КК, недостатньо конкретне формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 362 КК).

11. Дослідження відповідності національного кримінального законодавства про злочини у сфері використання інформаційних технологій принципу міжнародно-правової необхідності та допустимості криміналізації дозволяє казати про надлишковість зобов'язань, узятих на себе Україною при ратифікації Конвенції про кіберзлочинність, та необхідність внесення нових застережень до Закону України "Про ратифікацію Конвенції про кіберзлочинність".

12. Для розв'язання перелічених проблемних аспектів наводиться низка законотворчих пропозицій, що знайшли відбиття в проекті нової редакції розділу XVI КК України (додаток 10), а саме:

- включити до нормативних визначень досліджуваних злочинів такі "індикатори" суспільної небезпечності, як: порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб; порушення реалізації державних чи громадських інтересів; порушення діяльності юридичної особи;

- використовувати термін "комп'ютерні дані" для позначення предмета передбачених у розділі злочинів;

- виключити ст. 361-2 із Кримінального кодексу, однак повернутися до питання криміналізації збуту або розповсюдження відомостей з обмеженим доступом у розділі, присвяченому дослідженню кримінально-правових засобів охорони суспільних відносин щодо забезпечення доступу до інформації;

- відмовитися від формулювання ознак досліджуваних злочинів з використанням вказівки на діяння у вигляді несанкціонованого втручання в роботу комп'ютерної техніки;

- визнати суб'єктом порушення правил експлуатації комп'ютерних систем, порядку чи правил захисту комп'ютерних даних особу, яка відповідає за дотримання вимог інформаційної безпеки;

- встановити відповідальність за розсилання спаму в контексті порушення правил здійснення розсилання масових телекомунікаційних повідомлень;

- передбачити кримінальну відповідальність за несанкціоноване втручання в роботу мереж електрозв'язку в окремій статті КК;

- чітко сформулювати ознаки суб'єктивної сторони в кримінально-правових нормах, що передбачають відповідальність за злочини у сфері використання інформаційних технологій;

- сформулювати ознаки суб'єкта так званих "інсайдерських" злочинних посягань на комп'ютерні дані як особи, що

має правомірний доступ до комп'ютерних даних у зв'язку із займаною посадою або спеціальними повноваженнями;

- використовувати для позначення відповідної форми порушення права власності на комп'ютерні дані термін "порушення цілісності інформації";

- розглядати дії, що призводять до витоку інформації, не як злочин у сфері використання інформаційних технологій, а як посягання на відносин щодо забезпечення доступу до інформаційних ресурсів;

- криміналізувати незаконні дії зі шкідливими програмними чи технічними засобами, а також незаконний доступ як кваліфікуючі ознаки посягань на відносини власності на комп'ютерні дані (не як самостійних злочинів);

- відбити диференціацію тяжкості заподіяної шкоди в конструкції складів комп'ютерних злочинів;

- передбачити можливості змішаної повторності.

13. Для врахування динамічності досліджуваних злочинів видається необхідним нормативно закріпити вимогу періодичного аналізу тенденцій розвитку злочинів у сфері використання інформаційних технологій, чинників їх суспільної небезпечності, соціальних потреб у відповідних кримінально-правових заборонах та ефективності їх застосування у форматі засідань відповідних комітетів Верховної Ради України за участю представників правоохоронних і судових органів.

Глава 5

Кримінально-правова охорона суспільних відносин забезпечення доступу до інформаційного ресурсу

Місце і значущість відносин забезпечення доступу до інформаційного ресурсу в системі інформаційної безпеки визначаються такими міркуваннями. Суб'єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією. Такий стан досягається соціальною активністю в трьох взаємопов'язаних групах суспільних відносин: у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного ресурсу. У межах першої групи виконується завдання забезпечення функціонування ефективних засобів інформаційної діяльності, другої – забезпечення можливості суб'єктів отримувати доступ до необхідних інформаційних ресурсів, третьої – забезпечення формування інформаційного ресурсу, що відповідає потребам суб'єктів. Характеристика значущості певної групи суспільних відносин інформаційної безпеки дозволяє дати відповідь на питання щодо сутності відповідних порушень інформаційної безпеки.

Так, сутність порушень інформаційної безпеки, пов'язаних із втручанням у роботу інформаційних технологій, полягає в тому, що незаконні дії з даними в комп'ютерній системі призводять до неможливості або значного ускладнення використання певних технічних засобів інформаційної діяльності. Останнє, у свою чергу, зменшує або виключає можливість реа-

лізації інформаційної потреби певного суб'єкта. Інтенсивність наслідків, що настали через неможливість роботи з комп'ютерними даними, визначає межі кримінально-правового регулювання у сфері використання інформаційних ресурсів.

Сутність порушень інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу полягає в тому, що ускладнення чи унеможливлення реалізації інформаційної потреби зумовлюється або порушенням установленого режиму доступу до певного ресурсу, або неправомірним обмеженням доступу до певної інформації.

У загальному розумінні правове регулювання відносин забезпечення доступу до інформації є балансуванням двох груп протилежних соціальних інтересів: з одного боку – інтересів певних суб'єктів в обмеженні доступу до інформації, а з іншого – інтересів певних суб'єктів в отриманні інформації. Інтенсивність наслідків, що настають через порушення цих інтересів, має визначати межі кримінально-правового регулювання у сфері забезпечення доступу до інформаційного ресурсу. Дослідженню чинного законодавства про кримінальну відповідальність за порушення інформаційної безпеки в розгляданій сфері, установленню критеріїв суспільної небезпечності відповідних посягань на інформаційну безпеку та відповідності їм кримінально-правових заборон, що містяться в КК, і присвячено цю главу.

5.1. Аналіз законодавства про кримінальну відповідальність за незаконні дії з інформацією з обмеженим доступом

У загальному розумінні зміст відносин щодо інформації з обмеженим доступом складається з права одних суб'єктів обмежувати коло осіб, які мають доступ до певної інформації, і кореспондуючого з цим права обов'язку інших суб'єктів не порушувати встановлені обмеження. Ураховуючи це, сформу-

люємо принципово можливі види порушень таких відносин. Видається, що кожне посягання на відносини у сфері обмеження доступу до інформації можна віднести до одного з наступних видів: 1) отримання незаконного доступу до інформації; 2) надання незаконного доступу до інформації.

Під отриманням незаконного доступу будемо розуміти результат дій зловмисника, що полягає в ознайомленні або отриманні можливості ознайомлення з інформацією, на доступ до якої він не має права.

Надання незаконного доступу, у свою чергу, є результатом дій зловмисника, що полягає у створенні можливості ознайомлення з певною інформацією з обмеженим доступом для особи, яка не має права на це.

Обґрунтування наведеної позиціє не є складним. По-перше, оскільки Закон України "Про інформацію" чітко поділяє всю сукупність інформації на відкриту та з обмеженим доступом, суб'єкти інформаційних відносин можуть бути поділені на дві групи: особи, які мають доступ до інформації з обмеженим доступом, та особи які не мають доступу до такої інформації. По-друге, усі можливі порушення в досліджуваній сфері являють собою порушення порядку доступу до інформації, оскільки саме він виступає підставою відповідної класифікації. Нарешті, по-третє, єдиним можливим порушенням порядку доступу, яке може вчинити особа, котра не має доступу до інформації, є його незаконне отримання. У свою чергу, єдиним можливим порушенням порядку доступу з боку особи, яка має доступ до обмеженої інформації, є його незаконне надання іншим особам.

Аналіз чинного КК дозволяє виділити низку кримінально-правових засобів охорони обмеженого доступу до інформації. До їх числа слід зараховувати ст.ст. 111, 114, 132, 145, 158, 159, 163, 168, 182, 209-1, 231, 231-1, 232, 328, 330, 361-2, 361, 362, 376-1, 381, 387, 422.

Розподілимо ці норми на групи відповідно до змісту передбачених ними порушень. До першої групи віднесемо порушення, пов'язані з отриманням незаконного доступу, до другої – з наданням. Зазначимо, що більшість зазначених норм необхідно буде віднести як до першої, так і до другої групи, оскільки досить часто в одній нормі міститься заборона як отримання, так і надання незаконного доступу до певної інформації з обмеженим доступом. Наприклад, "передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю…" (ст. 114), "незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди…" (ст. 182), "умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей…" (ст. 231) тощо. Окремо зауважимо, що в диспозиціях низки норм визначені види порушення обмеженого доступу до інформації не розмежовуються. У цих статтях використовуються такі терміни, що охоплюють як надання, так і отримання незаконного доступу. Наприклад, "несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку… інформації" (ст. 361). Формулюванням "що призвело до витоку" охоплюються як випадки незаконного ознайомлення суб'єкта злочину з певною інформацією з обмеженим доступом, так і випадки створення внаслідок дій суб'єкта можливості ознайомлення з такою інформацією третіх осіб. Разом із тим, у подальшому викладі наводитимуться аргументи цієї тези. Окремий розгляд кримінально-правових заборон отримання та надання незаконного доступу є необхідним з огляду на різні чинники їх суспільної небезпечності.

Кожну з отриманих груп систематизуємо за методом аналізу контекстної законодавчої оцінки суспільної небезпечності посягань. Таким чином отримаємо послідовність кримінально-правових заборон отримання незаконного доступу до інформації та його надання, упорядковану за рівнем суворості відповідних санкцій (додатки 6, 7).

Подальший аналіз відповідності зазначених у диспозиціях статей чинників суспільної небезпечності конкретних посягань місцю, яке ці норми посідають у встановленій системі кримінально-правових засобів охорони обмеженого доступу до інформації, дозволить дійти обґрунтованих висновків щодо якісної оцінки національного законодавства про кримінальну відповідальність у цій сфері.

Отже, найбільш суспільно небезпечними посяганнями, пов'язаними з отриманням незаконного доступу до інформації, є державна зрада (ст. 111) та шпигунство (ст. 114). Це обґрунтовано передбаченими у відповідних нормах специфічними чинниками їх суспільної небезпечності. По-перше, ці заборони стосуються державної таємниці – одного з найбільш суспільно значущих видів інформаційних ресурсів. По-друге, наявність спеціальної мети передавання відомостей, що становлять предмет посягання, іноземній державі, іноземній організації або їх представникам чітко свідчить, що такі дії потенційно можуть призвести до істотних наслідків для безпеки країни. Таким чином, віднесення перелічених видів незаконного доступу до найбільш небезпечних є обґрунтованим.

Однак подальший розгляд наявної у КК системи кримінально-правових засобів охорони обмеженого доступу до інформації вимагає формулювання низки критичних зауважень.

Наступним за суворістю санкцій видом кримінально караного незаконного доступу до інформації є кваліфіковане порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ч. 2 ст. 163, $I_{кзосн}$ = 80,64). Це законодавче рішення виглядає доволі спірним. Диспозиція ч. 2 ст. 163 КК містить такі кваліфікуючі ознаки, як: вчинення дій щодо державних чи громадських діячів службовою особою або з використанням спеціальних технічних засобів. Оскільки просте порушення таємниці кореспонденції (ч. 1 ст. 163, $I_{кзосн}$ = 19,13) є злочином невеликої тяжкості, навряд чи обґрунтованим є збільшення санкції за означені кваліфіковані види цього посягання до рівня тяжкого злочину (максимальна межа санкції – 7 років

позбавлення волі). Подібне рішення є спірним і з огляду на те, що інші види незаконного доступу до інформації, *кримінальна відповідальність за які пов'язана з настанням певних наслідків, караються значно м'якше*. Так, наприклад, незаконне збирання відомостей, що становлять комерційну або банківську таємницю, відповідальність за яке настає лише в разі заподіяння істотної шкоди суб'єктові господарської діяльності, передбачає покарання у вигляді штрафу від трьох до восьми тисяч НМДГ (ст. 231, $I_{кзосн}$ = 39,86).

Наступну групу посягань складають кваліфіковані види незаконного доступу до комп'ютерної інформації, а саме: умисні несанкціоновані дії з інформацією, що міститься в базі даних Державного реєстру виборців, вчинені шляхом несанкціонованого доступу до бази даних Державного реєстру виборців, якщо такі дії вплинули на результати голосування виборців на виборчій дільниці або в межах виборчого округу, або призвели до неможливості визначити волевиявлення виборців на виборчій дільниці чи у відповідних виборах, а також вчинені за попередньою змовою групою осіб (ч. 12 ст. 158, $I_{кзосн}$ = 79,73); несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, вчинені за попередньою змовою групою осіб шляхом несанкціонованого доступу до автоматизованої системи документообігу суду (ч. 2 ст. 376-1, $I_{кзосн}$ = 79,50); несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку інформації, вчинене повторно або за попередньою змовою групою осіб, або якщо воно заподіяло значну шкоду (ч. 2 ст. 361, $I_{кзосн}$ = 78,82). Ці посягання доцільно розглядати разом, оскільки вони характеризуються дуже близькими значеннями індексів КЗОСН. За умови тотожності верхньої межі найбільш суворого основного покарання (6 років позбавлення волі) відповідні санкції розрізняються: наявністю альтернативного основного покарання (обмеження волі), нижньою межею додаткового покарання у вигляді позбавлення права, а також положеннями щодо застосування спеціальної конфіскації.

Стосовно розгляданої групи насамперед зазначимо, що суворість відповідних санкцій є ще одним аргументом на користь тези про спірність законодавчої оцінки суспільної небезпечності кваліфікованого порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ч. 2 ст. 163, $I_{кзосн} = 80,64$). Згідно з КК прослуховування телефонних розмов з використанням спеціального технічного засобу є небезпечнішим за несанкціоноване втручання в роботу Державного реєстру виборців, яке вплинуло на результати голосування виборців на виборчій дільниці або в межах виборчого округу. Так само незаконне ознайомлення службовою особою зі змістом навіть одного повідомлення електронної пошти слід, виходячи зі змісту КК, уважати більш небезпечним, ніж несанкціоноване втручання в роботу комп'ютерної мережі, що призвело до заподіяння шкоди, яка перевищує 100 неоподатковуваних мінімумів доходів громадян (станом на 1 січня 2011 року – 47050 гривень). Маємо очевидну *невідповідність* подібних *законодавчих оцінок реальній небезпеці* зазначених *посягань*.

Доволі спірною видається також доцільність криміналізації несанкціонованого втручання в роботу спеціалізованих автоматизованих систем. По-перше, санкції ч. 12 ст. 158, ч. 2 ст. 376-1 та ч. 2 ст. 361, як зазначалося раніше, практично однакові. Так само близькими є санкції, передбачені в КК за вчинення відповідних некваліфікованих посягань (ч. 11 ст. 158, ч. 1 ст. 376-1, ч. 1 ст. 361). Тобто законодавча оцінка суспільної небезпечності як простого, так і кваліфікованого отримання незаконного доступу до будь-якої комп'ютерної інформації (ст. 361) практично ідентична оцінці незаконного ознайомлення з інформацією, що обробляється в Державному реєстрі виборців (чч. 11, 12 ст. 158) або в автоматизованій системі документообігу суду (ст. 376-1). Тому виникає *питання доцільності створення певних спеціальних норм за умови практичної ідентичності їх санкцій загальній нормі*. По-друге, Державним реєстром виборців, а також автоматизованими системами документообігу судів не обмежуються наявні інформаційні системи, у яких обробля-

ються відомості великого суспільного значення. Це автоматизована система "Рада", потужні інформаційні системи правоохоронних органів, системи дистанційного банківського обслуговування, системи автоматизованого керування складними та небезпечними виробничими процесами. Крім того, із розвитком інформатизації варто очікувати появи нових автоматизованих інформаційних систем з важливою інформацією. Наприклад, введення біометричних паспортів зумовить створення подібної інфраструктури. Однак це не означає, що кожна подібна система вимагає чи вимагатиме відповідних спеціалізованих кримінально-правових засобів безпеки та, з урахуванням законодавчих пропозицій зроблених у попередній главі, свідчить про доцільність виключення з Кримінального кодексу чч. 11 та 12 ст. 158, а також ст. 376-1.

Структурним недоліком чинної системи кримінально-правових засобів забезпечення обмеження доступу до інформації є, як видається, неправильна оцінка значення автоматизованої обробки даних. Це виявляється в *необґрунтованому підвищенні санкцій за несанкціонований доступ у разі його вчинення з використанням інформаційних технологій*.

Так, *за умови настання однакових наслідків* – вплив на результати голосування виборців на виборчій дільниці або в межах виборчого округу, або неможливість визначити волевиявлення виборців на виборчій дільниці чи у відповідних виборах (референдумі) – *незаконний доступ до відомостей у Державному реєстрі виборців* (ч. 12 ст. 158, $I_{кзосн} = 79,73$) *карається більш суворо, ніж викрадення виборчого протоколу чи протоколу комісії з референдуму або скриньки з бюлетенями* (ч. 6 ст. 158, $I_{кзосн} = 74,72$), які також можна вважати специфічними формами отримання незаконного доступу до інформації. При цьому однозначної відповіді на питання, що є більш суспільно небезпечним – викрадення чи несанкціоноване втручання, – немає.

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, є кримінально караними, *якщо вони заподіяли істотну шкоду суб'єкту*

господарської діяльності (ст. 231, $I_{кзосн}$ = 39,86). Однак це посягання визнано законодавцем *менш небезпечним, ніж просте несанкціоноване втручання* в роботу комп'ютерної техніки, тобто таке, *яке не призвело до істотної шкоди* (ч. 1 ст. 361, $I_{кзосн}$ = 53,30). У свою чергу санкція норми, що передбачає відповідальність за несанкціоноване втручання, яке спричинило заподіяння істотної шкоди (ч. 2 ст. 361, $I_{кзосн}$ = 78,82), є набагато суворішою за санкцію ст. 231 КК. Таке законодавче рішення суперечить аксіоматичному положенню, сформульованому нами в попередній главі: суспільна небезпечність посягань у сфері використання комп'ютерної техніки не є самодостатньою, а визначається значущістю тих відносин, для інтенсифікації яких використовуються інформаційні технології.

Викрадення, привласнення, вимагання офіційних документів або заволодіння ними шляхом шахрайства чи зловживання особою своїм службовим становищем, *вчинене з корисливих мотивів або в інших особистих інтересах, якщо воно спричинило порушення роботи підприємства, установи чи організації, або вчинене щодо особливо важливих документів* (ч. 2 ст. 357, $I_{кзосн}$ = 45,10), відповідно до чинного КК за рівнем суспільної небезпечності *є близьким до простого несанкціонованого втручання* в роботу комп'ютерної техніки або мереж електрозв'язку, що призвело до витоку інформації (ч. 1 ст. 361, $I_{кзосн}$ = 53,30)*. Якщо пригадати наведені в попередній главі результати дослідження національної судової практики, виникає риторичне питання: чи можна вважати близькими за рівнем суспільної небезпечності викрадення офіційного документа, вчинене з корисливих мотивів, якщо воно спричинило порушення роботи підприємства, та несанкціоноване втручання, що призвело до витоку інформації у вигляді незаконного підключення до

* У цьому випадку спостерігається значна різниця індексів КЗОСН за умови близьких розмірів санкцій. Ця особливість використовуваного методу розглядалася в підглаві 2.2. У подібних випадках додатково досліджуватимемо інші показники законодавчої оцінки суспільної небезпечності діяння, зокрема верхню межу покарання у вигляді позбавлення волі.

мереж кабельного телебачення? Разом із тим, близький за об'єктивним рівнем суспільної небезпечності злочин – несанкціоноване втручання, що призвело до істотної шкоди (ч. 2 ст. 361, $I_{кзосн}$ = 78,82), характеризується значно суворішою санкцією. Якщо максимальна межа основного покарання за вчинення злочину, передбаченого ч. 2 ст. 357, становить 3 роки позбавлення волі, то відповідний показник санкції ч. 2 ст. 361 – 6 років позбавлення волі.

Нарешті, неможливо не звернути увагу на те, що на думку законодавця *значно меншою суспільною небезпечністю, ніж просте несанкціоноване втручання* (ч. 1 ст. 361, $I_{кзосн}$ = 53,30) характеризуються такі посягання:

- незаконне збирання інформації про особу без її згоди (ч. 1 ст. 182, $I_{кзосн}$ = 23,69);

- незаконне заволодіння будь-яким способом *паспортом або іншим важливим особистим документом* (ч. 3 ст. 357, $I_{кзосн}$ = 20,73);

- порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ч. 1 ст. 163, $I_{кзосн}$ = 19,13);

- викрадення, привласнення, вимагання *офіційних документів* або заволодіння ними шляхом шахрайства чи зловживання особою своїм службовим становищем, *вчинене з корисливих мотивів або в інших особистих інтересах* (ч. 1 ст. 357, $I_{кзосн}$ = 17,08);

- викрадення виборчого протоколу чи протоколу комісії з референдуму або скриньки з бюлетенями (ч. 5 ст. 158, $I_{кзосн}$ = 16,17).

Якщо просте несанкціоноване втручання є злочином середньої тяжкості, то всі перелічені вище посягання – це злочини невеликої тяжкості. Санкції відповідних норм навіть не передбачають покарання у вигляді позбавлення волі. Наявність у ч. 1 та 3 ст. 357, ч. 5 ст. 158 достатньо чітких критеріїв суспільної небезпечності передбачених ними видів незаконного доступу до інформації (характеристика предмета, мотиву) разом із відсутністю подібних критеріїв у ч. 1 ст. 361 (доведено в попередній главі) та порівнянням індексів КЗОСН зазначених посягань свідчить не на користь чинного КК. Отже, необхідно

актуалізувати питання побудови обґрунтованої та послідовної системи кримінально-правових засобів охорони обмеженого доступу до інформації.

Подібні недоліки властиві й системі кримінально-правових заборон, пов'язаних із незаконним наданням доступу до інформації.

Окремо зазначимо, що до системи кримінально караних видів незаконного надання доступу до інформації належать і посягання, передбачені ст. 361-2. Однак наведені в попередній главі аргументи на користь скасування цієї норми дозволяють, як видається, не повертатися до її розгляду. Таким чином, як і в попередній дослідженій групі, найбільш небезпечними видами незаконного надання доступу до інформації виступають державна зрада (ст. 111) та шпигунство (ст. 114). Знову ж таки це не викликає заперечень і є обґрунтованим з точки зору об'єктивної суспільної небезпечності незаконної передачі іноземним країнам або організаціям відомостей, що становлять державну таємницю.

Водночас достатньо спірним є рішення законодавця про те, що передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам економічних, науково-технічних або інших відомостей, що становлять конфіденційну інформацію, яка є власністю держави, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, вчинені з корисливих мотивів або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб (ч. 2 ст. 330, $I_{кзосн} = 85{,}19$), є близькими за рівнем суспільної небезпечності до розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, якщо воно спричинило тяжкі наслідки (ч. 2 ст. 328, $I_{кзосн} = 83{,}37$). Крім того посягання, передбачене ч. 2 ст. 330, на думку законодавця, є

менш небезпечним, ніж розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради, якщо воно спричинило тяжкі наслідки (ч. 3 ст. 422, $I_{кзосн} = 88{,}38$). Хоча на рівні основних складів (ч. 1 ст. 328, ч. 1 ст. 330, ч. 1 ст. 422) маємо приблизно однакову оцінку суспільної небезпечності цих посягань: максимальне основне покарання – 5 років позбавлення волі. Видається, що така оцінка суспільної небезпечності розголошення відомостей, що становлять державну таємницю, та передачі або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам конфіденційної інформації, яка є власністю держави, є помилковою, такою, що не відповідає змісту розгляданих посягань. Однак ця помилка породжує, у свою чергу, нові недоліки законодавчої оцінки суспільної небезпечності вже на рівні встановлення меж покарання за кваліфіковані види відповідних посягань.

Не можна не звернути уваги й на те, що некваліфіковані види розголошення відомостей, які становлять державну таємницю (ч. 1 ст. 328, ч. 1 ст. 422), а також просте збирання або передача конфіденційної інформації, яка є власністю держави (ч. 1 ст. 330), за рівнем законодавчої оцінки суспільної небезпечності є близькими до розголошення відомостей про заходи безпеки щодо особи, узятої під захист, *якщо воно спричинило смерть цієї особи* (ч. 2 ст. 381, $I_{кзосн} = 61{,}69$). Максимальна межа основного покарання за вчинення цих посягань – 5 років позбавлення волі. Знову ж таки маємо таку законодавчу оцінку небезпечності незаконного надання доступу до інформації, яка не відповідає його об'єктивній суспільній небезпечності.

При розгляді досліджуваної групи заборон підтверджується й висловлене раніше положення щодо структурного недоліку системи кримінально-правових засобів забезпечення обмеження доступу до інформації. Він, як зазначалося, полягає в неправильній, необґрунтовано завищеній оцінці значення автоматизованої обробки даних.

У межах групи кримінально-правових заборон, пов'язаних з незаконним наданням доступу до інформації, цей недолік

виявляється у завищеній оцінці суспільної небезпечності тих видів надання такого доступу, єдиним чинником заборони яких є спосіб – незаконні операції з комп'ютерною технікою. Так, злочинні посягання, які пов'язані з незаконним наданням доступу до комп'ютерної інформації (ч. 1 ст. 361, ч. 2, ст. 362, ч. 11 ст. 158, ч. 1 ст. 376-1) та *кримінальна відповідальність за які не залежить від настання інших, крім витоку, наслідків,* за рівнем законодавчої оцінки суспільної небезпечності (верхня межа основного покарання дорівнює трьом рокам позбавлення волі) близькі до таких злочинів:

- порушення таємниці голосування, *вчинене членом виборчої комісії або комісії з референдуму чи іншою службовою особою з використанням свого службового становища* (ч. 2 ст. 159, $I_{кзосн}$ = 56,26);

- розголошення таємниці усиновлення (удочеріння) усупереч волі усиновителя (удочерителя), *вчинене службовою особою або працівником медичного закладу*, яким відомості про усиновлення (удочеріння) стали відомі по службі чи по роботі, або *якщо воно спричинило тяжкі наслідки* (ч. 2 ст. 168, $I_{кзосн}$ = 53,76).

Крім цього злочинні посягання, пов'язані з незаконним наданням доступу до комп'ютерної інформації (ч. 1 ст. 361, ч. 2, ст. 362, ч. 11 ст. 158, ч. 1 ст. 376-1), виходячи з аналізу КК, є більш небезпечними, ніж:

- розголошення в будь-якому вигляді інформації, яка відповідно до закону надається спеціально уповноваженому центральному органові виконавчої влади зі спеціальним статусом з питань фінансового моніторингу, *особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю*, якщо такі дії заподіяли *істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб* (ч. 2 ст. 209-1, $I_{кзосн}$ = 39,64);

- незаконне використання таких відомостей, які становлять комерційну або банківську таємницю, *якщо це заподіяло істотну шкоду* суб'єктові господарської діяльності (ст. 231, $I_{кзосн}$ = 39,86);

- розголошення відомостей про заходи безпеки щодо особи, узятої під захист, службовою особою, якою прийнято рі-

шення про ці заходи, особою, яка їх здійснює, або службовою особою, якій ці рішення стали відомі у зв'язку з її службовим становищем, а так само особою, узятою під захист, *якщо ці дії спричинили шкоду здоров'ю особи*, узятої під захист (ч. 1 ст. 381, $I_{кзосн}$ = 20,05);

- розголошення даних досудового слідства або дізнання, *вчинене суддею, прокурором, слідчим, працівником органу дізнання, оперативно-розшукового органу* незалежно від того, чи брала ця особа безпосередньо участь у досудовому слідстві чи дізнанні, *якщо розголошені дані ганьблять людину, принижують її честь і гідність* (ч. 2 ст. 387, $I_{кзосн}$ = 11,16);

- умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння *спричинило тяжкі наслідки* (ст. 145, $I_{кзосн}$ = 6,38).

Виділені курсивом ознаки відповідних видів незаконного надання доступу до інформації дають їх чітку та прозору характеристику як суспільно небезпечних. Разом із тим, уже неодноразово зазначалося, що використання для надання незаконного доступу до певної інформації комп'ютерної техніки ще не дозволяє казати про його суспільну небезпечність. Однак проведений аналіз свідчить про те, що в чинному КК *настання об'єктивних наслідків від незаконного надання доступу* до інформації *розглядається як таке, що має приблизно однаковий або навіть менш значний вплив* на суспільну небезпечність посягання, *ніж надання такого доступу з використанням комп'ютерної техніки*.

Недоцільність цього підходу проілюструємо на прикладі. Близькими за змістом можна вважати такі посягання, як несанкціоноване перехоплення або копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації (ч. 2 ст. 362, $I_{кзосн}$ = 58,31), та умисне розголошення комерційної або банківської таємниці без згоди її власника особою,

якій ця таємниця відома у зв'язку з професійною або службовою діяльністю (ст. 232, $I_{кзосн} = 4,56$). Однак якщо для настання кримінальної відповідальності за перший злочин достатньо лише витоку інформації, то за другий злочин особа відповідатиме лише тоді, коли мали місце корисливі чи інші особисті мотиви і розголошення завдало істотної шкоди суб'єктові господарської діяльності. При цьому аналіз санкцій відповідних норм свідчить про те, що злочин, передбачений ч. 2 ст. 362, розглядається як такий, що є більш суспільно небезпечним, ніж посягання, передбачене ст. 232. Наявність таких законодавчих положень призводить до появи спірних із точки зору доцільності застосування кримінальної юстиції, але цілком правосудних рішень. У попередній главі згадувався вирок Крюківського районного суду м. Кременчука Полтавської області від 2 квітня 2010 року в справі № 1-103/2010. У цьому випадку суд кваліфікував дії винного за ч. 2 ст. 362 КК України, оскільки він протягом серпня – жовтня 2009 року, маючи право доступу до інформації, яка зберігається на його робочому персональному комп'ютері та сервері комп'ютерної мережі КБ ВАТ "Кредмаш", вчинив несанкціоноване копіювання інформації – робочих файлів із розробками "Гроход Дайлида" розробки іншого співробітника підприємства, асфальтозмішувальних установок: "ДС-1863", "ДС-1857", "КДМ-201", які є комерційною таємницею ВАТ "Кредмаш" та повинні зберігатися в конструкторському бюро підприємства. Він виніс інформацію за межі ВАТ "Кредмаш", що призвело до її витоку, який виразився в можливості ознайомлення із цією інформацією сторонніх осіб, котрі не мали права доступу до неї [153]. Якби цей інженер роздрукував відповідні дані та намагався винести за межі підприємства паперові носії, то його дії вже неможливо було б кваліфікувати за ст. 232, оскільки дані про шкоду, заподіяну суб'єктові господарської діяльності, у вироку не наводяться. Цей приклад показує, що форма представлення інформації необґрунтовано розглядається в чинному КК як фактор суспільної небезпечності незаконного надання доступу до інформації. У наведеному випадку тільки той факт, що інформація

була комп'ютерною, "забезпечив" кваліфікацію діяння як злочину середньої тяжкості, водночас як ті самі дії, але щодо інформації в іншому вигляді взагалі не є злочинними.

Слід також зазначити непослідовність законодавчої оцінки подібних за змістом ознак, що характеризують суб'єкта посягання. Так, аналіз диспозицій і санкцій свідчить про те, що однаково суспільно небезпечним є надання незаконного доступу до комп'ютерної інформації, вчинене як спеціальним, так і загальним суб'єктом. Санкції ч. 1 та ч. 2 ст. 361 ($I_{кзосн} = 53,30$; $I_{кзосн} = 78,82$), яка передбачає відповідальність загального суб'єкта за витік інформації, близькі за змістом до санкцій, що містяться в чч. 2 та 3 ст. 362 ($I_{кзосн} = 58,31$; $I_{кзосн} = 78,82$). Максимальна межа основного покарання за простий злочин – три роки позбавлення волі. Вони розрізняються лише наявністю альтернативних покарань та інтенсивністю додаткових. У свою чергу санкції за кваліфіковані посягання (заподіяння істотної шкоди, вчинення злочину повторно або за попередньою змовою групою осіб) є тотожними. У нормах, що передбачають спеціальні види надання незаконного доступу до комп'ютерної інформації (ч. 11, 12 ст. 158, та ст. 376-1), на рівні диспозиції дається однакова правова оцінка вчинення діяння як спеціальним, так і загальним суб'єктом. Наприклад, у диспозиції ч. 1 ст. 376-1: "…несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, чи інше втручання в роботу автоматизованої системи документообігу суду, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до автоматизованої системи документообігу суду". Близьке за змістом формулювання міститься і в ч. 11 ст. 158. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" містить ключові нормативні визначення для тлумачення розгляданих норм, а саме: 1) "доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі"; 2) "несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законо-

давства". Отже, відповідно до чч. 11 – 12 ст. 158 та ст. 376-1 несанкціонований доступ – це отримання особою, яка не має права доступу до спеціалізованої автоматизованої системи, можливості обробляти інформацію в ній. Тобто фактично ці норми за однакові дії – обробку інформації в системі – передбачають однакову відповідальність як спеціальних, так і загальних суб'єктів. Таке положення є додатковим аргументом на користь висловленої в попередній главі тези щодо необхідності криміналізації незаконного доступу як способу незаконного втручання, який полягає в одержанні винним можливості ознайомлюватися, знищувати, перекручувати або блокувати комп'ютерні дані, що мають специфічні організаційні, технічні або програмні засоби захисту. Отже, *у певній групі досліджуваних норм ознаки, що характеризують спеціального суб'єкта посягання, не впливають на законодавчу оцінку суспільної небезпечності діяння*.

Водночас ст. 231 та 232 ($I_{кзосн}$ = 39,86; $I_{кзосн}$ = 4,56), що передбачають відповідальність за надання незаконного доступу до відомостей, що становлять комерційну або банківську таємницю, характеризуються іншим підходом. За умови, що кримінальна відповідальність у цих випадках пов'язана із заподіянням істотної шкоди суб'єктові господарської діяльності, подібні *дії спеціального суб'єкта* – особи, якій "таємниця відома у зв'язку з професійною або службовою діяльністю" – *караються значно м'якше, ніж аналогічні дії загального суб'єкта*. Посягання, передбачене ст. 232 (спеціальний суб'єкт), належить до злочинів невеликої тяжкості. Проте вчинене загальним суб'єктом розголошення комерційної або банківської таємниці, зазначене в диспозиції ст. 231 як "незаконне використання таких відомостей", є злочином середньої тяжкості.

Нарешті, у системі кримінально-правових засобів забезпечення обмеженого доступу до інформації зустрічається й третій, на нашу думку, найбільш обґрунтований підхід: *ознаки, які характеризують спеціального суб'єкта певного виду незаконного надання доступу до інформації, розглядаються як чинники, що підвищують рівень законодавчої оцінки суспільної небезпечності відповід-*

них посягань. Такий підхід спостерігається, наприклад, у нормах, які передбачають відповідальність за таємницю усиновлення (удочеріння). Просте розголошення подібних відомостей, вчинене загальним суб'єктом (ч. 1 ст. 168, $I_{кзосн}$ = 6,15) являє собою злочин невеликої тяжкості, тоді як вчинення посягання "службовою особою або працівником медичного закладу, яким відомості про усиновлення (удочеріння) стали відомі по службі чи по роботі" (ч. 2 ст. 168, $I_{кзосн}$ = 53,76) – злочин середньої тяжкості. Подібний вплив ознак спеціального суб'єкта спостерігається і при встановленні кримінально-правових заборон за розголошення таємниці голосування (ч. 1 ст. 159, $I_{кзосн}$ = 20,05; ч. 2 ст. 159, $I_{кзосн}$ = 56,26).

Аналіз сукупності норм, що передбачають відповідальність за різні види незаконного надання доступу до інформації, допоміг також установити певну непослідовність у формулюванні спеціальних норм. Так, видається цілком обґрунтованим, що формулювання "незаконне … поширення конфіденційної інформації про особу без її згоди", яке міститься в диспозиції ст. 182, дозволяє визначати цю норму як загальну відносно розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132), незаконного розголошення лікарської таємниці (ст. 145), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення відомостей про заходи безпеки щодо особи, узятої під захист (ст. 381), розголошення даних досудового слідства або дізнання (ст. 387). Доцільність виокремлення цих спеціальних заборон викликає певні сумніви після аналізу відповідних санкцій. Виявляється, що з точки зору законодавчої оцінки суспільної небезпечності просте незаконне розголошення загальним суб'єктом будь-якої інформації про особу (ч. 1 ст. 182, $I_{кзосн}$ = 23,69) є близьким до порушення таємниці голосування (ч. 1 ст. 159, $I_{кзосн}$ = 20,05), розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132, $I_{кзосн}$ = 26,88) та роз-

голошення відомостей про заходи безпеки щодо особи, узятої під захист (ч. 1 ст. 381, $I_{кзосн}$ = 20,05). Верхня межа основного покарання за ці злочини складає 3 роки обмеження волі. При цьому до відповідальності за злочин, передбачений ст.ст. 132 та 381, *можуть притягатися тільки спеціальні суб'єкти.* Крім цього розголошення відомостей про заходи безпеки є кримінально караним тільки в тому випадку, коли ці дії "*спричинили шкоду здоров'ю особи, взятої під захист*". Більше того, порушення таємниці приватного життя (ч. 1 ст. 182), відповідно до змісту санкцій, є небезпечним за:

- розголошення даних досудового слідства або дізнання, вчинене *суддею, прокурором, слідчим, працівником органу дізнання, оперативно-розшукового органу* незалежно від того, чи брала ця особа безпосередньо участь у досудовому слідстві чи дізнанні, *якщо розголошені дані ганьблять людину, принижують її честь і гідність* (ч. 2 ст. 387, $I_{кзосн}$ = 11,16);

- умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння *спричинило тяжкі наслідки* (ст. 145, $I_{кзосн}$ = 6,38);

- розголошення таємниці усиновлення (удочеріння) усупереч волі усиновителя (удочерителя) (ч. 1 ст. 168, $I_{кзосн}$ = 6,15).

Навряд чи можна вважати, що в перелічених нормах КК дається об'єктивна оцінка суспільної небезпечності названих посягань. Радше слід погодитися з В.О. Навроцьким, який до негараздів, що "викликані засиллям спеціальних кримінально-правових норм у чинному законодавстві", відносив "відсутність більш-менш чітких критеріїв виділення спеціальних норм". Через що "спеціальні норми виділяються хаотично; часто важко зрозуміти, чому в одних випадках законодавець виділяє спеціальну норму за певною ознакою, а в аналогічних – обходиться без цього" [242, с. 133 – 134].

Необхідно звернути увагу і на непослідовність законодавчих рішень у питанні формулювання ознак кваліфікованих посягань на відносини щодо забезпечення обмеженого доступу до інформації. Вітчизняні науковці, які досліджували за-

гальні питання формулювання кваліфікованих складів злочинів, обґрунтовано доводили, що в КК непоодинокими є випадки порушень форми законодавчого закріплення кваліфікуючих ознак, системності їх вживання та впливу на збільшення міри покарання [4, с. 6 – 11]. Погоджуючись із їхніми висновками, уважаємо за доцільне навести деякі прояви розгляданої проблеми, установлення яких стало можливим в ході розгляду досліджуваних норм. Так, більшість кваліфікованих видів незаконного отримання та надання доступу до комп'ютерної інформації (ч. 12 ст. 158, ч. 2 ст. 361, ч. 3 ст. 362) однією з альтернативних кваліфікуючих ознак передбачають настання певних наслідків (істотна шкода, вплив на результати виборів тощо). Водночас, за умови практичної ідентичності санкцій кваліфікуючою ознакою несанкціонованого втручання в роботу автоматизованої системи документообігу суду (ч. 2 ст. 376-1) передбачено лише вчинення злочину за попередньою змовою групою осіб. Проте цілком зрозуміло, що настання кваліфікованих наслідків у разі вчинення подібного посягання є досить вірогідним. Як уже зазначалося, доволі спірним є рішення законодавця щодо підвищення санкції в ч. 2 ст. 163 ($I_{кзосн}$ = 80,64). Таке рішення виглядає непослідовним ще й з огляду на те, що норма, яку обґрунтовано можна вважати загальною відносно ст. 163, а саме ст. 182 у частині другій передбачає значно м'якшу відповідальність ($I_{кзосн}$ = 66,06), а кваліфікуючими ознаками передбачає настання істотної шкоди та повторність. Виникають цілком закономірні питання. Чому використання спеціального технічного обладнання під час прослуховування телефонних розмов значно підвищує караність діяння, а використання подібних приладів під час незаконного збирання інформації про особу в інший спосіб – ні? Чи обґрунтовано вважати прослуховування телефонних розмов з використанням спеціального обладнання більш небезпечним, ніж розголошення конфіденційної інформації про особу, що заподіяло істотну шкоду охоронюваним законом правам особи?

Системі кримінально-правових засобів охорони обмеженого доступу до інформації властивий і такий недолік, як не-

узгодженість використовуваної термінології. Наприклад, для позначення незаконного отримання доступу до інформації використовуються такі формулювання: "збирання відомостей" (ст.ст. 114, 182), "отримання відомостей" (ст. 231), "порушення таємниці" (ст. 163), "несанкціоновані дії з інформацією" (ч. 11 ст. 158, ст. 376-1), "витік інформації" (ст.ст. 361, 362). Незаконне надання доступу визначається в законі таким чином: "передача відомостей" (ст. 114, 330), "несанкціоновані дії з інформацією" (ч. 11 ст. 158, ст. 376-1), "витік інформації" (ст.ст. 361, 362), "розголошення відомостей" (ст.ст. 132, 328, 381, 422), "розголошення інформації" (ч. 2 ст. 209-1), "розголошення даних" (ст. 387), "розголошення таємниці" (ст. 145, 168, 232), "незаконне використання відомостей" (ст. 182, 231), "поширення інформації" (ст. 182), "порушення таємниці" (ст. 159), "несанкціоновані збут або розповсюдження інформації" (ст. 361-2). При цьому деякі формулювання використовуються з різним змістом. Так, за контекстом ст. 163 порушення таємниці являє собою незаконне отримання або ознайомлення з певними відомостями [188, с. 139]. Водночас таке саме формулювання в ст. 159 застосовується вже в іншому значенні – як "розголошення змісту волевиявлення". Стосовно доцільності використання одного формулювання для позначення як отримання, так і надання доступу зазначимо, що такий підхід через розширення кола діянь, заборонених нормою, призводить до ускладнень урахування об'єктивних чинників суспільної небезпечності відповідних посягань. Наприклад, об'єднання в одній нормі (ст. 231, $I_{кзосн} = 39{,}86$) заборони надання та заборони отримання доступу до інформації призвело до очевидної невідповідності контекстної законодавчої оцінки суспільної небезпечності передбаченого нею посягання його об'єктивній суспільній небезпечності. Ця норма передбачає відповідальність як за отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання, так і за їх використання. Останнє може виявлятися і в розголошенні відомостей [193, с. 638]. Проте якщо збирання таких відомостей з певною метою доцільно розглядати як посягання, що є більш небезпечним,

ніж розголошення таких відомостей особою, якій вони стали відомі у зв'язку з професійною або службовою діяльністю (ст. 232, $I_{кзосн} = 4{,}56$), то цього не можна сказати про розголошення комерційної або банківської таємниці, вчинюване загальним суб'єктом. Розголошення будь-якої таємниці, вчинене особою, котра отримала правомірний доступ до неї, за умови настання однакових наслідків (істотна шкода суб'єктам господарської діяльності) є безсумнівно більш небезпечним, ніж її розголошення, вчинене загальним суб'єктом. Таким чином, *неоднозначність та неузгодженість термінології, що використовується в системі кримінально-правових норм, які передбачають відповідальність за порушення у сфері обмеженого доступу до інформації*, не тільки є *порушенням формальних вимог до тексту закону*, але й значно *ускладнює нормативне відображення об'єктивних чинників суспільної небезпечності* досліджуваних посягань.

Отже, застосування методу контекстної законодавчої оцінки суспільної небезпечності діяння дозволило встановити низку невідповідностей і недоліків передбаченої чинним законодавством про кримінальну відповідальність системи кримінально-правових засобів забезпечення обмеженого доступу до інформації. Установлені недоліки за їх характером можна віднести до формально-логічних та структурно-організаційних.

Однак для отримання обґрунтованої й усебічної оцінки необхідно також проаналізувати відповідність досліджуваної системи засобів кримінально-правової протидії фактичним соціальним потребам у застосуванні кримінальної юстиції. Це можливо здійснити шляхом співставлення змісту досліджуваних заборон із тенденціями розвитку суспільно небезпечних посягань у цій сфері. Проведене дослідження дозволяє дійти висновку, що чинне кримінальне законодавство не відповідає наявним соціальним потребам у кримінально-правовій охороні відповідних суспільних відносин. *Національне правове поле не містить правових гарантій, які б відповідали сучасним проявам суспільно небезпечної поведінки у сфері отримання та надання незаконного доступу до інформації*.

Так, за даними європейських правоохоронців, сьогодні є підстави говорити про формування "тіньової цифрової економіки". Предметом незаконної торгівлі у цій сфері є дані про кредитні картки, банківські реквізити, реквізити в електронних платіжних системах, навіть фактичні адреси, телефони, імена та прізвища [207].

Наявність такого "сектору злочинної економіки" з необхідністю породжує "попит" на відповідну інформацію. Тому останнім часом можна зустріти численні повідомлення про незаконне заволодіння різноманітними персональними даними. Наприклад, у грудні 2010 року повідомлялося про те, що зловмисники отримали доступ до однієї з клієнтських баз даних мережі ресторанів швидкого харчування McDonald's. Зловмисники одержати контактну інформацію про клієнтів, передану для участі в промо-акціях. І хоча номерів кредитних карт і карт соціального страхування в базі не було, до злочинців потрапили адреси електронної пошти, дати народження, контактна інформація відвідувачів та інші "загальні дані" [369]*. Спеціалізовані білоруські видання повідомляли про затримання одного з молодих мешканців м. Гомеля, який за допомогою спеціальної програми, установленої на домашньому комп'ютері, отримував особисту інформацію абонентів одного із серверів (логіни, паролі та MAC-адреси) та передавав її третій особі [374]. Повідомлялося про затримання ФСБ Росії трьох молодих людей, які впродовж 6 місяців здійснили несанкціонований доступ до кількох тисяч європейських та американських комп'ютерів.

* Тут і далі наводитимуться посилання на публіцистичні джерела. Означена обставина потребує розв'язання питання про допустимість використання подібної інформації в науковому дослідженні. Безсумнівно, відомості, отримані з ненаукових джерел, не можуть бути включені як аргументи в науковий дискурс. Водночас вельми доречним видається використання такої інформації як фактичних або гіпотетичних прикладів можливих випадків, що потребують правової оцінки. У такий спосіб, як видається, забезпечується додаткова верифікація отриманих висновків. Оскільки публіцистична інформація в цьому дослідженні використовується саме для цього, відповідні джерела слід уважати допустимими.

Співробітники ФСБ з'ясували, що зловмисники "заражали" комп'ютери спеціальним шкідливим програмним забезпеченням, яке відкривало їм вільний доступ до будь-якої інформації на жорсткому диску [304].

Одним із "перспективних" середовищ для отримання персональних даних є соціальні мережі. Це пояснюється великою аудиторією даних інтернет-ресурсів. Як правило, у соціальних мережах зловмисників цікавлять персональні дані, що являють собою реквізити акаунтів (облікових записів) користувачів (логіни та паролі). Так, у вересні 2010 року повідомлялося про надзвичайну подію в мережі мікро-блогів Twitter. Використовуючи раніше невідому помилку в програмному забезпеченні сервісу та спеціалізований комп'ютерний вірус, зловмисники отримали дані акаунтів близько півмільйона користувачів [373]. У січні 2011 року Федеральний суд США оштрафував Філіпа Порембські на 360,5 млн. доларів за розсилання комерційних повідомлень у соціальній мережі. Порембські був визнаний винним у незаконному отриманні реквізитів як мінімум 116 тисяч користувачів Facebook та розсиланні спам-повідомлень від їх імені. Усього було відправлено більше 7,2 млн. рекламних повідомлень. Деякі з них було створено для залучення користувачів на підроблені, так звані фішингові сайти з метою подальшого заволодіння персональними даними. До наслідків діяльності обвинуваченого також віднесено блокування акаунтів користувачів [326].

Подібні посягання неодноразово фіксувалися і в Україні. Так, у березні 2011 року повідомлялося про затримання співкобітниками СБУ України 19-річного хакера, який незаконно заволодів конфіденційною інформацією більш ніж 190 тисяч користувачів одного з популярних одеських веб-форумів. Було встановлено, що зловмисник використовував спеціалізоване програмне забезпечення, а отриману інформацію збирався реалізувати з метою отримання прибутку. Слідчими СБУ в Одеській області було порушено кримінальну справу за ознаками складу злочину, передбаченого ч. 1 ст. 361 КК [45].

Вельми оригінальний спосіб незаконного отримання персональних даних був нещодавно використаний у м. Києві. В одному з торговельних центрів установили пристрій, що ззовні нагадував звичайний банкомат. Ті, хто намагався отримати через нього гроші, після введення PIN-коду одержували інформацію про те, що сервіс не працює. Водночас код та інші конфіденційні ідентифікаційні відомості, зчитані апаратом з картки, надсилалися зловмисникам за допомогою GSM-модему. Таким чином, зловмисники без особливих зусиль діставали повний доступ до рахунків жертв і знімали гроші. Клієнти розуміли, що відбувалося, лише після того, як перевіряли залишок на рахунку вже в справжньому банкоматі [114].

Те, що використання інформаційних технологій для отримання різноманітних даних з обмеженим доступом отримало характер досить поширеної суспільно небезпечної поведінки, підтверджується й тенденціями розвитку шкідливого програмного забезпечення. За повідомленнями компаній, які займаються розробленням антивірусних програмних засобів, останнім часом регулярно з'являються нові типи шкідливих програм, націлені на отримання закритих даних. Так, лише в листопаді 2010 року до вірусної бази Dr.Web було додано декілька модифікацій Trojan.PWS.Ibank.213. Ця програма крім основної функції, а саме накопичення та передачі персональних даних користувача, дозволяє відключати компоненти захисного програмного забезпечення та системний механізм створення точок відновлення. Щоб зібрати інформацію, необхідну для доступу до акаунтів систем дистанційного банківського обслуговування, програма перехоплює деякі системні функції, зберігає інформацію, яку користувач вводить з клавіатури [206].

Отримані в такий спосіб персональні дані, як правило, використовуються в подальшому для незаконного заволодіння майном, здійснення протизаконних спамерських розсилань від чужого імені тощо. Наприклад, восени 2010 року прокуратура США і ФБР оголосили про розкриття мережі, учасники якої викрали з американських банків понад 3 мільйони доларів. Слідчі повідомляли, що злочинці (один із яких громадянин

Росії) діяли за нескладною схемою. За допомогою електронної пошти вони розсилали жертвам повідомлення з вірусом Zeus Trojan. При відкритті прикріпленого файлу програма отримувала дані доступу до банківських рахунків і PIN-кодів пластикових карт жертв та в прихованому режимі направляла їх обвинуваченим. Потім гроші переказувалися на спеціально відкриті шахраями рахунки в інших банках [46]. Із розкриттям подібного злочину та використанням цього шкідливого програмного засобу пов'язана й широковідома спільна спеціальна операція СБУ та правоохоронців США, Великобританії та Нідерландів. Після її завершення (листопад 2010 року) ЗМІ повідомляли про затримання п'ятьох українців, які брали активну участь у конвертації грошей, одержаних злочинним шляхом, у готівкову форму [206].

У Калінінграді було засуджено групу хакерів за звинуваченням у незаконному заволодінні близько двох мільйонів рублів з трьох банків, розташованих у Ростові-на-Дону, Махачкалі та Єкатеринбурзі. У цьому випадку знову ж таки використовувалася троянська програма, яка дозволяла отримувати відомості, необхідні для авторизації й подальшого здійснення трансакцій у комп'ютерних мережах банків від імені їх клієнтів [115].

Повідомлялося також про те, що в Заєльцовському районному суді м. Новосибірська слухалася справа за обвинуваченням громадян РФ у вчиненні незаконного заволодіння чужим майном у великих розмірах. Злочин було вчинено за таких обставин. Діючи у складі міжнародної групи хакерів, підсудні на початку листопада 2008 року разом з не встановленими слідством особами отримали доступ до електронних ресурсів платіжної системи RBS WorldPay (процесинговий підрозділ Royal Bank of Scotland). Хакери скопіювали інформацію про рахунки клієнтів, включаючи PIN-коди. При цьому вони збільшили баланси і ліміт зняття з кожної картки грошових коштів. Потім з використанням отриманих відомостей виготовили банківські картки. За версією звинувачення, 7 і 8 листопада 2008 року через банкомати Іспанії, Японії, Китаю, Туреччини, Великобри-

танії, США, Голландії, Нової Зеландії, Філіппін, України і Росії (у Санкт-Петербурзі, Кемерові, Красноярську й Ачинську) зловмисники заволоділи близько 10 мільйонами доларів [61].

Разом із тим, використання незаконно отриманої інформації з обмеженим доступом не обмежується її подальшим застосуванням суб'єктом незаконного доступу для незаконного заволодіння майном. Вельми поширеними є й інші способи. Ідеться про формування й становлення певного сегменту тіньової економіки – ринку незаконно отриманої інформації з обмеженим доступом. Так, за даними моніторингу чатів і форумів, який проводився компанією Symantec у 2008 році, в Інтернеті нараховувалося близько 70 тисяч активних користувачів, які пропонували придбати чужу банківську інформацію, відомості про кредитні картки та облікові записи електронної пошти. Обсяг чорного ринку даних про банківські рахунки та кредитні картки може складати понад 184 мільйони фунтів. При цьому відзначається зростання організованості учасників ринку, включення до процесу злочинних співтовариств [390].

У 2011 році відомий розробник антивірусного програного забезпечення PandaLabs оприлюднив результати спеціального моніторингу Інтернету. Фахівці виявили велику мережу, що складається з форумів і більше ніж 50 інтернет-магазинів та в межах якої здійснюється продаж реквізитів викрадених банківських карток разом з іншими видами подібних інформаційних продуктів. Цей ринок дуже швидко зростає, і зловмисники викрадають все більше особистої інформації для отримання в подальшому прибутку. Показовим є той факт, що на цьому ринку вже сформувалася певна система чинників, які впливають на ціну відповідної інформації. Так, ціна інформації про банківську картку (від 10$ до 1500$) залежить від можливості доступу до перевірки рахунку, наявності та кількості грошей на ньому, наявності фактів перерахування коштів із цього рахунку для оплати покупок в інтернет-магазинах через платіжні системи, наприклад PayPal, тощо. Достатньо тривожним сигналом є і встановлені спеціалістами PandaLabs ознаки конкурентної боротьби в досліджуваній сфері. Так, пропонуються

знижки "оптовим" покупцям, пробний період користування певною інформацією або сервісом, гарантії повернення коштів або обміну послуги. Усе це свідчить про масштабність і потужність такого негативного явища, як "чорний" ринок інформації з обмеженим доступом [201].

На сьогодні повідомляється щодо наявності в продажу таких інформаційних ресурсів про громадян України та країн ближнього зарубіжжя, як: бази даних володарів приватних автомашин із зазначенням адреси проживання та контактних телефонів; реєстри юридичних осіб; зведені відомості про платників податків із зазначенням адрес і задекларованих доходів; бази даних абонентів телефонного зв'язку, у тому числі операторів мобільного телефонного зв'язку; відомості стосовно зовнішньоекономічних операцій тощо [56]. Існує можливість придбання баз даних Пенсійного фонду із зазначенням усіх місць роботи та відповідного рівня офіційної заробітної плати конкретних осіб, а також спеціалізованих інформаційних ресурсів МВС, у яких систематизовано відомості про надзвичайні події на певній території, дані паспортних столів, персональні дані осіб, які перебувають під наглядом, тощо [83].

Російські аналітичні видання відзначали також розгалуженість суб'єктів ринку незаконного доступу до інформації. Так, "виробниками" виступають особи, які безпосередньо отримують доступ до захищених баз даних та створюють їх копії. Як зауважують фахівці, найчастіше незаконні копії баз даних створюються особами, котрі мають до них правомірний доступ. Достатньо велику групу суб'єктів досліджуваного ринку складають "посередники", до яких відносять як осіб, що скуповують бази даних для їх подальшого перепродажу, так і так званих "інформаційників", або "чорних аналітиків". Останні скуповують максимально можливі обсяги інформації, постійно займаються її актуалізацією (оновленням) та пропонують інформаційні послуги зацікавленим особам. Нарешті, "споживачі", залежно від суми, яка витрачається, представлені двома категоріями: 1) особи, які придбавають відносно дешеві бази даних у дрібних посередників (дрібні підприємці, приватні

охоронні підприємства, що не мають надійних джерел інформації, тощо); 2) замовники "інформаційників". Останню категорію утворюють, як правило, бізнесмени. Отримана інформація дозоляє їм мінімізувати ризики й отримати перевагу під час перемовин. Разом із цим, дійсні мотиви отримання інформації не цікавлять осіб, які займаються такою неофіційною аналітичною роботою. Тому фахівці не виключають, що замовники можуть використовувати отриману інформацію із протиправною метою. Наприклад, особи, котрі займаються вимаганням, у відповідь на запевнення бізнесмена, що він працює тільки на податки, можуть продемонструвати йому документи, у яких зазначено його нерухомість, кількість автомобілів і куди він востаннє виїжджав відпочивати. У свою чергу, особи, які займаються угонами коштовних транспортних засобів, частіше за все на етапі готування злочину перевіряють їх за базами даних автомобільної інспекції [356].

Таким чином, формування потужних інформаційних ресурсів як реакція на ускладнення суспільних відносин, безсумнівно, має позитивне значення, дозволяє інтенсифікувати діяльність людини, підвищити її ефективність. Разом із тим, наявність можливостей отримання інформації з обмеженим доступом незаконним шляхом, а також постійний попит на це з боку певних соціальних груп спричинили появу та поширення незаконної діяльності у сфері отримання й надання доступу до інформації. Фактичні дані свідчать про кількісне зростання суб'єктів такої діяльності та якісні зміни показників їх організованості. Тому обґрунтованим видається висновок про те, що оцінка чинної системи кримінально-правових засобів забезпечення обмеженого доступу до інформації повинна даватися з позицій її здатності бути нормативною базою для мінімізації розвитку негативних суспільних тенденцій, пов'язаних із формуванням відповідного сектору тіньової економіки. Інакше кажучи, необхідним є аналіз того, наскільки наявні в КК норми відповідають соціальним потребам у кримінально-правовому захисті суспільних відносин, зумовленим тендерціями зростання ринку незаконно отриманої інформації.

Отже, протидія діяльності "виробників" на цьому ринку, тобто осіб, які отримують незаконний доступ до інформації з обмеженим доступом, у цілому на достатньому рівні забезпечена відповідними кримінально-правовими засобами. Хоча останні й не позбавлені певних недоліків.

Головний з них пов'язаний з тим, що отримання персональних даних чи відомостей, що становлять комерційну або банківську таємницю, можливе не тільки шляхом незаконних операцій з комп'ютерною технікою. У попередній главі ми доводили недоцільність асоціації відповідальності за витік інформації тільки з формою представлення даних. Разом із тим, відповідно до чинного законодавства, якщо персональні дані збираються особою у спосіб, який не передбачає застосування комп'ютерної техніки, відповідальність настає за ст. 182. При цьому найбільш суворим покаранням за злочин, передбачений ст. 182 (індекс КЗОСН) є три роки обмеження волі, тоді як ч. 1 ст. 361 (індекс КЗОСН) передбачає покарання до трьох років позбавлення волі. У свою чергу, як зазначалося раніше, незаконне збирання відомостей, що становлять комерційну таємницю, є кримінально караним тільки за умови настання шкоди (ст. 231), тоді як збирання таких відомостей без настання шкоди, але з використанням комп'ютерної техніки (ч. 1 ст. 361) є злочином середньої тяжкості. Вельми цікавим тут буде зарубіжний досвід. У США злочини, пов'язані з незаконним збиранням персональних даних для подальшого отримання матеріальної вигоди, отримали назву "крадіжка особистості". За даними агенції Javelin Strategy & Research, у 2009 році жертвами подібних злочинів стали 11,1 мільйона американців, причому загальний збиток склав близько 54 мільярдів доларів. За висновками Федеральної комісії з торгівлі США, основний збиток від "крадіжки особистості" спричинений витоком даних кредитних карт і номерів соціального страхування. При цьому американські дослідники не обмежують подібні випадки тільки використанням інформаційних технологій. До них відносять і так званий притекстинг (від англ. pretext – не реальна причина, а привід), коли зловмисники (зазвичай по телефону),

використовуючи хибні приводи та видаючи себе за працівників фінансових установ чи операторів зв'язку, отримують особисту інформацію, а також звичайні крадіжки документів. Крім цього у відповідній правовій площині розглядаються крадіжки гаманців, особистих і фінансових документів, навіть перевірка контейнерів для сміття у фінансових установах. Останній спосіб навіть одержав спеціальну назву – Dumpster Diving [29]. Отже, очевидно, що незаконне отримання доступу до інформації шляхом використання комп'ютерної техніки само по собі не може свідчити про суспільну небезпечність посягання. Об'єктивними її чинниками є зміст, мета подальшого використання, заподіяна шкода тощо. Тому *властиве національному законодавству конструювання кримінально-правових заборон незаконного доступу на основі ознак форми їх представлення* слід визнати таким, що *не відображає фактичної суспільної небезпечності цих* посягань.

Також зазначимо, що випадки незаконного отримання доступу до комп'ютерної інформації з обмеженим доступом відповідно до національного законодавства слід розглядати як несанкціоноване втручання в роботу комп'ютерної техніки, що призвело до витоку інформації (ст. 361). Однак ця кримінально-правова заборона сформульована досить широко, унаслідок чого *неможливо врахувати об'єктивні чинники суспільної небезпечност*і. Наприклад, за ч. 1 ст. 361 слід кваліфікувати як діяння особи, що незаконно отримала персональні дані близько 190 тисяч користувачів веб-форуму (див. наведений раніше приклад), так і доступ до облікового запису одного користувача комп'ютерної мережі та отримання особистого пароля доступу до його електронної пошти (Вирок Прилуцького міськрайонного суду Чернігівської області в справі № 1-200/2010 від 29 липня 2010 року [159]).

Що ж стосується діяльності "посередників", тобто осіб, які самостійно не здійснюють незаконного доступу до певних ресурсів, але придбавають інформацію, здобуту незаконним шляхом, з метою подальшого отримання прибутку, то наявні в КК правові засоби протидії їй потребують удосконалення.

Нетиповою, але вельми показовою є ситуація, що склалася з відомим інтернет-ресурсом інформації з обмеженим доступом WikiLeaks. Останній являє собою створений у 2006 році міжнародний соціальний мережевий проект, мета якого полягає в такій публікації документів, що стали доступними внаслідок витоку інформації, яку неможливо відстежити. Найбільш відома публікація сайту – це майже півмільйона таємних файлів Держдепартаменту США, які містили дані про листування американських дипломатів. Цей мережевий ресурс та його засновник, громадянин Австралії Джуліан Ассандж, стали дуже популярними. І вже наприкінці 2010 року відомий The Wall Street Journal повідомляв, що прибуток сайту від пожертвувань склав 1 мільйон євро [310], а його засновник продав авторські права на автобіографічне видання за 1,5 мільйона доларів [107]. Усе вищезазначене, як видається, дає підстави розглядати діяльність засновника WikiLeaks як певний прояв незаконного ринку інформації. На окрему увагу заслуговує юридична оцінка його дій. Повідомлялося, що американські слідчі не змогли знайти переконливих доказів, аби притягнути Джуліана Ассанджа до суду за публікацію конфіденційних документів Держдепартаменту США. Американське слідство мало намір звинуватити Ассанджа в злочинній змові, а саме в підбурюванні до крадіжки федеральної власності, якою є документи держдепу. Слідчі намагалися довести, що Бредлі Меннінг, який передав WikiLeaks урядові документи, і Джуліан Ассандж були в злочинній змові. Проте довести, що Ассандж підбурював Меннінга передати йому секретні матеріали, так і не вдалося [9]. Якщо подібні дії було б вчинено стосовно України та відомостей, які відповідно до національного законодавства становлять державну таємницю, то наданню вільного доступу до них через інтернет-сайт так само важко було б дати кримінально-правову оцінку. До кримінальної відповідальності за розголошення таких відомостей можна притягнути тільки ту особу, якій вони були довірені або стали відомі у зв'язку з виконанням службових обов'язків (ст. 328). Ознаки складу шпигунства

(ст. 114) також відсутні, оскільки його суб'єктивна сторона передбачає *прямий* умисел та специфічну мету. Особа усвідомлює, що відомості збираються або передаються *конкретній* іноземній державі, організації або їх представникам. У досліджуваній ситуації збирання інформації та подальше її оприлюднення не характеризуються відповідними метою та адресатом передачі.

Розглянемо більш типову ситуацію. Наприклад, А. придбав бази даних податкової адміністрації, що містять відомості реєстру юридичних осіб, зареєстрованих на певній території, та відповідно до чинного законодавства віднесені до конфіденційної інформації, яка є власністю держави. Ці бази він придбав у особи, яка заволоділа ними злочинним шляхом. За оплату він надавав особам, котрі зверталися до нього, інформацію про юридичну адресу, контактні дані керівників, інші відомості реєстру. Яку кримінально-правову оцінку діям цієї особи можна дати? Під ознаки складу злочину, передбаченого ст. 361-2, ці дії не підпадають. Раніше ми зазначали, що ознаки предмета, які містяться в диспозиції розгляданої статті, значно ускладнюють її використання. Частина перша ст. 330 також не може бути застосована, оскільки передбачає відповідальність за передачу або збирання з метою передачі відомостей, що становлять конфіденційну інформацію, яка є власністю держави, *іноземним підприємствам, установам, організаціям або їх представникам*. При цьому вплив кримінальної юстиції в таких випадках є необхідним, тому що подібна діяльність формує "попит" на бази даних, отримані злочинним шляхом, та, відповідно, стимулює зростання злочинних проявів у сфері незаконного отримання доступу до інформації.

Таку саму ситуацію матимемо і при спробі дати кримінально-правову оцінку подібних дій стосовно інших видів інформації з обмеженим доступом. Так, за певні види надання незаконного доступу передбачено відповідальність тільки спеціальних суб'єктів (ст.ст. 132, 145, 209-1, 381, 387), а отже, "посе-

редник" не може бути притягнутий до кримінальної відповідальності за ознаками складів цих злочинів. Хоча достатньо очевидною є суспільна небезпечність незаконного надання доступу до відомостей щодо проведення медичного огляду (ст. 132), відомостей, що становлять лікарську таємницю (ст. 145); інформації спеціального органу виконавчої влади з питань фінансового моніторингу (ст. 209-1); відомостей про заходи безпеки (ст. 381); даних досудового слідства (ст. 387). Зазначимо, що надання незаконного доступу до такої інформації загальним суб'єктом може розглядатися в контексті кримінально-правової заборони розголошення даних про особу без її згоди (ч. 1 ст. 182). Однак навряд чи можна погодитися з тим, що інтенсивність санкції цієї норми ($I_{кзосн}$ = 23,69) відповідає суспільній небезпечності посягання. Такий самий недолік властивий і правовим ґарантіям обмеження доступу до відомостей, що становлять таємницю голосування (ч. 1 ст. 159, $I_{кзосн}$ = 20,05), а також таємницю всиновлення (ч. 1 ст. 168, $I_{кзосн}$ = 6,15). Очевидно, що названі правові засоби орієнтовані на випадки разового порушення відповідної таємниці та не можуть розглядатися як відповідна правова оцінка діяльності щодо надання незаконних інформаційних послуг.

Можливості притягнення особи, яка в означений спосіб надавала доступ до відомостей, що становлять комерційну або банківську таємницю (ст. 231), значно ускладнені через наявність такої обов'язкової ознаки цього складу злочину, як наслідки – заподіяння істотної шкоди господарюючому суб'єктові. Зрозуміло, що в умовах, коли особа не обізнана щодо подальшого використання відомостей, які вона надає, притягти її до відповідальності за шкоду, яка буде заподіяна внаслідок використання цих відомостей, дуже проблематично. Таке саме зауваження можна зробити і щодо можливостей використання ч. 2 ст. 182 КК.

Здійснений аналіз дозволяє дійти таких висновків. Передбачена чинним КК система кримінально-правових засобів забезпечення обмеженого доступу до інформації характеризу-

ється: 1) непослідовністю впливу фактичних чинників суспільної небезпечності на інтенсивність санкцій за окремі види незаконного надання та отримання доступу до інформації; 2) невідповідністю соціальним потребам кримінально-правової протидії, пов'язаним з формуванням тіньового ринку інформації, здобутої злочинним шляхом. Так, дослідження, проведене з використанням методу контекстної законодавчої оцінки суспільної небезпечності, дозволило встановити: 1) непоодинокі випадки очевидної невідповідності суспільної небезпечності діяння, передбаченого КК, інтенсивності санкції відповідної норми (наприклад, ч. 2 ст. 163, ч. 3 ст. 422, ч. 2 ст. 381, ст. 145 тощо); 2) непослідовність законодавчих рішень у питанні встановлення кримінальної відповідальності за спеціальні види незаконного отримання або надання доступу до інформації, при цьому особливо слід відзначити необґрунтоване підвищення санкцій за несанкціонований доступ у разі його вчинення з використанням інформаційних технологій (чч. 11, 12 ст. 158, ст.ст. 361, 362, 376-1); 3) недоліки законодавчої оцінки подібних за змістом ознак, що характеризують суб'єкт посягання; 4) спірні законодавчі рішення в питанні формулювання ознак кваліфікованих посягань на відносини щодо забезпечення обмеженого доступу до інформації; 5) неузгодженість використовуваної термінології.

У свою чергу, дослідження кримінально-правових засобів забезпечення обмеженого доступу до інформації на предмет їх відповідності сучасним проявам суспільно небезпечної поведінки у сфері отримання та надання незаконного доступу до інформації дозволяє стверджувати щодо фрагментарності та несистемності законодавства в цій сфері. Наявні в КК норми не можуть розглядатися як нормативна база ефективної протидії зростанню тіньової цифрової економіки.

Аналіз контекстних законодавчих оцінок суспільної небезпечності посягань у сфері забезпечення обмеженого доступу до інформації, а також трансформаційних тенденцій суспільно небезпечної поведінки в цій сфері дає змогу сформулювати пріоритетні завдання вдосконалення системи кримінально-

правових засобів забезпечення обмеженого доступу до інформації, а саме:

- подолання фрагментарності кримінально-правової охорони;

- пошук загальних підходів до законодавчої оцінки суспільної небезпечності окремих видів незаконного отримання або надання доступу;

- розвиток системи як засобу протидії формуванню ринку незаконних інформаційних послуг.

Отже, необхідність удосконалення системи кримінально-правових засобів охорони обмеженого доступу до інформації є очевидною. Сформулюємо можливі шляхи виконання вищезазначених завдань. Подолання фрагментарності кримінально-правової охорони та забезпечення об'єктивної законодавчої оцінки суспільної небезпечності досліджуваних посягань можна забезпечити відмовою від надмірної деталізації кримінально караних видів порушень обмеженого доступу до інформації. Б.Г. Розовський чітко зафіксував одну з основних закономірностей розвитку кримінального законодавства: від первинного поняття злочину, яке за змістом було примітивно простим та передбачало оцінку небезпеки посягання на конкретний матеріалізований предмет – крадіжка коня, крадіжка зброї, позбавлення ока тощо, до узагальнень (наприклад, крадіжка не коня, а крадіжка худоби), відмови від предметної індивідуалізації, появи видових узагальнень (крадіжка, шахрайство). Такий підхід дозволяє авторові критично оцінити сучасні законотворчі процеси в кримінальному праві. Б.Г. Розовський обґрунтовано доводить, що останнім часом відбувається зворотний процес – декристалізація, повернення у варварство: однотипні за своєю суттю злочини все частіше диференціюються. Слід погодитися і з М.Й. Коржанським, який зазначав, що "законодавець у галузі кримінального законодавства постійно дублює законодавчі акти… Внаслідок такої законодавчої практики закон, по-перше, перевантажується нормами про позбавлення волі, відповідальність за діяння, які за своєю сутністю не досягають ступеня суспільної небезпечності злочину, а по-дру-

ге, наповнюється нормами, що повторюють одна одну" [140, с. 3 – 4]. Подібна ситуація склалася і з кримінально-правовою охороною обмеженого доступу до інформації. Як видається, велика кількість спеціальних заборон у цій сфері є об'єктивною передумовою якісного оновлення відповідної системи кримінально-правових засобів. Доцільною видається відмова від розгалуженої системи норм, які передбачають відповідальність за фактично однакові діяння, але відносно інформації з обмеженим доступом різних видів. При цьому є сенс у збереженні низки спеціальних заборон, але тільки тих, які характеризуються істотно більшою суспільною небезпечністю.

На користь наведеної пропозиції свідчить і специфіка сучасних процесів у сфері інформатизації. Подальший розвиток полягатиме в об'єднанні розрізнених джерел і ресурсів інформації, тих які використовуються в різноманітних сферах людської діяльності (освіта, охорона здоров'я, продаж товарів, пропонування послуг тощо), в одному інформаційному полі. Інтеґрація інформаційних ресурсів забезпечує істотне підвищення ефективності їх використання, саме тому вона і є основним напрямом процесів інформатизації суспільства. Найбільш яскраво цей процес може бути продемонстровано на прикладі розвитку системи інформаційного забезпечення правоохоронної діяльності. Так, під час виконання завдань щодо виявлення та розкриття злочинів, розшуку осіб, які їх вчинили, працівники ОВС мають потребу в інформації щодо стану здоров'я окремих осіб, їх освіти тощо. Що відбувалося раніше? Надсилалися письмові запити до наркологічного та психоневрологічного диспансерів, дитячих лікувальних закладів, закладів освіти, військкоматів тощо, там потрібну картку шукали в архіві, після цього поштою надсилали відповідь. Якою була ефективність цього процесу в контексті протидії злочинності, легко можна уявити. Нині ця інформація формується в єдиний банк даних.

Зрозуміло, що в масштабі держави для прийняття відповідних управлінських рішень, розроблення програм і перспективних планів розвитку, формування законотворчої політики

централізація всієї інформації щодо процесів, які відбуваються в суспільстві, вкрай важлива та необхідна. Інтеґрація інформаційних ресурсів відбувається й у сфері господарювання. Наприклад, торговельні мережі, використовуючи різноманітні засоби, здійснюють накопичення й аналіз великих обсягів інформації для забезпечення більш ефективних продажів і реклами.

У процесі створення таких систем неминуче виникне потреба в чіткій реґламентації порядку їх функціонування, а також наданні єдності системі відповідальності за порушення встановлених приписів. Тобто необхідність інтеґрації інформаційних ресурсів неодмінно приведе до уніфікації правового реґулювання й охорони відповідних суспільних відносин. Отже, наведена раніше пропозиція щодо відмови від розгалуженої системи спеціальних норм та їх заміни загальними цілком відповідає тенденції процесів інформатизації суспільства.

Окремо зауважимо, що відповідальність за незаконне надання доступу та незаконне отримання доступу доцільно передбачати в різних нормах. Це пояснюється як принциповою різницею чинників суспільної небезпечності таких посягань, так і вимогою чіткості та визначеності закону про кримінальну відповідальність. Наприклад, у диспозиціях ч. 1 ст. 361 та ч. 2 ст. 362 використовується термін "витік інформації". Системне тлумачення цих норм та аналіз ознак суб'єктів посягань дозволяє встановити, що під витоком у ст. 361 розуміється як отримання незаконного доступу до інформації, так і його надання. У свою чергу, у ч. 2 ст. 362 під витоком розуміється тільки надання незаконного доступу. Зрозуміло, що наявність одного терміна з різним змістом у диспозиціях статей Особливої частини КК є неприпустимою. Пригадаємо і ситуацію, що склалася з кримінально-правовими ґарантіями обмеження доступу до відомостей, що становлять комерційну таємницю (ст.ст. 231, 232). Об'єднання в одній нормі (ст. 231) заборони надання та отримання доступу до інформації призвело до очевидної невідповідності контекстної законодавчої оцінки суспільної небезпечності передбаченого нею посягання його об'єктивній су-

спільній небезпечності: розголошення відомостей загальним суб'єктом (ст. 231, $I_{кзосн}$ = 50,77) визнано законодавцем більш небезпечним, ніж аналогічні дії особи, яка зобов'язувалася зберігати відповідну таємницю (ст. 232, $I_{кзосн}$ = 35,54).

Про необхідність окремих законодавчих формулювань злочинних видів отримання незаконного доступу до інформації та його надання свідчить і різниця чинників суспільної небезпечності таких посягань. Так, очевидно, що для інтенсивності кримінальної відповідальності за незаконне надання доступу до інформації матиме значення наявність у суб'єкта посягання певних прав щодо доступу до інформації та обов'язків щодо його обмеження. Однак для законодавчого формулювання незаконних видів отримання доступу до інформації така ознака не може використовуватися, оскільки незаконне отримання доступу передбачає відсутність у суб'єкта будь-яких повноважень щодо ознайомлення з інформацією, яка становить предмет посягання. Водночас чинником суспільної небезпечності незаконного отримання доступу до інформації слід уважати його вчинення з використанням шкідливих програмних засобів або шляхом подолання спеціалізованих технічних засобів захисту. Використання таких ознак для законодавчого визначення незаконного надання доступу не має сенсу.

Таким чином, з метою вдосконалення дослідженої системи кримінально-правових засобів забезпечення обмеженого доступу до інформації пропонується: 1) доповнити Кримінальний кодекс загальними нормами про відповідальність за незаконне надання доступу до інформації та незаконне отримання доступу до інформації; 2) виключити з кодексу спеціальні норми, у яких передбачено відповідальність за окремі види таких діянь.

Для криміналізації *незаконного надання доступу* до інформації пропонується доповнити КК статтями такого змісту:

"Стаття 361-2. Незаконне надання доступу до інформації

1. Незаконне надання доступу до таємної, службової або конфіденційної інформації, якщо воно заподіяло умисне істотне порушення реалізації прав, свобод або законних інте-

ресів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, –

карається штрафом до однієї тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі до п'яти років, або позбавленням волі до трьох років.

2. Те саме діяння, вчинене з корисливою метою або повторно, або групою осіб за попередньою змовою, або особою, яка має правомірний доступ до інформації у зв'язку з займаною посадою чи спеціальними повноваженнями, або вчинене з використанням засобів масової інформації чи інших інформаційних технологій, що забезпечують доступ до інформації значної кількості осіб, або якщо воно заподіяло значну шкоду, –

карається позбавленням волі від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією майна або без такої.

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони заподіяли тяжкі наслідки, –

караються позбавленням волі від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією майна або без такої.

Примітка: Надання доступу до таємної, службової або конфіденційної інформації не може бути визнано незаконним, якщо суд установить, що ця інформація, на час надання доступу до неї, була суспільно необхідною.

Стаття 362-2. Заподіяння необережної шкоди через незаконне надання доступу до інформації

1. Незаконне надання доступу до таємної, службової або конфіденційної інформації, вчинене особою, яка має правомірний доступ до інформації у зв'язку з займаною посадою або спеціальними повноваженнями, якщо воно з необережності заподіяло значну шкоду, –

карається штрафом до п'ятисот неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до

ста двадцяти годин або виправними роботами на строк до одного року.

2. Те саме діяння, якщо воно з необережності заподіяло тяжкі наслідки, –

карається штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до двохсот сорока годин, виправними роботами на строк до двох років або обмеженням волі до трьох років".

Для криміналізації *незаконного отримання доступу* до інформації пропонується доповнити КК статтею такого змісту:

"Стаття 363-1. Незаконне отримання доступу до інформації

1. Незаконне отримання доступу до таємної, службової або конфіденційної інформації, вчинене шляхом подолання технічних, програмних або організаційних засобів захисту інформації, –

карається штрафом до ста неоподатковуваних мінімумів доходів громадян, або громадськими роботами до ста вісімдесяти годин, або арештом до трьох місяців.

2. Ті самі дії, вчинені шляхом використання технічних або програмних засобів, призначених для незаконного отримання доступу до інформації, з метою надання незаконного доступу до інформації, повторно, групою осіб за попередньою змовою, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на строк до трьох років з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи".

З виключно наукової точки зору, керуючись намаганням побудувати чітку юридичну конструкцію, яка б повною мірою враховувала всі наведені раніше аргументи, можна було б запропонувати збереження спеціальних норм про відповідальність тільки за такі найбільш небезпечні види незаконного отримання та надання доступу, як державна зрада (ст. 111) та шпигунство (ст. 114). Що стосується решти норм про відповідальність за незаконне надання доступу до інформації (ст.ст. 132,

145, чч. 11, 12 ст. 158, ст.ст. 159, 168, 182, 209-1 ч. 2, 231, 232, 328, 330, 361, 362, 376-1, 381, 387, 422) та незаконне отримання доступу (чч. 11, 12 ст. 158, ст.ст. 163, 182, 231, 361, 376-1), то прийняття запропонованих новел дозволило б їх скасувати повністю або в частині заборони певних видів надання чи отримання незаконного доступу до інформації. Певні зміни мали б бути внесені й до диспозиції ч. 1 ст. 232-1 КК. З метою уникнення зайвого "дублювання" кримінально-правових заборон доцільно було б виключити з диспозиції вказівку на такі форми передбаченого цією нормою злочину, як умисне незаконне розголошення, передача або надання доступу до інсайдерської інформації. Таке рішення дозволило б подолати фрагментарність кримінально-правової охорони обмеженого доступу до інформації, гіпотетично забезпечило б обґрунтований підхід до законодавчої оцінки суспільної небезпечності відповідних посягань, прозору диференціацію кримінальної відповідальності. Крім того, скасування названих норм і прийняття запропонованих дозволило б декриміналізувати ті види незаконного надання доступу, які не завжди можна відносити до суспільно небезпечних. Ідеться про такі кримінально карані види незаконного надання доступу до інформації, які не характеризуються заподіянням істотної шкоди тим суспільним відносинам, реалізація яких вимагає обмеження доступу до певної інформації. Дійсно, доволі спірною, за буквального тлумачення закону про кримінальну відповідальність, може видаватися доцільність використання кримінальної юстиції в тих випадках, коли шкода, заподіяна посяганням, обмежується виключно створенням можливості ознайомлення третіх осіб з певною інформацією з обмеженим доступом. Такі випадки передбачено чинним кримінальним законодавством: ч. 1 ст. 328, ч. 1 ст. 330, ч. 1 ст. 422, ч. 2 ст. 362, ч. 11 ст. 158, ч. 1 ст. 376-1, ч. 1 ст. 361, ст. 132, ч. 1 ст. 182, ч. 1 ст. 159, ч. 1 ст. 168, ч. 1 ст. 387. У свою чергу, реалізація наведених законодавчих пропозицій дозволила б їх декриміналізувати та, ще раз зазначимо, *гіпотетично* забезпечила б більш раціональне використання засобів кримінальної юстиції.

Проте подібне законодавче рішення мало б низку суттєвих недоліків. Головним чином вони зумовлювалися б тим, що фактичні суспільні відносини є настільки строкатими, а можливі суспільно небезпечні наслідки незаконного надання або отримання доступу до інформації – настільки різноманітними, що не можуть отримати адекватного відображення в загальних, уніфікованих юридичних конструкціях. Так, посягання, пов'язані з розголошенням державної таємниці або відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави (ст.ст. 328, 330, 422), характеризуються надто складним механізмом заподіяння суспільно небезпечних наслідків. Складність та багатомірність суспільних відносин у сфері державної таємниці часом призводить до того, що встановити суспільно небезпечні наслідки певного розголошення видається можливим тільки через достатньо тривалий проміжок часу. У таких умовах, нормативно передбачена залежність кримінальної відповідальності від настання суспільно небезпечних наслідків зумовила б певне зменшення ефективності правових засобів охорони національної безпеки. Особливості змісту наслідків зумовлюють і доцільність збереження відповідних кримінально-правових ґарантій реалізації виборчого права (чч. 11, 12 ст. 158, ст. 159) та здійснення правосуддя (ст.ст. 381, 387).

Нарешті, заміна загальною спеціальної норми про відповідальність за незаконне розголошення в будь-якому вигляді інформації, яка надається спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу (ч. 2 ст. 209-1), може призвести до певних політичних наслідків. Ураховуючи підвищений інтерес міжнародної спільноти до питання протидії леґалізації доходів, отриманих злочинних шляхом, означене законодавче рішення може створити певну напруженість у відносинах України з відповідними міжнародними організаціями.

Наведені арґументи свідчать про доцільність збереження означених кримінально-правових заборон (чч. 11,12 ст. 158, ст. 159, ч. 2 ст. 209-1, ст.ст. 328, 330, 381, 387, 422 КК). Водночас

доповнення КК запропонованими нормами про відповідальність за незаконне надання доступу до інформації та його незаконне отримання дозволить забезпечити ефективний захист тих суспільних відносин, які на сьогодні є безпосередніми об'єктами злочинів, передбачених статтями 132, 145, 163, 168, 182, 231, 232 КК, а також ст. 232-1 КК у частині захисту від незаконного надання доступу до інсайдерської інформації та ст.ст. 361, 362, 376-1 в частині захисту від витоку комп'ютерної інформації з обмеженим доступом. Тому названі норми, у разі прийняття відповідного законодавчого рішення, можуть бути скасовані.

Отже, останнє рішення є більш виваженим, ніж запропоноване раніше (гіпотетичне). Разом із цим, з огляду на позначену раніше тенденцію інтеґрації інформаційних ресурсів і створювану нею потребу в уніфікації засобів правового реґулювання та охорони відносин у сфері інформатизації варто зазначити, що найбільш імовірним напрямом розвитку системи кримінально-правових засобів забезпечення обмеженого доступу до інформації буде її подальше наближення саме до гіпотетичної моделі. Наприклад, з розвитком суспільних відносин очевидною стала необхідність у відмові від диференціації кримінальної відповідальності за посягання на власність залежно від її форми. Видається, що аналогічний процес буде відбуватись і стосовно посягань у сфері обмеженого доступу до інформації. З часом напрацьована практика та подальший розвиток правового реґулювання, можливо, дозволять сформулювати та забезпечити ефективне використання засобів кримінально-правової охорони єдиних для всіх видів інформації з обмеженим доступом. Урешті-решт уже сьогодні досить складно відповісти на питання: "Що є більш небезпечним – розголошення лікарської таємниці, що спричинило спробу самогубства, чи розголошення комерційної таємниці, яке заподіяло матеріальні збитки?", "Чи можна вважати, що розголошення таємниці усиновлення, яке викликало тривалий розрив родинних стосунків, є менш небезпечним, ніж розголошення державної таємниці без настання очевидних наслідків?" тощо. От-

же, пропонуючи наведені раніше зміни до законодавства про кримінальну відповідальність, маємо зазначити, що вони являють собою спробу поступової уніфікації засобів кримінально-правової обмеженого доступу до інформації, необхідність якої зумовлена природним розвитком суспільних процесів інформатизації.

Розглянемо зміст ознак складів злочинів, передбачених статтями, що пропонуються. Як можна побачити з диспозицій, основним безпосереднім об'єктом пропонується передбачити суспільні відносини у сфері забезпечення обмеженого доступу до інформації. Додатковий обов'язковий безпосередній об'єкт (ст.ст. 361-2, 362-2) складатимуть різноманітні суспільні відносини, у межах яких використовується інформація з обмеженим доступом і яким, у разі незаконного надання доступу до неї, заподіюється шкода.

Предметом злочинів, передбачених запропонованими нормами, є інформація з обмеженим доступом, яка може бути трьох видів: таємною, службовою та конфіденційною. Відповідно до ст. 21 Закону України "Про інформацію" до таємної інформації відноситься така, доступ до якої обмежується законом (державна таємниця, банківська та ін.). Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Нарешті, службовою інформацією є така, доступ до якої в порядку, передбаченому законом, обмежено суб'єктом владних повноважень, тобто органом державної влади, місцевого самоврядування або іншим суб'єктом, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень (ст. 1 названого закону). Як можна побачити, пропонується об'єднати в одній нормі кримінально-правові засоби забезпечення обмеженого доступу до різних видів інформації. Це головним чином зумовлено тим, що суспільна небезпечність посягання на досліджувані відносини залежить насамперед від наслідків незаконного доступу, а не від суб'єкта та правових підстав обмеження доступу. Крім того, використання в тексті

закону про кримінальну відповідальність таких термінів Закону України "Про інформацію", як таємна, службова або конфіденційна інформація, дозволить забезпечити незалежність Кримінального кодексу від постійного оновлення відповідного інформаційного законодавства. Наприклад, останнім часом чималий обсяг законодавчих новел пов'язаний з категорією "персональні дані". Розроблюється та постійно вдосконалюється правова база регулювання суспільних відносин щодо накопичення, збирання, поширення відомостей про людину. Прогнозованою є поява правових норм у сфері забезпечення таємниці інтернет-сесій, даних соціальних мереж, електронної комерції тощо. Без сумніву, означені відносини потребуватимуть кримінально-правового захисту. Однак якщо використовувати законотворчий підхід, властивий чинному КК, кожна зміна в правовому регулюванні інформаційних відносин потребуватиме включення до КК відповідної спеціальної норми, тимчасом як запропонований підхід, через використання для опису предмета термінів, що характеризують загальні види інформації з обмеженим доступом, дозволить поширювати наявні кримінально-правові заходи на нові об'єкти правового регулювання в інформаційній сфері. Певною мірою запропонований підхід підтверджується Рішенням Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України (справа № 1-9/2012) від 20 січня 2012 року [299]. У резолютивній частині суд зазначив: "…інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною". Таким чином, використання в запропонованій нормі терміна "конфі-

денційна інформація" дозволяє охопити кримінально-правовим захистом ті суспільні відносини, які на сьогодні охороняються статтями 132, 145, 163, 168, 182 КК України тощо.

Злочини, передбачені запропонованими нормами про відповідальність *за незаконне надання доступу до інформації*, відносяться до посягань з матеріальним складом. За особливостями конструкції об'єктивної сторони вони являють собою злочини з похідними наслідками. Ознаками їх об'єктивної сторони виступають: *діяння*, яке виражається у вчиненні будь-яких дій, спрямованих на створення можливості ознайомлення з інформацією, що складає предмет посягання, для осіб, які не мають на це права; *основний наслідок* – незаконне надання доступу до інформації – у вигляді можливості ознайомлення з інформацією з обмеженим доступом осіб, які не мають на це права; *похідний наслідок* у вигляді істотного порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, державних чи громадських інтересів, діяльності юридичної особи; *причинний зв'язок* між діянням та основним наслідком, основним і похідним наслідками.

Зауважимо, що діяння в цьому випадку характеризується так званою змішаною протиправністю. Висновок про те, чи було надання доступу незаконним, робиться на підставі аналізу нормативно-правових актів, що встановлюють режим доступу до інформації, яка виступає предметом посягання. При цьому необхідно звернути увагу на положення ч. 3 ст. 30 Закону України "Про інформацію", де зазначається, що суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд установить, що ця інформація є суспільно необхідною. І хоча науковці доволі скептично оцінюють перспективи використання положень цієї статті в умовах відсутності законодавчого визначення поняття "суспільна значущість інформації" [122, с. 110], певні правозастосовчі орієнтири можуть бути отримані з практики Європейського суду з прав людини. Так, у справі Фресо та Руара проти Франції було встановлено таке: два автори в період багатотисячного страйку робітників на підприємствах

фірми "Пежо" з вимогами збільшення зарплати опублікували отриману від своїх джерел конфіденційну інформацію про дані податкових декларацій президента фірми пана Кальве, з яких стало видно, що його зарплата за останні два роки виросла на 50%. Французький суд засудив авторів за розголошування конфіденційної інформації, проте Європейський суд дійшов висновку, що оприлюднена авторами інформація була суспільно значущою і люди мали право під час соціального конфлікту її отримати [266]. Означена особливість надання доступу до інформації потребує, як видається, певної акцентуації в тексті закону про кримінальну відповідальність. Саме тому до наведеної статті пропонується примітка, яка містить конкретизацію ознаки протиправності діяння. Варто зазначити, що питання про визначення надання доступу до інформації як протиправного на сьогодні набуває значення самостійної наукової проблеми, яка розв'язується в межах інформаційного права.

Окремого обґрунтування потребує використання в диспозиціях запропонованих норм звороту "незаконне надання доступу". Як зазначалося раніше, для позначення незаконного надання доступу до інформації КК використовує низку різноманітних термінів: "розголошення відомостей" (ст.ст. 132, 328, 381, 422,), "розголошення інформації" (ч. 2 ст. 209-1), "розголошення даних" (ст. 387), "розголошення таємниці" (ст. 145, 168, 232), "несанкціоновані дії з інформацією" (ч. 11 ст. 158, ст. 376-1), "витік інформації" (ст.ст. 361, 362), "незаконне використання відомостей" (ст. 182, 231), "порушення таємниці" (ст. 159), "поширення інформації" (ст. 182), "передача відомостей" (ст. 114, 330), "несанкціоновані збут або розповсюдження інформації" (ст. 361-2). Проте необхідність використання звороту "незаконне надання доступу" обґрунтовується тим, що жоден із наявних у КК способів опису не відповідає сформульованим раніше потребам у вдосконаленні відповідного законодавства про кримінальну відповідальність. Так, використання терміна "розголошення" необґрунтовано обмежуватиме коло можливих випадків застосування запропонованої норми. Справа в тому, що термін "роз-

голошення" в більшості випадків застосовується для характеристики незаконного надання доступу до інформації, що вчиняється особою, яка має правомірний доступ до предмета посягання у зв'язку з виконуваною роботою або наявними повноваженнями. Водночас запропонована норма передбачає відповідальність загального суб'єкта (обґрунтування наводиться нижче). Отже, використання терміна, який традиційно використовується для позначення дій спеціальних суб'єктів, у нормі, що передбачає відповідальність загального, є недоцільним, оскільки створюватиме зайві ускладнення під час її тлумачення.

Поняття "витік", "незаконне використання" і "порушення таємниці", навпаки, характеризуються надто широким змістом і не забезпечуватимуть чіткого виокремлення з усієї сукупності порушень обмеженого доступу до інформації саме тих, які полягають у незаконному наданні доступу. Так, терміном "витік" може позначатись як незаконне надання, так і незаконне отримання доступу до інформації. "Порушення таємниці" у контексті ст. 163 КК являє собою незаконне отримання певних відомостей або ознайомлення з ними. Одночасно таке саме формулювання в ст. 159 КК використовується вже в іншому значенні – як "розголошення змісту волевиявлення".

Нарешті, використання термінів "поширення", "передача", "збут" і "розповсюдження" є недоцільним, через те що їх змістом не охоплюються певні можливі прояви суспільно небезпечного незаконного надання доступу до інформації. Так, наведені терміни характеризують ті випадки, коли шкода заподіюється через надання певним суб'єктам, які не мають права доступу до інформації, оригіналів носіїв, їх копій або змісту обмеженої інформації в іншій формі. При цьому названі поняття не охоплюють створення можливості для ознайомлення з інформацією з обмеженим доступом іншим шляхом. Наприклад, у світовій практиці непоодинокими є суспільно небезпечні посягання, які полягають у незаконному розміщенні на відкритих інтернет-ресурсах інформації з обмеженим доступом, що належить певним суб'єктам господарювання. Такі дії

заподіюють значну шкоду власникові інформації, як правило, через падіння ділової репутації. У подібних випадках порушення відносин у сфері обмеженого доступу до інформації полягає саме у створенні можливості ознайомлення з нею сторонніх осіб, шкода настає не через те, що хтось ознайомився або отримав певну інформацію, а через те, що було створено можливість такого ознайомлення.

Отже, найбільш обґрунтованим, таким, що відповідає встановленим потребам удосконалення законодавства про кримінальну відповідальність, буде використання звороту "незаконне надання доступу до інформації".

Для визначення похідних наслідків у вигляді істотного порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи пропонується використовувати формулювання, яке наводилися в попередній главі. Що ж до питання особливостей змісту матеріальної шкоди від незаконного надання доступу до інформації, то основні засади його розв'язання достатньо ґрунтовно досліджено в роботах О.Е. Радутного [297], С.О. Харламової [375] та П.С. Берзіна [23]. Так, обґрунтовано, що до суспільно небезпечних наслідків незаконного надання доступу до комерційної або банківської таємниці, які є так званими "комбінованими наслідками", слід відносити: "1) реальну позитивну шкоду – прямі матеріальні збитки, у тому числі витрати на захист своїх прав, перепрофілювання діяльності, упровадження нових технологій, додаткові заходи охорони, повідомлення додаткової інформації споживачам, закупівлю нового обладнання тощо; 2) упущену вигоду – неотримання тих майнових вигод, які суб'єкт господарської діяльності повинен був отримати за умови належного користування своїми правами стосовно комерційної таємниці й належного виконання своїх обов'язків іншими суб'єктами суспільних відносин, у тому числі збитки від зниження реалізації продукції, послуг, робіт, спаду виробництва, зменшення клієнтури, зниження цін на товари, роботи й послуги тощо" [296, с. 16]. Наведений підхід, звичайно, з урахуванням специ-

фіки суспільних відносини, які виступають додатковим обов'язковим об'єктом посягання, може бути застосований і при встановленні змісту матеріальної шкоди, заподіяної незаконним наданням доступу до інших видів інформації.

Висновок про те, чи відносяться наслідки у вигляді нематеріальної шкоди до істотного порушення реалізації прав, свобод або законних інтересів, повинен робитися в кожному конкретному випадку з урахуванням практики правозастосування й на підставі критеріїв, зумовлених значущістю та специфікою суспільних відносин, які виступають додатковим обов'язковим об'єктом.

Окремо зауважимо, що необхідність залежності кримінальної відповідальності за незаконне надання доступу до інформації від певних наслідків продиктована передусім потребою в підвищенні ефективності застосування законодавства про кримінальну відповідальність. Чинній системі кримінально-правових засобів охорони обмеженого доступу до інформації властивий недолік, подібний до того, що був установлений в ході дослідження кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій: більшість норм, що входять до її складу, не містить чітких і прозорих критеріїв суспільної небезпечності передбачених посягань. Цілком зрозуміло, що в разі вчинення незаконного надання доступу до інформації необхідність застосування засобів кримінальної юстиції, а також їх інтенсивність повинні залежати від того, наскільки порушено ті суспільні відносини, які зумовили обмеження доступу до певної інформації.

Крім того, відсутність залежності кримінальної відповідальності за посягання у сфері обмеженого доступу до інформації від заподіяної шкоди веде до набуття кримінальною відповідальністю статусу альтернативної до цивільної або адміністративної та, відповідно, істотно знижує її ефективність. Цю тезу стосовно заборон, передбачених ст.ст. 162, 163 та 182 КК, обґрунтовано доводить С. Лихова. Дослідниця справедливо зазначає, що в умовах, коли кримінально-правові заборони не відрізняються за змістом від законодавчої характеристики ад-

міністративних проступків або цивільно-правових деліктів і, як наслідок, кримінальна відповідальність стає альтернативною, норми КК "залишаються нормами декларативного характеру, що з'явилися в КК України тому, що принцип відповідності поточного законодавства нормам Конституції України та міжнародним стандартам у галузі охорони прав людини було сприйнято надто дослівно і прямо…" [208, с. 103].

Окремим аргументом на користь запропонованого визначення кримінально караних видів незаконного надання доступу до інформації є і те, що воно розв'язує описані раніше очевидні суперечності в законодавчих оцінках суспільної небезпечності досліджуваних посягань. Як уже зазначалося, важко знайти аргументи на користь того, наприклад, чому безнаслідкове поширення конфіденційної інформації про особу (ч. 1 ст. 182, $I_{кзосн}$=24, 28) є більш небезпечним, ніж розголошення лікарської таємниці, що заподіяло тяжкі наслідки (ст. 145, $I_{кзосн}$=3,75)? У свою чергу, відповідно до запропонованого визначення будь-яке незаконне надання доступу до інформації буде визнаватися злочинним на підставі основного чинника його фактичної суспільної небезпеки – заподіяної шкоди.

Як можна побачити з диспозиції запропонованої норми (ст. 361-2), суб'єкт незаконного надання доступу до інформації – загальний. Як правило, надання незаконного доступу пов'язується з діяльністю певних спеціальних суб'єктів – осіб, яким доступ було надано у зв'язку з професійною діяльністю. Разом із тим, на сучасному етапі розвитку інформаційних технологій є підстави говорити про суспільно небезпечні види надання доступу, які вчиняють загальні суб'єкти. Ідеться про непоодинокі випадки протиправного надання доступу до закритих інформаційних ресурсів, що вчиняється шляхом так званих "хакерських атак". Наприклад, у червні 2011 року повідомлялося про поширення в мережі Інтернет частини конфіденційної інформації ресурсу SonyPictures.com, вчинене хакерською групою LulzSec. Оскільки інформація містила персональні дані клієнтів компанії, її діловій репутації було заподіяно значну шкоду [420]. Саме така специфіка сучасних посягань у дослі-

джуваній сфері зумовила пропозицію про віднесення до злочинних тих видів незаконного надання доступу, які здійснюються загальними суб'єктами. А врахування підвищеної суспільної небезпечності вчинення таких дій спеціальними суб'єктами відбувається на рівні кваліфікуючих ознак посягання.

Суб'єктивній стороні посягань, що полягають у незаконному наданні доступу до інформації (ст.ст. 361-2, 362-2), властиві особливості, притаманні злочинам із похідними наслідками. Як і в законодавчих пропозиціях щодо посягань у сфері використання інформаційних технологій, в окремих статтях КК пропонується передбачити відповідальність за умисне незаконне надання доступу до інформації, пов'язане з умисним або необережним ставленням до похідних наслідків. При цьому відповідальність за незаконне надання доступу до інформації, якщо він спричинив настання похідних наслідків із необережності, пропонується передбачити тільки для тих осіб, яким надано правомірний доступ до інформації, що є предметом посягання.

У частинах другій та третій статті 361-2 пропонується передбачити низку кваліфікованих складів незаконного надання доступу до інформації. Вчинення досліджуваного злочину *особою, яка має правомірний доступ* до інформації, що складає предмет посягання, у зв'язку з займаною посадою або спеціальними повноваженнями, матиме місце в тих випадках, коли особа, що надає незаконний доступ, має правомірний доступ до предмета посягання у зв'язку з виконуваною роботою або наданими законом повноваженнями. Характеристика ознак таких осіб наводилася в попередній главі.

Наявність такої кваліфікуючої ознаки, як "*вчинення злочину з корисливою метою*", пов'язана з обґрунтованою раніше необхідністю формування кримінально-правових заходів протидії тіньовій цифровій економіці. До більш суворої відповідальності пропонується притягати тих суб'єктів надання незаконного доступу, які в ході надання незаконного доступу переслідують мету збагачення.

Вчинення незаконного надання доступу *з використанням засобів масової інформації або інших інформаційних технологій, що забезпечують доступ до інформації значної кількості осіб*, пропонується відносити до кваліфікуючих ознак незаконного надання доступу у зв'язку з підвищеною суспільною небезпечністю організації незаконного доступу для великої кількості осіб. До інформаційних технологій масового доступу крім ЗМІ можуть відноситися інтернет-сайти, пірингові та торент-мережі тощо.

Ключове питання в *криміналізації незаконного отримання доступу* до інформації (ст. 363-1) полягає в тому, що на відміну від незаконного надання доступу його отримання далеко не завжди призводить до певних наслідків. О.Е. Радутний більш категоричний, він зазначає: "… важко навіть гіпотетично уявити собі приклад реального заподіяння істотної шкоди діями, які спрямовані тільки на отримання комерційної таємниці". Зробивши такий висновок, він пропонує передбачити кримінальну відповідальність лише за таке збирання, яке утворює реальну можливість заподіяння істотної шкоди суб'єкту господарської діяльності. [296, с. 16]. Видається. що подібний підхід має певний недолік, пов'язаний з дотриманням такого принципу криміналізації, як процесуальна здійсненність переслідування. Доволі проблематичним видається доведення можливості настання конкретних наслідків, зумовленої лише самим фактом ознайомлення з певною інформацією. Крім того, подібне законодавче рішення створило б передумови для формулювання механізму уникнення відповідальності за незаконне отримання доступу. Наприклад, за певних умов обвинуваченому було б достатньо наполягати на тому, що незаконний доступ до інформації він здійснив виключно з метою ознайомлення з нею, а отже, і можливості настання наслідків не було. Тому запропоноване визначення кримінально караного отримання доступу до інформації побудовано з урахуванням ознак, що характеризують спосіб посягання. Злочинним пропонується вважати отримання незаконного доступу, вчинене шляхом

подолання специфічних заходів захисту інформації. Розглянемо докладніше ознаки складу запропонованого злочину.

Передбачене запропонованою нормою посягання являє собою злочин із матеріальним складом. До ознак об'єктивної сторони відносяться: *діяння*, що виражається у вчиненні будь-яких дій, спрямованих на отримання можливості ознайомлення з інформацією, що складає предмет посягання; *суспільно небезпечні наслідки* у вигляді отримання незаконного доступу до інформації; *причинний зв'язок* між діянням і наслідками; *спосіб* – подолання технічних або програмних засобів захисту інформації.

Під отриманням доступу до інформації розуміється таке порушення відносин у сфері обмеженого доступу до інформації, яке полягає в копіюванні, ознайомленні або отриманні можливості ознайомлюватися з певною інформацією чи копіювати її повністю або частково. Доступ слід уважати незаконним тоді, коли його вчиняє особа, яка не має права ознайомлюватися з певною інформацією чи копіювати її. При цьому кримінально караним пропонується визнавати лише таке отримання незаконного доступу, яке пов'язане з подоланням технічних, програмних або організаційних засобів захисту інформації (характеристика цих засобів наводилася в попередній главі).

Наявність у системі ознак об'єктивної сторони специфічних характеристик способу забезпечить, як видається, достатньо чітке виокремлення з масиву всіх видів незаконного отримання доступу до інформації саме тих, які є найбільш суспільно небезпечними та мають бути включені до кримінально-правового поля. Наприклад, ознайомлення з інформацією, що відноситься до державної таємниці США та представлена на відомому загальнодоступному інтернет-ресурсі WikiLeaks, очевидно, не становить суспільної небезпеки. Водночас копіювання певних відомостей, вчинене, наприклад, шляхом подолання системи авторизованого доступу, нпевне, становить суспільну небезпеку, достатню для застосування в подібних випадках засобів кримінально-правової протидії. Інший приклад: у лип-

ні 2011 року повідомлялося, що стався масштабний витік інформації щодо змісту sms-повідомлень одного з російських операторів мобільного зв'язку. Тексти sms протягом певного часу були доступні через пошукову систему Яндекс [43]. Чи можна говорити, що особи, які ознайомлювалися з цими повідомленнями, вчиняли "порушення таємниці кореспонденції, що передається через комп'ютер" (ст. 163 КК)? Мабуть, так, але очевидно й те, що таке ознайомлення не є суспільно небезпечним. І відповідно до запропонованого формулювання незаконного отримання доступу подібні дії не відносяться до злочинних.

Потребує аргументування використання звороту "незаконне отримання доступу". Як свідчить аналіз чинного КК, для позначення незаконного отримання доступу до інформації використовуються такі формулювання, як "збирання відомостей" (ст. ст. 114, 182), "отримання відомостей" (ст. 231), "порушення таємниці" (ст. 163), "несанкціоновані дії з інформацією" (ч. 11 ст. 158, ст. 376-1), "витік інформації" (ст.ст. 361, 362). Використання трьох останніх способів, як зазначалося раніше, є недоцільним через надто широкий зміст понять "порушення таємниці", "несанкціоновані дії" та "витік інформації".

Окремо розглянемо можливості законодавчого визначення незаконного отримання доступу до інформації з використанням термінів "збирання" або "отримання відомостей". Головний аргумент на користь використання звороту "незаконне отримання доступу" продиктований тим, що відповідне законодавче формулювання має охоплювати суспільно небезпечні види незаконного отримання доступу як до інформації, поданої в традиційному вигляді (паперовий документ), так і до інформації у формі, яка дозволяє здійснювати її обробку за допомогою різноманітних технічних засобів. З цієї точки зору терміни "збирання інформації" або "отримання інформації" відповідає згаданій вимозі лише наполовину. Їх використання для опису випадків незаконного отримання доступу до інформації, поданої на "традиційних" носіях, є прийнятним. Однак спроба поширити їх на випадки, пов'язані з використанням

сучасних інформаційних технологій, наочно демонструє недоцільність застосування останніх в тексті закону. Проблема полягає в можливості неоднозначного тлумачення. Так, наприклад, немає чіткої відповіді на питання про те, чи слід уважати збиранням тільки несанкціонований доступ до комп'ютерної мережі, вчинений із використанням чужих реквізитів авторизації. У цій ситуації особа не отримує відомостей з обмеженим доступом, вона отримує лише можливість вчинення певних дій з інформацією з обмеженим доступом. Отже, відповідь на питання про те, чи охоплюються подібні випадки термінами "збирання інформації" або "отримання інформації", є доволі дискусійною. Разом із цим, як свідчать описані раніше тенденції трансформації посягань у сфері незаконного отримання доступу до інформації, такі випадки можуть становити значну суспільну небезпеку та потребувати кримінально-правової оцінки. Саме тому найбільш доцільно використати термін, який має чітке законодавче визначення та може бути поширений на всі види розгляданих посягань незалежно від їх технічної основи.

Так, Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року [102] містить такі визначення "доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі", "обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання введення, записування, перетворення зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів". Тлумачення означених визначень дозволяє дійти однозначного висновку: формулювання "незаконне отримання доступу до інформації", якщо воно буде використане в законі про кримінальну відповідальність, забезпечить можливість кримінально-правової оцінки посягань, пов'язаних як зі збиранням інформації з обмеженим доступом, що обробляється в інформаційно-телекомунікаційних системах, та ознайомленням з нею, так і з отриманням можливості збирати таку інформацію чи ознайо-

млюватися з нею. При цьому оскільки запропонована норма (363-1) не пов'язана виключно з інформацією, яка подана у формі, що дозволяє її обробку за допомогою різноманітних технічних засобів, то наведене формулювання охоплюватиме й випадки, пов'язані з незаконним отриманням доступу до інформації на "традиційних" носіях. Отже, саме використане в запропонованій нормі формулювання ("незаконне отримання доступу до інформації") є найбільш прийнятним.

До кваліфікуючих ознак незаконного отримання доступу до інформації (ч. 2 ст. 363-1) пропонується відносити: 1) використання для вчинення доступу спеціалізованих програмних або технічних засобів; 2) отримання незаконного доступу з метою його подальшого надання третім особам.

Під спеціалізованими програмними або технічними засобами пропонується розуміти такі комп'ютерні програми або устаткування, які розроблено спеціально для отримання незаконного доступу до інформації. Це можуть бути різного роду "троянські" програми, спеціалізоване обладнання для зняття інформації з каналів зв'язку тощо.

Пропозиція криміналізації отримання незаконного доступу з метою його подальшого надання третім особам продиктована обґрунтованою раніше необхідністю вдосконалення кримінально-правових засобів протидії "тіньовій цифровій економіці". Про наявність такої мети може свідчити подальша передача отриманих відомостей або їх розміщення на загальнодоступних інформаційних ресурсах.

Слід зауважити, що запропоновані норми усувають такий установлений раніше недолік чинного кримінального законодавства, як необґрунтоване завищення законодавчої оцінки суспільної небезпечності посягань у сфері обмеженого доступу до інформації в разі їх вчинення з використанням комп'ютерних технологій. Відповідно до наведених пропозицій однаковою є законодавча оцінка суспільної небезпечності як незаконного надання доступу у вигляді передачі певних паперових носіїв інформації, так і надання доступу до захищених комп'ютерних даних; немає принципової різниці і в оцінці не-

законного отримання доступу до інформації шляхом, наприклад, злому сейфу з документацією або шляхом підбору пароля до захищеної інформаційної системи. При цьому підвищена суспільна небезпечність використання для надання або отримання доступу спеціалізованих програмних або технічних засобів ураховується на рівні кваліфікуючих ознак. Таким чином, як видається, законодавча оцінка суспільної небезпечності досліджуваних посягань наближається до її фактичних чинників.

Для обґрунтування розмірів санкцій запропонованих норм маємо ще раз звернутися до питання суспільної небезпечності посягань на інформаційну безпеку в цілому та відносин у сфері обмеженого доступу до інформації зокрема. Як було доведено в першій главі, суспільна небезпечність посягання на інформаційну безпеку визначається значущістю тих суспільних відносин, у межах яких виникає інформаційна потреба. Наведені пропозиції враховують таку специфіку насамперед у тому, що кримінальна відповідальність як за посягання у сфері використання інформаційних технологій, так і за посягання у сфері обмеженого доступу до інформації залежить від настання похідних наслідків: істотного порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, державних чи громадських інтересів, діяльності юридичної особи. При цьому, як правильно зазначає О.О. Книженко, "загальні вимоги щодо санкції полягають у тому, що покарання, зазначене в санкції, має відбивати ступінь суспільної небезпечності названого в диспозиції діяння та бути узгодженим із санкціями статей, що передбачають відповідальність за вчинення інших близьких за видом та характером злочинів" [85, с. 35]. Отже, інтенсивність означених похідних наслідків є критерієм диференціації суворості санкій за злочини у сфері обмеженого доступу до інформації, а їх розмір узгоджується з санкціями статей, що передбачають відповідальність за вчинення злочинів у сфері використання інформаційних технологій, які близькі за характером наслідків (ст.ст. 361, 361-1, 362, 362-1 запропонованого проекту закону).

Таким чином, реалізація наведених пропозицій щодо вдосконалення системи кримінально-правових засобів забезпечення обмеженого доступу до інформації дозволить наблизити законодавчі оцінки суспільної небезпечності відповідних посягань до їх фактичних чинників. Таке оновлення законодавства про кримінальну відповідальність створить передумови для раціональнішого використання засобів кримінальної юстиції в означеній сфері. Крім цього, застосування загальних норм забезпечить певну стабільність законодавства про кримінальну відповідальність, його готовність в умовах подальшої інформатизації суспільства до прогнозованого зростання видів інформації з обмеженим доступом. Як правильно зазначає В.О. Навроцький, "розвиток кримінального законодавства шляхом надання пріоритету загальним нормам, окрім інших переваг, дозволить скоротити коло прогалин у кримінальному законі" [242, с. 136].

5.2. Кримінально-правове забезпечення реалізації прав громадян на доступ до інформації

Властива правовому регулюванню відносин надання доступу до інформації дуалістичність забезпечує існування двох груп правових засобів забезпечення інформаційної безпеки у її відповідному сегменті. Ця дуалістичність, як зазначалося раніше, полягає в забезпеченні правовими заходами балансу між протилежними суспільними інтересами: потребою в обмеженні доступу до інформації та потребою в отриманні доступу до інформації. Відповідно існують дві групи правових заходів: правові заходи інформаційної безпеки у сфері обмеженого доступу до інформації та правові заходи інформаційної безпеки у сфері отримання доступу до інформації. Специфіку кримінально-правових заходів першої групи було досліджено в попередній підглаві. Розглянемо особливості кримінально-правової протидії порушенням у сфері отримання доступу до інформації.

Як правильно зазначає А.І. Марущак, доступ до інформації – це "гарантована державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб" [228]. Отже, у загальному розумінні зміст відносин у сфері отримання доступу полягає в наявності в одних суб'єктів права на отримання певної інформації, а в інших – відповідного обов'язку надавати її. Порушення таких відносин полягає зазвичай у ненаданні інформації або наданні неправдивої чи неповної інформації особою, яка має зобов'язання щодо надання доступу до цих відомостей. Ураховуючи це, уважаємо за можливе до системи кримінально-правових засобів забезпечення отримання доступу до інформації віднести положення КК про відповідальність за такі види ненадання певної інформації: неповідомлення про перебування особи в небезпечному для життя стані (ст. 136); неподання, несвоєчасне подання або подання недостовірної інформації про фінансові операції, що відповідно до закону підлягають фінансовому моніторингу, спеціально уповноваженому центральному органові виконавчої влади зі спеціальним статусом з питань фінансового моніторингу (ч. 1 ст. 209-1); ненадання інформації про діяльність емітента в межах, передбачених законом, або надання йому недостовірної інформації (ст. 232-2); приховування або умисне перекручення відомостей про екологічний, у тому числі радіаційний, стан, який пов'язаний із забрудненням земель, водних ресурсів, атмосферного повітря, харчових продуктів, продовольчої сировини та який негативно впливає на здоров'я людей, рослинний і тваринний світ, а також про стан захворюваності населення в районах з підвищеною екологічною небезпекою (ст. 238-1); неповідомлення про підготовлюване або здійснене внаслідок крайньої потреби скидання чи невідворотні втрати в межах внутрішніх морських і територіальних вод України або у відкритому морі шкідливих речовин чи сумішей, що містять такі речовини понад

установлені норми (ч. 3 ст. 243); неповідомлення капітаном судна іншому судну, що зіткнулося з ним у морі, назви і порту приписки свого судна, а також місця свого відправлення та призначення (ст. 285); приховування документів Національного архівного фонду (ст. 298-1); відмова свідка від давання показань (ст. 385).

Дослідження цієї системи норм методом контекстної законодавчої оцінки суспільної небезпечності дозволяє стверджувати, що вона відповідає чинникам фактичної небезпечності відповідних посягань, є послідовною й обґрунтованою (додаток 8). Так, відповідно до чинного КК найбільш небезпечними видами кримінально караного обмеження доступу до інформації є: приховування відомостей про екологічний стан у місцевості, оголошеній зоною надзвичайної екологічної ситуації, або таке, що спричинило загибель людей чи інші тяжкі наслідки (ч. 2 ст. 238, $I_{кзосн} = 69{,}93$), а також кваліфіковане й особливо кваліфіковане приховування документів Національного архівного фонду (ч. 3 ст. 298-1, $I_{кзосн} = 66{,}51$; ч. 2 ст. 298-1, $I_{кзосн} = 52{,}39$). Ці посягання належать до злочинів середньої тяжкості, решта посягань виділеної групи – злочини невеликої тяжкості. Як можна побачити з додатка, досліджувана система норм характеризується достатньо послідовним урахуванням чинників суспільної небезпечності та їх обґрунтованим впливом на інтенсивність відповідних санкцій.

При цьому більшість розгляданих норм пов'язують настання кримінальної відповідальності за обмеження доступу до інформації із заподіянням певної, чітко визначеної шкоди (ч. 2 ст. 238, ст. 232-1, ч. 3 ст. 243, ч. 1 ст. 209-1, ч. 1 ст. 136). Решта ж норм передбачають відповідальність за злочини із нормальними складами, але містять конкретні, прозорі й очевидні критерії суспільної небезпечності відповідних посягань. Ці критерії: 1) стосуються змісту відомостей, до яких обмежується доступ (відомості про екологічний стан (ч. 1 ст. 238), свідчення в кримінальній справі (ст. 385), документи Національного архівного фонду (ст. 298-1)); 2) зумовлені обстановкою, у якій здійснюється обмеження доступу (перебування малолітнього в не-

безпечному для життя стані (ч. 2 ст. 136)); 3) продиктовані ратифікованими міжнародними зобов'язаннями (обов'язок повідомлення назви судна при зіткненні, ст. 285). Таким чином, система кримінально-правових норм щодо відповідальності за окремі види обмеження доступу до інформації характеризується відсутністю очевидних недоліків, пов'язаних із законодавчим описом чинників суспільної небезпечності відповідних посягань.

Разом із тим, аналізу потребує відповідність цієї системи сучасним соціальним потребам у кримінально-правовій протидії обмеженню доступу до інформації. Слід зазначити, що питання правового регулювання забезпечення доступу до інформації активно обговорюється в юридичній науці.

Ключові тези дискурсу щодо соціального значення реалізації права на доступ до інформації, а відповідно, і чинників небезпеки його порушення, можна систематизувати таким чином. По-перше, в умовах інформатизації суспільства доступ *набуває значення об'єктивної потреби*. Як правильно зазначає О. Яременко, "діяльність держави супроводжується інформаційними процесами, у результаті яких у системі державного механізму концентруються значні за обсягом та важливістю інформація та інформаційні ресурси. У суспільстві постійно зростає значення даної інформації та попит на неї…" [388]. По-друге, забезпечення доступу до інформації є атрибутивною властивістю демократичного розвитку. Так, А. Марущак доводить, що "отримання учасниками суспільних відносин достовірної і повної інформації про процеси та явища у суспільстві, державі, навколишньому середовищі є основою реалізації їх (учасників) інформаційних потреб, *складовою формування демократичного суспільства*" [226]. Цю тезу розвиває Л. Задорожня, яка зазначає, що можливості доступу до суспільно значущої інформації слід розглядати як прояви формування в країні громадянського суспільства. А забезпечення доступу "можна розглядати як основу для реальної участі громадян в управлінні справами держави, контролю за діяльністю органів влади і громадських організацій. Доступ до інформації та її своєчасне

отримання є реальною гарантією забезпечення прав громадянина на чисте навколишнє середовище та безпечні продукти, на судовий захист та інших прав" [97, с. 7 – 8]. Нарешті, потретє, наголошується на *значенні доступу в цивілізаційному контексті*. Так, І.В. Арістова звертає увагу на правові механізми подолання "цифрового розподілу", соціальної нерівності, зумовленої різними можливостями в доступі до інформації, та обґрунтовує, що саме ефективне нормативне регулювання доступу громадян до знань, які мають суспільне значення, слід розглядати як одну з необхідних умов розвитку українського суспільства, його включення до світових модернізаційних процесів [15].

Отже, забезпечення доступу до інформації є соціально значущим. У зв'язку з цим виникає справедливе питання щодо відповідності системи кримінально-правових засобів забезпечення доступу до інформації, передбаченої чинним КК, соціальній потребі в захисті відповідної групи відносин. Актуальності питанню додає й той факт, що в кримінальному законодавстві деяких країн передбачено спеціальну відповідальність за обмеження доступу до інформації. Так, ст. 140 КК РФ "Відмова в наданні громадянину інформації" передбачає відповідальність за "неправомірну відмову посадової особи в наданні зібраних у встановленому порядку документів і матеріалів, які безпосередньо торкаються прав і свобод громадянина, або надання громадянинові неповної чи свідомо неправдивої інформації, якщо ці діяння заподіяли шкоду правам і законним інтересам громадян". Пропозиції щодо доповнення КК України подібною нормою висловлювалися й у вітчизняному науковому дискурсі. Н.А. Савінова вважає доцільним доповнення КК України статтею про відповідальність за "ненадання особі або її представникові, який діє на законних підставах, інформації про таку особу (персональної інформації) службовою особою підприємства, установи, організації" [308, с. 294]

Відповідь на поставлене питання слід давати починаючи з висновків російських дослідників щодо практики й ефективності використання вищезазначеної норми. Так, російська до-

слідниця О.В. Красненкова констатує вкрай незначну практику використання ст. 140 КК РФ. При цьому вона звертає увагу на численні порушення з боку посадових осіб, зобов'язаних надавати певну інформацію, і робить обґрунтований висновок щодо неефективності кримінально-правової протидії в цій сфері [146, с. 102]. У зв'язку з цим Д.О. Калмиков пропонує внести зміни до розгляданої норми та передбачити кримінальну відповідальність за сам факт ненадання певної інформації незалежно від наслідків, що настали. Він аргументує це рішення складністю встановлення наслідків та значущістю права на доступ до інформації як такого [116, с. 140 – 147]. Із такою пропозицією важко погодитися, особливо враховуючи доведені раніше висновки щодо специфіки суспільної небезпечності посягань на інформаційну безпеку, її залежності від інтенсивності шкоди, заподіяної тим суспільним відносинам, у межах яких використовується інформація, що є предметом посягання. Більш обґрунтованою видається позиція російського дослідника В.Н. Лопатіна. Він зазначає, що, незважаючи на задекларованe Конституцією право на свободу інформації та передбачену в Кримінальному кодексі РФ відповідальність за ненадання громадянам інформації (ст. 140 КК РФ), реалізації цього права багато в чому перешкоджає декларативність законів. Тобто головна проблема зумовлена не стільки неефективністю засобів кримінально-правового захисту, скільки недоліками правового регулювання інформаційної діяльності [216, с. 26].

До критичних зауважень російських дослідників додамо також співставлення санкцій за незаконну відмову в наданні інформації та зловживання або перевищення влади чи службових повноважень, оскільки відмова в наданні інформації фактично є їх спеціальним видом. Якщо найбільш суворе покарання за відмову в наданні інформації – 5 років позбавлення права обіймати певні посади чи займатися певною діяльністю, то за некваліфіковане зловживання службовими повноваженнями або їх перевищення можливе покарання до 4-х років позбавлення волі. При цьому відповідальність за всі ці злочини

настає за умови заподіяння певної шкоди правам, свободам або інтересам громадян. Подібний підхід до формулювання спеціальних норм викликає зауваження щодо доцільності й обґрунтованості зниження суворості кримінальної відповідальності саме за цей вид зловживання чи перевищення влади або повноважень.

Таким чином, ефективність кримінально-правового захисту відносин забезпечення доступу до інформації залежить насамперед від якості правового регулювання інформаційної діяльності. Наявність чіткого й прозорого інформаційного законодавства дозолить "задіяти" наявні в КК правові засоби (норми про відповідальність за злочини у сфері службової діяльності) для охорони відносин у сфері реалізації права на доступ до інформації.

Вищенаведений висновок можна цілком застосувати й до національних реалій. Недосконаліть чинного інформаційного законодавства не дозволяє повною мірою забезпечувати захист відносин у сфері надання доступу кримінально-правовими засобами. Так, Л. Задорожня зазначає, що незважаючи на передбачені законодавством ґарантії прав громадян та юридичних осіб на інформацію, механізм її реальної доступності потребує вдосконалення. Дослідниця звертає увагу на відсутність системного правового регулювання процесів взаємодії органів влади з фізичними та юридичними особами: норми, що встановлюють окремі правила інформаційної взаємодії, розпорошені в підзаконних актах; положення окремих норм мають суперечливий характер, не узгоджуються одне з одним; наявність значної кількості "білих плям" у законодавстві щодо інформаційної взаємодії держави з громадянами; відсутність чіткого розмежування адміністративного та цивільно-правового регулювання в галузі інформаційної взаємодії, що призводить до суперечностей при регулюванні відповідних суспільних відносин [97, с. 15]. О. Яременко звертає увагу на проблеми юридичного закріплення права на доступ до правової інформації та механізмів його реалізації. Він обґрунтовує, що "на сьогодні у зв'язку із постійним зростанням ролі правової

інформації, ускладненням інформаційно-правових відносин, розвитком інформаційно-комунікаційних систем існує об'єктивна необхідність подальшого вдосконалення матеріальних та процесуальних норм щодо доступу до цієї інформації" [389]. О. Ботвінкін фіксує проблему недостатнього правового регулювання інформаційної діяльності, пов'язану з тим, що залишаються нормативно не визначеними механізми доступу громадян до інформації органів державної влади та місцевого самоврядування, не встановлені норми відповідальності за обмеження чи порушення права громадянина на доступ до інформації [31, с. 58]. Г. Шлома дійшов висновку, що органи влади фактично безпідставно відмовляють у наданні інформації, відносячи її до інформації з обмеженим доступом, направомірно використовуючи грифи обмеження доступу [Шлома Г.О. Місце інституту службової таємниці в діяльності державних органів України // Науковий вісник Львівського державного університету внутрішніх справ: Сер. юрид. – Л., 2006. – Вип. 3. – С. 157 – 168]. Отже, слід погодитися з думкою тих дослідників, які вважають, що першочерговим законодавчим заходом, спрямованим на поліпшення нормативного забезпечення реалізації інформаційних прав громадян, має стати конкретизація, на рівні відповідних законів, можливих випадків обмеження інформаційних прав громадян [Ліпкан, В. Інформаційні права і свободи людини та громадянина / В. Ліпкан, Ю. Максименко // Підприємництво господарство і право. – 2011. – № 9. – С. 64 – 68. – С. 68].

Залежність ефективності кримінально-правових засобів забезпечення доступу до інформації від якості законодавчих актів, що регулюють відповідні відносини, можна доволі чітко простежити шляхом аналізу судової практики Європейського суду з прав людини. Так, самостійним питанням є правове забезпечення реалізації прав громадян на доступ до інформації про себе. Якість нормативних приписів у розгляданій сфері неодноразово була предметом розгляду цього суду. Його рішення є, так би мовити, "концентрованим" викладом основних аспектів мети, доцільності та меж правового регулювання в

зазначеній сфері. Саме тому, а також ураховуючи, що відповідно до Закону України "Про виконання рішень та застосування практики Європейського суду з прав людини" від 23 лютого 2006 року (стаття 17) національні суди використовують практику Європейського суду з прав людини як джерело права, огляд цих рішень є важливим для нашого дослідження.

Право на отримання інформації про себе розглядається в судовій практиці як складова права на повагу до приватного життя (ст. 8 Європейської конвенції про захист прав людини та основоположних свобод). Головні риси такого підходу було сформульовано в рішеннях у справах Leander v. Sweden (1987) та Gaskin v. UK (1989). Посилаючись на останнє рішення, суд у справі "Мікулич проти Хорватії" (2002) [322] постановив, що "згідно з положенням про повагу до приватного життя кожен повинен мати змогу з'ясувати конкретні відомості про свою особу як конкретну людину і що право людини на таку інформацію є значущою завдяки своєму визначальному впливу на її особистість". Це, можна сказати, загальна норма. Спеціальні норми, такі, що стосуються, наприклад, діяльності правоохоронних органів, містяться в рішеннях у справах "Сегерштед-Віберг та інші проти Швеції" (2006 рік) [137] і "Класс та інші проти Німеччини" (1978 рік) [321].

Питання можливості суб'єктів персональних даних ознайомлюватися з інформацією про себе, що міститься в базах даних правоохоронних органів, було предметом розгляду в справі "Сегерштед-Віберг та інші проти Швеції" [137], рішення у якій було ухвалено 6 червня 2006 року. П. Сегерштед-Віберг, п. Нигрен, п. Ехенбом, п. Фрейд та п. Шмід зверталися із запитами про отримання цілковитого доступу до справ, що були порушені щодо них поліцією безпеки Швеції, однак одержали відмову на тій підставі, що відкриття цих даних може загрожувати національній безпеці та суперечить меті запобігання злочинності.

Суд дослідив висновки національних судових та адміністративних структур про те, що розкриття інформації в повному обсязі може мати негативні наслідки для функціонування

системи таємного спостереження, яка створена й функціонує з метою захисту національної безпеки країни та боротьби з тероризмом. За результатами цього дослідження суд дійшов висновку, що в держави були необхідні підстави вважати інтереси національної безпеки та боротьбу з тероризмом важливішими, ніж заінтересованість заявників у наданні їм повного доступу до матеріалів про них. Таким чином, відмова в наданні повного доступу до інформації про заявників не була визнана порушенням статті 8 Конвенції. Рішення в цій справі, як видається, є певним орієнтиром для вдосконалення чинного національного законодавства з питань надання громадянам доступу до інформації про них, яка обробляється в автоматизованих системах персональних даних правоохоронних органів. На нашу думку, Закон України "Про оперативно-розшукову діяльність" має містити певну конкретизацію положень ст. 32 Конституції України стосовно можливості ознайомлення громадян з інформацією про себе, яка накопичується підрозділами, що здійснюють оперативно-розшукову діяльність. Абсолютно зрозуміло, що закон не повинен передбачувати повного доступу, він (доступ) має бути чітко обмежений метою оперативно-розшукової діяльності, необхідністю захисту прав і свобод інших громадян, вимогами національної безпеки тощо. Наявність таких норм забезпечить обґрунтоване й ефективне застосування засобів кримінальної юстиції до тих посадових осіб правоохоронних органів, які незаконно обмежують доступ громадян до інформації про себе.

Питання повідомлення громадян про здійснення щодо них оперативно-розшукових заходів досліджувалося в справі "Класс (Klass) та інші проти Німеччини" (рішення від 6 вересня 1978 року) [321]. Заявники оскаржували положення законодавства ФРН про те, що органи влади не зобов'язуються повідомляти зацікавлених осіб про застосування обмежень права на таємницю листування, поштових відправлень і телефонних розмов, чим виключається можливість оскарження таких заходів у суді. Із цього приводу заявники зверталися до Конституційного

Суду ФРН, який визнав оскаржуваний закон таким, що не відповідає Основному Законові в частині, що не допускає повідомлення особи, за якою здійснювалося спостереження, навіть тоді, коли таке повідомлення можна було зробити, не заподіявши шкоди меті здійснених заходів. Однак заявники залишилися незадоволеними цим рішенням, уважаючи несумісною з гарантіями основних прав і свобод громадян заміну судового захисту прав у цій сфері наглядовими функціями уповноважених органів. Суд ретельно дослідив питання можливості та доцільності обов'язкового повідомлення в усіх випадках та дійшов таких висновків: діяльність або небезпека, проти якої застосовуються засоби спостереження, може тривати певний час після призупинення цих заходів; подальше повідомлення кожної особи, яка піддавалася призупиненому заходу, може створити значну загрозу для довгострокової мети, що була причиною застосування спостереження; такі повідомлення можуть спричинити розголошення методів і сфер діяльності розвідувальних служб та навіть розсекречення їх агентів; саме неповідомлення про застосовані заходи гарантує ефективність втручання. З урахуванням наведених міркувань суд дійшов висновку про відсутність у розгляданому випадку порушення прав на повагу до приватного життя, передбаченого статтею 8 Конвенції. Це рішення, як видається, є достатньо вагомим аргументом для внесення змін до ч. 9 ст. 9 Закону України "Про оперативно-розшукову діяльність", яка передбачає право громадян на отримання пояснень з приводу обмеження прав і свобод, але зовсім не містить положень стосовно того, чи в кожному випадку відповідного звернення громадянина правоохоронні органи мають давати таке пояснення. Певною мірою можна погодитися, що відповідь на це питання міститься в наступній частині згаданої статті, але в частині десятій ідеться не про "пояснення", а про "відомості", що потенційно може породжувати неоднозначне розуміння положень закону, і це знову ж таки повертає нас до питання якості закону та залежної від нього ефективності кримінально-правового захисту.

Зазначимо, що останнім часом питанню правового регулювання забезпечення доступу до інформації приділяється значна увага. Так, прийнято Закон України "Про доступ до публічної інформації", суттєво оновлено Закон України "Про інформацію", певним чином відрегульовано відносини у сфері забезпечення доступу громадян до інформації про себе (Закон України "Про захист персональних даних"). Кодекс про адміністративні правопорушення передбачає відповідальність за неправомірну відмову в наданні інформації (ст. 212-3). У тих випадках, коли означені дії призводять до істотних наслідків, можна застосувати норми КК, які передбачають відповідальність за зловживання повноваженнями або перевищення їх (ст.ст. 364, 364-1, 365, 365-1). Однак через те, що низка питань, зокрема щодо механізму реалізації права на доступ до інформації, підстави його обмеження тощо, залишається відкритою, можливості застосування зазначених кримінально-правових засобів є обмеженими.

Таким чином, ефективність кримінально-правового захисту відносин у сфері надання доступу до інформації залежить насамперед від якості правового регулювання інформаційних відносин. Водночас, передбачена чинним законодавством система відповідних кримінально-правових засобів є обґрунтованою й достатньою, дозволяє забезпечити ефективний захист відносин у сфері надання доступу до інформації. Разом із тим, оскільки ці питання перебувають поза межами предмета дослідження, зазначимо, що проблема вдосконалення нормативного регулювання реалізації прав громадян на доступ до інформації потребує подальшого наукового аналізу. Також зауважимо, що вельми перспективним напрямом кримінально-правових досліджень видається аналіз можливостей використання чинних законів про кримінальну відповідальність за зловживання, перевищення повноважень та недбалість як засобів правової охорони прав громадян на доступ до інформації.

Висновки до п'ятої глави

Проведений аналіз кримінально-правових засобів за безпечення доступу до інформації дозволяє зробити такі висновки:

1. Сутність порушень інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу полягає в тому, що ускладнення чи унеможливлення реалізації інформаційної потреби зумовлюється порушенням установленого режиму доступу до певного ресурсу або неправомірним обмеженням доступу до певної інформації. Межі кримінально-правового регулювання у сфері забезпечення доступу до інформаційного ресурсу визначаються інтенсивністю наслідків, які настають через обмеження можливості реалізації інформаційної потреби відповідних суб'єктів.

2. Дослідження чинної системи кримінально-правових засобів забезпечення обмеженого доступу до інформації з використанням методу контекстної законодавчої оцінки суспільної небезпечності дало змогу встановити її вади: 1) очевидна невідповідність суспільної небезпечності низки діянь, передбачених КК, інтенсивності санкцій відповідних норм; 2) непослідовність законодавчих рішень у питанні встановлення кримінальної відповідальності за спеціальні види незаконного отримання або надання доступу до інформації, особливо необґрунтоване підвищення санкцій за несанкціонований доступ у разі його вчинення з використанням інформаційних технологій; 3) непослідовна законодавча оцінка схожих за змістом ознак, що характеризують суб'єкт посягання; 4) спірні законодавчі рішення в питанні формулювання ознак кваліфікованих посягань на відносини щодо забезпечення обмеженого доступу до інформації; 5) неузгодженість використовуваної термінології.

3. Аналіз кримінально-правових засобів забезпечення обмеженого доступу до інформації на предмет відповідності сучасним проявам суспільно небезпечної поведінки у сфері отри-

мання та надання незаконного доступу до інформації свідчить про фрагментарність і несистемність законодавства в цій сфері. Наявні в КК норми не можуть розглядатися як нормативна база ефективної протидії зростанню тіньової цифрової економіки.

4. Сформульовано пріоритетні завдання вдосконалення системи кримінально-правових засобів забезпечення обмеженого доступу до інформації. До них віднесено: 1) подолання фрагментарності кримінально-правової охорони; 2) пошук загальних підходів до законодавчої оцінки суспільної небезпечності окремих видів незаконного отримання або надання доступу; 3) розвиток системи як засобу протидії формуванню ринку незаконних інформаційних послуг.

5. Обґрунтовано, що як просту форму кримінально караного надання доступу до інформації доцільно криміналізувати незаконне надання доступу до таємної, службової або конфіденційної інформації, якщо це спричинило істотне порушення реалізації прав, свобод, законних інтересів.

6. До кваліфікуючих ознак незаконного надання доступу до інформації пропонується відносити: повторність; вчинення злочину групою осіб за попередньою змовою; вчинення злочину особою, яка має правомірний доступ до інформації у зв'язку із займаною посадою або спеціальними повноваженнями; використання засобів масової інформації або інших інформаційних технологій, що забезпечують доступ до інформації значної кількості осіб; вчинення злочину з корисливою метою; спричинення тяжких наслідків.

7. Запропоновано визначення простої форми злочинного отримання доступу до інформації як отримання незаконного доступу до таємної, службової або конфіденційної інформації, вчинене шляхом подолання технічних, програмних або організаційних засобів захисту інформації.

8. До кваліфікуючих ознак незаконного отримання доступу до інформації пропонується відносити: повторність; вчинення злочину групою осіб за попередньою змовою; використання технічних або програмних засобів, призначених для незаконного отримання доступу до інформації; вчинення злочину з метою надання незаконного доступу до інформації.

9. Для наближення законодавчих оцінок суспільної небезпечності посягань у сфері обмеженого доступу до їх фактичних чинників, створення передумов для більш раціонального використання засобів кримінальної юстиції в розгляданій сфері та забезпечення стабільності законодавства про кримінальну відповідальність в умовах подальшої інформатизації суспільства запропоновано зміни до КК, які передбачають: доповнення КК загальними нормами про незаконне надання доступу та його отримання; скасування низки норм, що передбачають окремі види порушень обмеженого доступу до різноманітних видів інформації.

10. Передбачена чинним законодавством система кримінально-правових засобів забезпечення надання доступу до інформації є обґрунтованою та достатньою, дозволяє забезпечити ефективний захист відносин у сфері надання доступу до інформації. Разом із тим, її ефективність залежить від якості правового регулювання інформаційної діяльності.

Глава 6

Кримінально-правова охорона суспільних відносин у сфері формування інформаційного ресурсу

Специфіка досліджуваної в цій главі сукупності кримінально-правових заборон зумовлена особливостями соціальної значимості суспільних відносин інформаційної безпеки відповідної групи та, як наслідок, особливостями характеру суспільної небезпечності посягань на ці відносини. Як зазначалося в першій главі, інформаційна безпека являє собою відносини, у межах яких забезпечується можливість реалізації інформаційної потреби. Ця реалізація здійснюється шляхом отримання доступу до необхідної інформації, ґрунтується на використанні інформаційних технологій та забезпечується формуванням інформаційного ресурсу. Отже, соціальна значимість досліджуваної складової інформаційної безпеки полягає в тому, що завдяки функціонуванню суспільних відносин формування інформаційного ресурсу забезпечується можливість реалізації інформаційної потреби.

Таким чином, специфіка посягань на інформаційну безпеку в розгляданій сфері полягає в тому, що певні суспільно небезпечні наслідки настають через те, що суб'єкт отримує інформаційний ресурс, який не дозволяє ефективно розв'язувати поставлені перед ним завдання, призводить до вчинення суб'єктом певних негативних дій. Наприклад, суспільна небезпечність публічних закликів до повалення конституційного ладу (ст. 109 КК) полягає в тому, що певні суб'єкти суспільного життя, які мають потребу в суспільно-політичній інформації щодо можливостей розвитку країни, будуть введені в оману

стосовно доцільності розв'язання нагальних соціальних проблем шляхом насильства. У свою чергу наявність значної кількості таких суб'єктів становитиме загрозу національній безпеці країни.

Тобто якщо порушення у сфері використання інформаційних технологій або забезпечення доступу до інформації унеможливлюють реалізацію інформаційної потреби, то в разі порушення інформаційної безпеки у сфері формування ресурсу суб'єкт одержує можливість реалізувати інформаційну потребу, але через порушення така реалізація призводить до настання певних наслідків, так би мовити, соціально дезорієнтує суб'єкта.

Як зазначалося раніше, соціальна потреба в правовій охороні відносин формування інформаційного ресурсу актуалізується наявністю таких неґативних суспільних тенденцій: надмірна капіталізація інформаційного простору; небезпека антидемократичного розвитку через маніпуляції суспільною свідомістю в політичній сфері; зростання рівня ідеологічної вразливості політичних систем через наявність потенціалів глибоких соціальних конфліктів, які можуть бути задіяні шляхом використання інформаційних технологій; втрата навичок роботи з інформацією через надмірне насичення нею соціального буття; небезпека системних порушень права на повагу до приватного життя та тотального контролю над особистістю через створення надпотужних баз персональних даних. У цій главі ми розглянемо, наскільки чинне законодавство про кримінальну відповідальність кореспондується із зазначеними соціальними потребами.

6.1. Кримінально-правове забезпечення формування інформаційного ресурсу в контексті соціальних тенденцій

До кримінально-правових засобів охорони суспільних відносин інформаційної безпеки у сфері формування інформаційного ресурсу, передбачених чинним КК, видається можли-

вим віднести норми про відповідальність за такі дії: публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (чч. 2, 3 ст. 109); публічні заклики чи розповсюдження матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, установленого Конституцією України (ст. 110); умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образа почуттів громадян у зв'язку з їхніми релігійними переконаннями (ст. 161); перешкоджання законній професійній діяльності журналістів (ст. 171); публічні заклики до вчинення терористичного акту (ст. 258-2); заклики до вчинення дій, що загрожують громадському порядку (ст. 295); ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300); ввезення, виготовлення, збут та розповсюдження порнографічних предметів (ст. 301); публічні заклики до геноциду (ч. 2 ст. 442).

Аналіз наведеної сукупності законів про кримінальну відповідальність методом контекстної оцінки суспільної небезпечності діяння (додаток 9) дозволяє стверджувати, що чинний КК містить у цілому обґрунтовані та послідовні оцінки суспільної небезпечності злочинних посягань у сфері формування інформаційного ресурсу. Разом із цим, необхідно звернути увагу на низку спірних положень.

Цілком зрозумілим, таким, що не потребує додаткової аргументації, є питання протидії створенню та розповсюдженню дитячої порнографії. Однак певним перебільшенням видається те, що чинний КК незаконні дії з дитячою порнографією, вчинені повторно або за попередньою змовою групою осіб, або з отриманням доходу у великому розмірі (ч. 5 ст. 301, $I_{кзосн} = 93,39$), за рівнем суспільної небезпечності прирівнює до публічних закликів до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку,

установленого Конституцією України, *які призвели до загибелі людей або інших тяжких наслідків* (ч. 3 ст. 110, $I_{кзосн} = 92,71$). Так само заслуговує на увагу і той факт, що некваліфіковані незаконні дії з дитячою порнографією (ч. 4 ст. 301, $I_{кзосн} = 89,52$) визнаються більш небезпечними, ніж умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образа почуттів громадян у зв'язку з їхніми релігійними переконаннями, які були вчинені *організованою групою осіб або спричинили тяжкі наслідки* (ч. 3 ст. 161, $I_{кзосн} = 83,37$). На нашу думку, підтвердженням необґрунтованого підходу законодавця до оцінки суспільної небезпечності злочинів, пов'язаних зі створенням або розповсюдженням порнографії, є й те, що за умови практично рівної оцінки простих незаконних дій з порнографічними предметами (ч. 1 ст. 301, $I_{кзосн} = 25,51$) та простих незаконних дій із творами, які пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 1 ст. 300, $I_{кзосн} = 25,74$), законодавчі оцінки кваліфікованих видів цих посягань суттєво відрізняються. Так, відповідальність за повторне або вчинене групою осіб поширення творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 3 ст. 300, $I_{кзосн} = 74,03$), є менш суворою, ніж за вчинення незаконних дій з порнографічними предметами за наявності аналогічних кваліфікуючих ознак (ч. 3 ст. 301, $I_{кзосн} = 82,46$). Така непослідовність є більш помітною при порівнянні суворості санкцій за примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру (ч. 4 ст. 301, $I_{кзосн} = 89,52$) та примушування неповнолітніх до участі у створенні творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 3 ст. 300, $I_{кзосн} = 74,03$).

Досить спірною видається і майже однакова законодавча оцінка суспільної небезпечності (верхня межа санкції – 5 років

позбавлення волі) незаконних дій щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збуту неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру (ч. 2 ст. 301), з одного боку, а з іншого:

1) публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до таких дій, вчинених особою, яка є *представником влади, або повторно, або організованою групою, або з використанням засобів масової інформації* (ч. 3 ст. 109);

2) публічних закликів чи розповсюдження матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, установленого Конституцією України, *вчинених особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднаних з розпалюванням національної чи релігійної ворожнечі* (ч. 2 ст. 110);

3) умисних дій, спрямованих на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образи почуттів громадян у зв'язку з їхніми релігійними переконаннями, *поєднаних з обманом чи погрозами, а також вчинених службовою особою* (ч. 2 ст. 161);

4) публічних закликів до здійснення терористичного акту, *вчинених з використанням засобів масової інформації* (ст. 258-2);

5) публічних закликів до *геноциду* (ч. 2 ст. 442).

Необхідно звернути увагу й на те, що некваліфіковані види незаконних дій з порнографічними предметами (ч. 1 ст. 301, $I_{кзосн} = 25{,}51$) та з творами, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 1 ст. 300, $I_{кзосн} = 25{,}74$), розглядаються як такі, що за рівнем суспільної небезпечності є близькими до перешкоджання законній професійній діяльності журналістів (ч. 1 ст. 171, $I_{кзосн} = 20{,}96$) та закликів до вчинення дій, що загрожують громадському порядку (ст. 295, $I_{кзосн} = 20{,}96$).

Отже, дослідження кримінально-правових засобів забезпечення формування інформаційного ресурсу методом контекстної законодавчої оцінки суспільної небезпечності діяння дозволило встановити, що в цілому система кримінально-правових засобів є обґрунтованою, однак спостерігається певне завищення суворості санкцій за окремі дії з порнографічними предметами.

Разом із тим, очевидним є і те, що наявні в КК засоби протидії посяганням у сфері формування інформаційного ресурсу не відповідають усій сукупності встановлених соціальних потреб у правовій охороні в цій сфері. Поза увагою КК залишаються такі небезпечні тенденції, як комерціалізація інформаційного простору, небезпека втрати навичок роботи з інформацією, загрози формування надпотужних баз персональних даних тощо. Докладніше розглянемо перелічені небезпеки та можливості використання кримінально-правових засобів для протидії їм.

Небезпечність порушень у сфері формування інформаційного ресурсу є багатоплановою та складною за змістом і структурою чинників. Окреслити характер суспільно небезпечних наслідків порушень інформаційної безпеки в досліджуваній сфері можливо шляхом аналізу загроз, передбачених Доктриною інформаційної безпеки України (додаток 1). Так, у зовнішньополітичній сфері до суспільно небезпечних наслідків посягань у сфері формування інформаційного ресурсу слід відносити: шкоду національним інтересам України, заподіяну розповсюдженням у світовому інформаційному просторі викривленої, недостовірної й упередженої інформації та змінами в національній суспільній свідомості, зумовленими зовнішніми негативними інформаційними впливами через засоби масової інформації, а також мережу Інтернет. Небезпеку для внутрішньополітичної сфери становлять маніпуляції із суспільною й індивідуальною свідомістю та прояви обмеження свободи слова. У воєнній сфері суспільно небезпечні наслідки порушень у сфері формування інформаційного ресурсу можуть виявлятися в послабленні готовності населення України,

у тому числі особового складу військових формувань, до оборони держави, погіршенні іміджу військової служби. Державній безпеці порушення у сфері формування інформаційного ресурсу, відповідно до Доктрини інформаційної безпеки України, загрожують підривом конституційного ладу, суверенітету, територіальної цілісності та недоторканності кордонів України, а також посиленням сепаратних настроїв у суспільстві. Небезпека посягань, пов'язаних із формуванням інформаційного ресурсу, полягає в поширенні невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської та національної гідності; витісненні з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля.

Дані соціологів, результати наукових досліджень свідчать про те, що деякі з перелічених теоретично можливих загроз і небезпек вже стають фактичними характеристиками національного суспільного буття. Однак перед тим, як розглянути, проаналізуємо соціально-економічні умови процесів формування інформаційного ресурсу, що дозволить з'ясувати природу суспільно небезпечних наслідків досліджуваних посягань на інформаційну безпеку.

Ключовою ознакою сучасних процесів формування інформаційного ресурсу є *комерціалізація інформаційного простору*. Починаючи з другої половини 70-х років частка промислового виробництва як в обсязі національного продукту, так і в пропорції зайнятості стала помітно зменшуватися. Складаючи 1975 року в США 33,2%, у Великобританії – 28,4%, у Німеччині – 38% і у Франції – 30,2%, вона вже на початку 90-х років коливалася в США між 22,7 і 21,3% та близько 20% становила в країнах ЄС (від 15% у Греції до 30% у ФРН). При цьому характерно, що відносне зниження частки оброблювальних галузей у валовому продукті, не занадто значне, супроводжувалося різким падінням частки зайнятого у них населення (між 1980 і 1994 рр. зайнятість в оброблювальній промисловості США впала більш ніж на 11%, досягнувши 18% працездатного населення, у країнах Європейського союзу вона залишалася дещо вищою – близько 24%). Водночас спостерігається зростання зайнятості в інформаційному секторі – з 30,6% в 1950 р. до 48,3% у 1991, а її відношення до зайнятості в промисловому виробництві – з 0,44 до 0,93 [112, с. 9]. За даними західних дослідників, тенденція "дрейфу" робочої сили триватиме, усе більше людей працюватиме в комунікаційних секторах економіки [94, с. 165, 179].

Діяльність у сфері надання інформації розглядається сьогодні не інакше як господарська, підприємницька. При цьому вважається, що ринок засобів масової інформації забезпечує неупереджений, невидимий механізм вільного обміну ідеями в суспільстві. Ринкова конкуренція тут розуміється як свобода від втручання держави і, відповідно, як спосіб забезпечення прав індивідів на вільний обмін інформацією без втручання ззовні. Прибічники виключно ринкових механізмів розглядають функцію масової комунікації як двоєдиний процес. Суть його полягає, з одного боку, в наданні програм аудиторії, а з іншого – наданні аудиторії рекламодавцям. Наявність комерційних засобів масової комунікації ґарантує наявність конкуренції, яка створює умови для вільного й самостійного вибору окремим споживачем інформації, що цікавить його, стають можливими оперативні технічні інновації, ціни на інформаційні послуги при цьому виявляються низькими, а їх якість – високою. Конкуренція надає кожному підприємцеві, у якого є що сказати людям, можливість виходу на ринок інформації. Тим самим комерційні засоби задовольняють потреби як широкої більшості, так і окремих частин аудиторії [245].

Така модель, цілком послідовна й обґрунтована, тим не менше не спрацьовує. Фактичні процеси у сфері формування інформаційного поля характеризуються принципово іншими тенденціями. Можна сказати, що проблеми, які виникають, є подібними до питань класичної економічної теорії: ефективна саморегуляція формування інформаційного поля під впливом попиту на інформацію неможлива, необхідним є державне ре-

ґулювання процесу, що, відповідно, породжує питання методів і меж державного впливу.

Проблему, що унеможливлює ефективне саморегулювання інформаційної сфери, можна сформулювати таким чином: через капіталізацію діяльності суб'єктів масової комунікації суспільний інформаційний ресурс зазвичай формується за рахунок тих відомостей, які потенційно можуть збільшити коло споживачів конкретних засобів масової комунікації. Так, зазначається, що концепція "свободи друку" служить значною мірою інтересам рекламодавців і великого бізнесу, тому для сучасної сфери масової інформації характерною є тенденція монополізації, і якщо у недемократичних режимах свобода друку обмежувалася державою, то тепер тенденції до монополізації серйозно обмежують свободу вибору інформації [245].

Наслідком такого обмеження виступають істотні негативні зміни в суспільній свідомості. По-перше, кількість культурно-пізнавальних передач зменшується. По-друге, вони стають малозмістовними. У більшості з них ігноруються норми моралі та права людини. Ця тенденція поширюється в усіх сферах мовлення, навіть у новинах та аналітичних програмах [300]. Російські дослідники В.І. Данілов-Данільян та І.Є. Рейф зазначають, що, забезпечивши більшості населення високий рівень добробуту, розвинена ринкова економіка майже нічого не зробила для підвищення культурного рівня рядового американця або європейця. Навпаки, вигідним виявилося "промивання мізків" за допомогою реклами й інших піартехнологій, щоб спростити його духовні потреби та понизити культуру до субкультури з її кінобойовиками, любовно-еротичними, детективними романами, попсовою музикою, усілякими "диснейлендами", фітнес-клубами, комерційним спортом, казино тощо. "Адже стотисячний стадіон дає набагато більший дохід, ніж філармонічний зал, концерти в якому потребують ще і спонсорської підтримки… Масова субкультура, що затопляє світ, веде до ерозії національних традицій і освячених віками моральних цінностей" [80]. Відома "свобода вибору", якою так пишаються розвинені країни, нерідко перетворюється на су-

купність потреб, нав'язаних масовою комунікацією. При цьому, як пише російський соціолог А.Б. Вебер, корпорації "примушують людей "хотіти" значно більше, ніж треба для задоволення дійсних потреб. Ринок перетворюється на механізм, що створює і формує попит, включаючи попит на те, що виходить за рамки розумних людських потреб" [52, наводиться за 80]. Висновки дослідників можна повною мірою застосувати для характеристики українського інформаційного поля та соціальних наслідків його впливу, оскільки, на думку експертів, темпи й обсяги капіталізації національного інформаційного ресурсу виявилися дуже значними в порівнянні з країнами сталої демократії, і це створило серйозні загрози нашій інформаційній сфері. "Коли ж починаєш слухати наш, український, ефір, то нерідко виникає враження, начебто все організовано проти цієї нації, проти її духовності, культури... Навіть спортивні передачі містять рекламу алкоголю..." [240].

Отже, комерційна основа засобів масової комунікації досить чітко диктує характер відомостей, що надаються (тільки те, що може зацікавити широку аудиторію). Це, призводить до небезпечних соціальних наслідків. Механізм їх формування можна охарактеризувати на основі дослідження П. Бергера і Т. Лукмана "Соціальне конструювання реальності: трактат із соціології знання" [22]. Реальність розуміється ними як "якість, властива феноменам, мати буття, незалежно від нашої волі і бажання". Знання визначає "упевненість у тому, що феномени є реальними і мають специфічні характеристики" [22, с. 9]. Повсякденне життя є "реальністю, що інтерпретується людьми та має для них суб'єктивну значущість як цілісний світ" [22, с. 38]. Це світ, який створюється в їх думках і діях, вони переживають як реальний. Дослідники обґрунтовують, що в сучасному суспільстві, на відміну від традиційного, саме ЗМІ "генерують соціальну пам'ять" і задають соціальне значення подіям, що відбуваються [295]. Назвемо "реальність повсякденного життя", сформовану на основі відомостей із засобів масової інформації, "новою реальністю". Як приклад такої реальності наведемо цитату з оповідання Дж. Д. Селінджера: "Елейн прожила ли-

пень і серпень... у кіно-радіо світі, заселеному виключно зірками газетного репортажу, блискучими молодими редакторами, молодими нейрохірургами, безстрашними молодими детективами, які незрівнянно б'ються, оперують або вистежують, якщо тільки їх не відводить у бік їх власна невикорінна чарівливість. У світі Елейн усі прекрасно причісувалися самі або довіряли своє волосся дорогим перукарям. Усі чоловіки говорили глибокими, добре поставленими голосами" [327].

"Новій реальності", світу, який створюється в думках та діях і який людина переживає як реальний, відповідає "нове знання". Наприклад, працівник правоохоронних органів – це або надсильна, така, що досконало володіє прийомами рукопашного бою, влучно стріляє й ніколи не помиляється, зазвичай весела молода людина, або зрадник, "поганий поліцейський", який є слабким, погано стріляє, незграбний, з верткими очима і, як правило, зловживає алкоголем, наркотиками, азартними іграми тощо. Інших образів у "новій реальності" просто не може бути, оскільки вони непривабливі, не забезпечують засобам масової інформації зростання аудиторії, а отже, не з'являються на екранах телевізорів або сторінках газет.

Урешті-решт, людина, опинившись в оточенні сенсацій (а воно так і є, бо в умовах комерціалізації засобів масової інформації альтернативи немає), втрачає можливість об'єктивного сприйняття дійсності. Подібно до навколишнього природного середовища, яке людина освоює й підпорядковує собі за допомогою досягнень індустріальної технології, природа людського спілкування та пізнання світу виявилася під таким самим впливом, але з боку технологій інформаційної доби. Наслідки спроб підкорення людиною навколишнього природного середовища сьогодні є очевидними. "Забруднення" інформаційного оточення, якщо врахувати, що інформаційні зв'язки опосередковують взаємини людей між собою, природою і технікою, призводить насамперед до соціальних дисфункцій, зумовлених неадекватним сприйняттям дійсності.

Так, наявність значного суспільного інтересу до кримінальних подій спричинила появу самостійного й вагомого сег-

менту інформаційного поля та, урешті-решт, перетворила його на криміногенний чинник. В.В. Коваленко зазначає: "Засоби масової комунікації … все частіше вводять свого споживача в стан, де діють механізми і неписані закони особистого збагачення, відчуженості, байдужості до суспільства, усе більше розбещують його безсоромністю і насильством, пропагандою наркотиків, алкоголю, злочинності і безкарності" [130, с. 84]. Окремі експерти зауважують, що пропаганда насильства й екстремізму в українському сегменті Інтернету набуває загрозливих масштабів. У ході спеціальних досліджень у мережі було виявлено: численні коментарі новин та інших матеріалів сайтів з проявами образи національної гідності або релігійних переконань; провокативні оголошення, наприклад про винагороду до 5 тисяч доларів США за вибиті зуби львівських націоналістів; зняте на мобільні телефони відео, де неповнолітні знущаються зі своїх слабших однолітків або катують бездомних; інструкції з "вуличного екстремізму" тощо [48]. О. Бугера обґрунтовує, що одним із чинників формування мотивації протиправної поведінки неповнолітніх є "деструктивний вплив ЗМІ, у яких нерідко пропагуються стандарти поведінки, несумісні із ціннісними орієнтаціями нашого суспільства, зокрема культ сили та жорстокості" [34, с. 70]. Ці висновки підтверджуються результатами соціологічних досліджень. Так, установлено, що 37,3% молоді готові вчиняти протиправні дії, наслідуючи героїв телевізійних програм [380].

Також дослідники соціальних наслідків у сфері формування національного інформаційного ресурсу звертають увагу на появу нового виду шкідливих залежностей, так званих нехімічних залежностей (адикцій) – залежностей від Інтернету, комп'ютера, телебачення, мобільного телефону, коли людина, віддаючись своїй хворобливій прихильності, не лише втрачає сім'ю, друзів, роботу, але й забуває про їжу та сон. Однією з найпоширеніших адикцій є ігроманія, яка може виявлятися в імпульсивності, проблемах зі спілкуванням, появі невмотивованого почуття радості, ейфорії, нездатності контролювати час, дратівливості, спалахах гніву або стані пригніченості, депресії.

Саме такий розлад було визнано Всесвітньою організацією здоров'я хворобою XXI століття. Про актуальність цієї проблеми, реальну небезпечність адикцій для українського суспільства свідчать результати соціологічного опитування батьків підлітків (жовтень 2006 року). З'ясувалося, що 14% дітей узагалі не займалися спортом (окрім уроків фізкультури), 34% – не відвідують гуртки. Разом із тим, 55% батьків відповіли, що їх діти більшу частину вільного часу присвячують перегляду телевізійних передач і фільмів, а кожний третій підліток – комп'ютерним іграм. Ускладнює ситуацію і недостатність нормативної бази у сфері категоризації інформаційних продуктів, зокрема комп'ютерних ігор та інтернет-контенту. Наприклад, один із прихильників комп'ютерної гри Manhunt Чо Син Хі у квітні 2007 року вбив 32 людини в Політехнічному університеті Вірджинії. У багатьох країнах цю гру заборонили, у Британії її двічі відмовилися ліцензувати, але в Україні вона продається легально [96]. У цьому контексті не можна не звернути уваги й на те, що діти та підлітки – це одна з найбільш динамічно зростаючих груп користувачів Інернету. Так, за результатами моніторингових досліджень Eurobarometer, які проводяться у 27 країнах-членах ЄС, 75% дітей у віці від шести до сімнадцяти років активно користуються Інтернетом [294]. І хоча українські показники значно скромніші, вектор розвитку національної інтернет-аудиторії та динаміка цього процесу ідентичні європейським, а отже, додають актуальності означеній проблемі як національній.

Крім підвищення рівня агресивності негативний вплив інформаційного поля на свідомість дітей і підлітків може виявлятися в певних психологічних розладах. Співробітники лабораторії психології дошкільника Інституту психології АПН України переконалися в тому, що чим далі дитина перебуває від мегаполісів (далі від щільного інформаційного потоку), тим більш захищеною вона себе почуває. Про це свідчить порівняння результатів дослідження рівня емоційного благополуччя, упевненості в собі, відкритості до світу, допитливості, отри-

маних під час роботи з дошкільнятами Києва, Житомира, Житомирської області [57].

Специфіка українського інформаційного поля полягає ще й у тому, що основне його навантаження продукується закордонними виробниками, які, "користуючись нашим безпомічно-ліберальним законодавством, вільно й безкарно господарюють у нашому інформаційному домі, поетапно зміцнюючи свої позиції" [240]. Такий стан речей поглиблює загрози, пов'язані з втратою національної ідентичності.

Певні небезпеки комерціалізація інформаційного простору створює для демократичного розвитку. Американські дослідники П. Лазерсфельд і Р. Мертон уважають, що сучасні ЗМІ знижують рівень активної участі в громадському житті та перетворюють людей на пасивних споживачів новин. Оскільки мас-медіа підтримуються великим бізнесом, пов'язаним з відповідною соціально-економічною системою, вони, зрозуміло, роблять свій внесок у збереження цієї системи. Підтримуючи статус-кво, ці засоби виявляються нездатними ставити під сумнів структуру суспільства, порушувати гострі та важливі соціальні проблеми. Навпаки, комерціалізовані засоби масової інформації справляють на суспільство "цементуючий вплив", оскільки пасивність ґарантує збереження статус-кво [273]. Зрозуміло, що такий стан речей створює достатньо реальні небезпеки на шляху демократичного розвитку.

На окрему увагу заслуговують й такі небезпечні наслідки комерційно орієнтованого формування інформаційного ресурсу, як зниження інтелектуального рівня та втрата навичок роботи з інформацією. Механізм виникнення цих соціальних тенденцій пов'язаний з тим, що комерціалізованість суспільної комунікації практично виключає з неї складну інформацію, тобто таку, усвідомлення якої потребує певних інтелектуальних зусиль. Оскільки зазначені відомості не забезпечують аудиторії, то інформація для спрощення її сприйняття подається переважно поверхово та з яскравою візуалізацією. Ґенералізація такого підходу призводить до розвитку неґативних

соціальних тенденцій. Так, результати національного не залежного тестування з математики 2011 року показали, що 30% випускників шкіл не виконали завдання з теореми Піфагора [239]. Схожі проблеми зафіксовано і в інших країнах. Наприклад, видання Evening Standard повідомляє, що мільйон жителів Лондона, за даними дослідження Національного управлінням у справах грамотності (National Literacy Trust), ледве вміють читати, а кожна четверта дитина в британській столиці, закінчуючи початкову школу, залишається безграмотною. До 40% компаній у Лондоні говорять про те, що їх співробітники насилу пишуть і читають. Загалом по одній тільки Англії рівень грамотності 5% дорослого населення залишається на рівні 7-річної дитини. Одне з опитувань показало, що кожна третя дитина в Лондоні взагалі не має жодної книги, при тому, що у 85% дітей є комп'ютерна приставка. Кожен п'ятий учень страждає на якесь порушення, пов'язане з процесом освіти, наприклад на дислексію. Серед випускників лондонських шкіл кожен четвертий читає і пише важко, кожен п'ятий не вміє читати взагалі [44]. За повідомленням агенції Bloomberg, згідно з результатами дослідження Міністерства освіти США більше половини учнів початкової та середньої шкіл не змогли показати свою країну на карті. А серед учнів 4-х класів лише третина дітей розмістила правильно в порядку зменшення площі Північну Америку, США, Каліфорнію та Лос-Анджелес [272]. Звернімо увагу й на той факт, що зазначені тенденції спостерігаються в країнах, які належать до світових лідерів з питань інформатизації.

Урешті-решт, можна погодитися з О. Кендюховим, який у результаті дослідження змін, що відбулися в національній свідомості в контексті формування суспільства споживання, доходить невтішного висновку: "З високою часткою ймовірності можна стверджувати, що зміни, які протягом останнього десятиліття відбуваються в суспільній свідомості, катастрофічні для України й приведуть молоду незалежну Українську державу до національного краху й фактичної втрати своєї неза-

лежності". Дослідник обґрунтовує, що сучасне національне інформаційне середовище, орієнтоване насамперед на культивацію "філософії споживання", зумовлює такі негативні соціальні трансформації: "духовне й інтелектуальне виродження суспільства, фактично добровільна відмова від таких громадянських свобод, як свобода вибору, свобода совісті, свобода слова і, зрештою, формування імітаційної форми демократії"; "імітація правильності всіх форм суспільного життя: науки, освіти, охорони здоров'я, правоохоронної та судової систем, армії тощо"; "гроші сприймаються як мірило інтелекту, правосуддя, великодушності та благородства"; "втрата здатності українського суспільства до критичного мислення; загальнонаціональне подурнішання"; "духовна деградація суспільства" [124].

Зафіксувавши, настільки тривожними є соціальні тенденції, розглянемо, які засоби можуть бути використані для їх попередження та мінімізації наслідків. Ураховуючи предмет дослідження, головну увагу приділимо можливостям використання норм законодавства про кримінальну відповідальність.

Найбільш поширеним та, можливо, історично першим засобом протидії суспільно небезпечним наслідкам порушень у сфері формування інформаційного ресурсу є контроль за змістом повідомлень та обмеження доступу до них. Саме до таких засобів слід відносити розглянуті на початку підглави норми чинного КК (чч. 2, 3 ст. 109, ст. 110, ст. 161, ст. 171, ст. 258-2, ст. 295, ст. 300, ст. 301, ч. 2 ст. 442). Проте ці кримінально-правові заборони не можна розглядати як цілісну систему, вони являють собою законодавчу реакцію на найбільш небезпекні прояви порушень формування інформаційного ресурсу, що відносяться до різноманітних сфер соціального буття: національної безпеки, протидії расовій неприязні та ксенофобії, громадської безпеки, суспільної моральності, безпеки людства тощо. Можливо, установлені суспільно небезпечні наслідки сучасних процесів формування інформаційного поля потребують кримінально-правових заборон більш широкого спектру дії? Таких, які б забезпечували протидію включенню будь-

якого негативного контенту до суспільного інформаційного ресурсу, виключали б можливість маніпулювання суспільною свідомістю? Так, О. Бугера звертає увагу на необхідність суворого дотримання вимог обмеження глядацької аудиторії та індексації повідомлень ЗМІ залежно від змісту [34, с. 71]. З метою запобігання негативному впливу змісту, наприклад, інтернет-ресурсів пропонується ведення "білих" та "чорних" списків. Перші містять рекомендовані або перевірені користувачами джерела, інші – джерела, помічені в поширенні небажаної інформації [380]. Н.А. Савінова пропонує передбачити кримінальну відповідальність за такі посягання, як "умисні впливи на свідомість", "необережні впливи на свідомість", "умисне поширення хибної соціально значущої інформації", "поширення принизливої для України медіа-продукції", "використання прихованих засобів впливу на свідомість у засобах масової інформації" [308, с. 252 – 299].Отже, можливо, КК необхідно доповнити нормами про відповідальність за недотримання правил індексації контенту, або про відповідальність провайдерів телекомунікаційних послуг за трансляцію суспільно шкідливого контенту, або про відповідальність випускаючих редакторів ЗМІ за поширення відомостей, які спричиняють настання суспільно небезпечних наслідків?

Відповідь на поставлені питання є негативною. По-перше, розширення видів інформації, розповсюдження якої підпадає під дію законодавства про кримінальну відповідальність, входить в очевидну суперечність з однією з основних тенденцій соціальної політики нашого суспільства – демократизацією взагалі та забезпеченням свободи слова зокрема. Тому подібне законодавче рішення не відповідало б принципу кримінально-політичної адекватності криміналізації.

По-друге, посилення державного контролю за діяльністю засобів масової інформації шляхом включення до його механізму додаткових кримінально-правових засобів потенційно небезпечне згортанням процесів демократизації через надто широкі правові можливості держави та втрату громадянським суспільством важливих інструментів впливу на владу. Отже, роз-

ширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційної безпеки слід визнавати й таким, що не відповідає принципу спів розмірності позитивних і негативних наслідків криміналізації.

По-третє, спроба сформулювати подібні новели до Кримінального кодексу приведе до цілком очікуваної проблеми. Як видається, принципово неможливо сформулювати чітке та операціональне загальне визначення для позначення тих відомостей, включення яких до суспільного інформаційного поля слід уважати суспільно небезпечним. Вельми проблематичною буде й спроба чіткого, а саме таке є необхідним для кримінально-правової норми, визначення суспільно небезпечних наслідків. Така ситуація з необхідністю приведе до формулювання кримінально-правової заборони на основі оцінних понять, що у свою чергу створить необґрунтований ризик можливості кримінально-правової оцінки діянь, які не є суспільно небезпечними. З подібними проблемами вітчизняна практика постійно стикається під час застосування норм про відповідальність за поширення порнографії (ст. 301) та пропаганду культу насильства та жорстокості (ст. 300). Однак якщо в означених випадках необхідність кримінально-правового впливу є очевидною, оскільки зумовлена виключною небезпечністю відповідної інформації, то використання подібного рішення для інших видів інформації є дуже спірним.

По-четверте. Описана складність механізму формування суспільно небезпечних наслідків, що настають через надмірну комерціалізацію інформаційного простору, порушує проблему процесуальної здійсненності переслідування. Питання про можливість доведення наявними процесуальними засобами причинного зв’язку між поширенням певної інформації та настанням відповідних суспільно небезпечних наслідків очевидно є риторичним. Таким чином, через невідповідність принципу процесуальної здійсненності переслідування обговорювані гіпотетичні доповнення, скоріше за все, перетворилися б на декларативні норми.

Нарешті, по-п'яте. Поширення глобальних інформаційних технологій (Інтернет, мережі супутникового мовлення) взагалі робить все менш ефективними методи, що ґрунтуються на обмеженні або забороні поширення певної інформації. Наприклад, тотальний моніторинг Інтернету, на думку значної частини західних фахівців з питань інформаційної безпеки, не може допомогти в боротьбі з екстремізмом навіть суто теоретично. Щільність сучасних інформаційних потоків настільки велика, що навіть для вибіркової вчасної перевірки окремих інформаційних джерел знадобиться така кількість фахівців, яка в декілька разів перевищує економічно обґрунтовану чисельність всіх правоохоронних органів держави [262]. Варто погодитися і з О. Зернецькою, яка звертає увагу на транснаціональність проблем формування інформаційного ресурсу з використанням сучасних технологій медіатизації: "Вертикальна регуляторна схема, що спрацьовує відносно мінімізації загроз, пов'язаних з поширенням шкідливого контенту в традиційних мас-медіа, не діє в умовах інтерактивності й глобальності" [109]. Більше того, тенденції сучасних процесів інформатизації дозволяють стверджувати, що в більшості випадків спроби обмежити поширення певних відомостей є вкрай неефективними. Як правило, наслідком заборони або обмеження роботи певного ресурсу інформації стає сплеск зацікавленості щодо змісту відомостей, доступ до яких обмежено. Зростання соціального попиту на таку інформацію веде до збільшення ресурсів, які її надають, а отже, і кола суб'єктів, що отримали доступ до інформації. Таким чином, спроба обмежити доступ до певної інформації врешті-решт призводить до того, кількість осіб, які з нею ознайомлюються, зростає в геометричній прогресії. Ще раз зауважимо, що подібні ситуації є непоодинокими й навіть отримали спеціальний термін – "ефект Стрейзанд" [415, Yiannopoulos, M. What is 'The Streisand Effect'? [Electronic resourse] / Yiannopoulos M. // The Daly Telegraph site. – Mode of access: http://blogs.telegraph.co.uk/technology/miloyiannopoulos/8248311/What_is_The_Streisand_Effect/]. Приклад дії цього ефекту можна було спостерігати й у національному сегменті мережі Ін-

тернет у лютому 2012 року. Після того як ухвалою Деснянського районного суду м. Києва від 10.02.2012 р. в цивільній справі №2-1346/12 було тимчасово зупинено надання послуг хостингу для веб-сайту "Дорожній контроль" (http://roadcontrol.org.ua), відеозапис, який був підставою обмеження роботи сайту, був наданий для доступу на інших сайтах, а кількість його переглядів збільшилася в рази [336]. Отже, доповнення КК новими нормами про відповідальність у сфері формування інформаційного ресурсу є недоцільним і через їх прогнозовану неефективність.

Саме через неефективність традиційних засобів протидії негативним інформаційним впливам фахівці зауважують, що усвідомлювати серйозність проблем, які створює сучасне інформаційне поле, зовсім не означає тільки карати, забороняти, фільтрувати, закривати, конфісковувати. Особливо в українському контексті, у якому, як підкреслює глава Всеукраїнської мережі боротьби з комерційною експлуатацією дітей К. Левченко, ще тільки належить розібратися, за що, яка і на кого має покладатися відповідальність. У зв'язку з цим звертається увага на такі заходи попередження негативного інформаційного впливу, як виховання поваги до прав інших людей та уміння відстоювати свої власні, батьківський контроль, обмеження віртуальних соціальних контактів, розвиток навичок критичного сприйняття інформації, що надходить з медійного простору, тощо [294]. Також наголошується на необхідності організації дозвілля для молоді, зростання значимості родини. Наприклад, у ході одного з досліджень більше третини українських підлітків відповіли, що їх батьки знають небагато або нічого про те, хто їх друзі, де вони бувають після школи та чим займаються у вільний час. Саме відсутність достатньої уваги з боку батьків є однією з причин занурення дитини у віртуальний світ [96]. До заходів протидії нехімічним залежностям фахівці зараховують: проведення інформаційних кампаній; створення та функціонування мережі консультаційних пунктів і центрів реабілітації хворих на нехімічні залежності; підготовку відповідних фахівців та підвищення кваліфікації психоло-

гів, соціальних працівників, педагогів; роботу дитячих і молодіжних громадських організацій [96].

Отже, маємо констатувати: 1) кількісні та якісні показники формування національного інформаційного ресурсу свідчать про значний потенціал можливих суспільно небезпечних наслідків; 2) чинне законодавство про кримінальну відповідальність забезпечує фрагментарний захист суспільних відносин від посягань у сфері формування інформаційного ресурсу; 3) разом із тим, розширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення "суспільно небезпечної інформації", є недоцільними через прогнозовану неефективність і декларативність таких норм, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації.

Таким чином, Кримінальний кодекс України не потребує змістових змін і нових заборон щодо формування інформаційного ресурсу. Зайвим і, з огляду на наявні тенденції формування інформаційного ресурсу, очевидно неефективним буде використання засобів кримінальної юстиції для попередження розвитку встановлених негативних соціальних тенденцій. Разом із цим, слід визнати, що з розвитком технологій медіатизації, психології та соціології формулювання подібних норм, можливо, стане дійсністю. Тут слід погодитися з Н.А. Савіновою, яка зазначає, що одним із напрямів кримінально-правового забезпечення розвитку інформаційного суспільства в Україні має стати запровадження заходів кримінально-правового прогнозування, зокрема в частині визначення критеріїв криміналізації посягань у сфері формування інформаційного ресурсу [308, с. 306].

Порушені в цій підглаві питання вимагають формулювання певного доповнення до аргументованих раніше положень щодо меж кримінально-правової охорони інформаційної безпеки. У попередніх главах було послідовно доведено тезу про те, що доцільність застосування методів кримінальної юстиції

для охорони інформаційної безпеки перебуває в прямій залежності від інтенсивності наслідків, які настають у результаті відповідних посягань. При цьому такі наслідки являють собою порушення в різноманітних сферах суспільного буття, у межах яких використовується інформація, що є предметом посягання. Знищення або перекручення інформації, обмеження доступу до неї небезпечні не самі по собі, а лише в контексті тієї діяльності, для здійснення якої використовується певна інформація. Однак з урахуванням викладеного в цій главі маємо зазначити, що межі кримінально-правової охорони інформаційної безпеки визначаються не лише інтенсивністю таких наслідків, але й узагалі доцільністю використання норм про кримінальну відповідальність.

6.2. Можливі напрями подальшого наукового пошуку з питань кримінально-правового забезпечення формування інформаційного ресурсу

Проведене дослідження дозволяє стверджувати, що ін.-формаційна безпека – це поняття з досить широким обсягом. Як інформаційна діяльність пронизує практично всі сфери суспільного буття, так і зміст інформаційної безпеки визначається, урешті-решт, сукупністю різноманітних інформаційних потреб, що виникають у відповідних сферах діяльності людини. Зазначена специфіка зумовлює й те, що певні аспекти кримінально-правової охорони інформаційної безпеки можуть, а в умовах становлення інформаційного суспільства і повинні стати предметом суміжних досліджень. У зв'язку з цим видається доцільним окреслити можливі напрями подальшого наукового пошуку у цій сфері.

Самостійною проблемою сучасної кримінально-правової науки є охорона інтелектуальної власності. Як зазначалося в першій главі, для сучасного інформаційного суспільства принципово важливим аспектом розвитку та стабільності є

конкурентоспроможність національної продукції, яка досягається шляхом широкого використання інноваційних рішень. Цілком зрозуміло, що інноваційність розвитку потребує відповідних умов. Головною з них є ефективний механізм захисту прав інтелектуальної власності. Саме ці міркування й обґрунтовують необхідність розгляду кримінально-правових засобів забезпечення прав інтелектуальної власності в контексті проблематики формування інформаційного ресурсу як складової інформаційної безпеки. Зазначене підтверджується й у Доктрині інформаційної безпеки України, де формулюються такі загрози: економічна сфера – відставання вітчизняних наукомістких і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій та використання неліцензованого й несертифікованого програмного забезпечення, засобів і комплексів обробки інформації; науково-технологічна сфера – зниження наукового потенціалу в галузі інформатизації та зв'язку, низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку, відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності. Про актуальність розгляданої проблеми свідчать і ґрунтовні дослідження вітчизняних науковців [376, 76, 252].

Однак найбільш вагомим аргументом на користь подальшого наукового пошуку є фактичний стан речей у сфері охорони інтелектуальної власності в Україні. Ураховуючи, що докладний аналіз зазначеної проблеми потребує самостійного дослідження, розглянемо один із її сегментів – так зване "комп'ютерне піратство", порушення авторського права на програмне забезпечення. Цей вид протиправних посягань є відносно новим та динамічно розвивається, тому виступає достатньо задовільним індикатором для отримання уявлення щодо загального стану проблеми.

Отже, за даними Асоціації виробників програмного забезпечення (BSA), Україна посідає сьоме місце у світі серед країн із найвищим рівнем комп'ютерного піратства. За оцінкою фахівців, комерційна вартість неліцензійного програмного забез-

печення, установленого на персональні комп'ютери в нашій країні, сягає 571 млн. дол. США [145]. Вельми інформативною є динаміка цього явища. Як повідомляє International Data Corporation, серйозні кроки у боротьбі з піратством Україна робила лише після того, як 2001 року потрапила до списку "Special 301", який складає Торговельний представник США, і була змушена сплачувати істотні штрафні санкції – 75 млн дол. щорічно. Рівень "піратського" програмного забезпечення на той час був понад 90%. Коли ж рейтинг України в цьому списку підвищився, 2005 року обтяжливі штрафні санкції було знято. Із цього часу рівень контрафактного програмного забезпечення залишається приблизно однаковим (2005 р. – 85%, 2006 р. – 84%, 2007 р. – 83%, 2008 р. – 82%, 2009 р. – 84%). Коментуючи ці показники, юридичний представник BSA в Україні В. Шаповал зазначив, що останніми роками в нашій державі настала "болотяна стабільність", коли ситуація суттєво ані погіршується, ані поліпшується: "Комп'ютерів і ноутбуків з року в рік продається щораз більше, а ліцензійного програмного забезпечення у кращому разі продається стільки ж, скільки й продавалося… Проблема піратства в Україні знову постає дуже гостро" [257]. Керівник департаменту із захисту прав інтелектуальної власності "Майкрософт Україна" Ю. Омельченко звертає увагу на істотні економічні втрати від "комп'ютерного піратства". Він зауважує, що зниження навіть на 10% показника незаконного використання програмного забезпечення за кілька років дало б низку позитивних змін в економіці країни. "З'явилося б 2600 додаткових високооплачуваних робочих місць для українських фахівців. Регіональні та місцеві бюджети отримали б додаткових 69 млн. дол. податкових надходжень, а обіг ІТ-сектору збільшився б на 941 млн. дол. Поки що ці суми працюють на тіньову економіку" [257].

Урешті-решт негативні наслідки описаного стану речей можна сформулювати таким чином:

- нездатність України виробляти конкурентоспроможне програмне забезпечення, що призведе до залежності від іноземних виробників;

- залежність істотного сеґменту національної економіки від закордонних суб'єктів господарської діяльності через цивільно-правові зобов'язання, що виникають унаслідок незаконного використання об'єктів інтелектуальної власності;

- істотні економічні втрати держави.

Зрозуміло, що поширення незаконного використання програмного забезпечення та перелічені неґативні наслідки вимагають застосування також і кримінально-правових засобів протидії. Сьогодні вони використовуються вельми активно. Однак ефективність кримінальної юстиції в цій сфері, як свідчать наведені раніше статистичні дані, є недостатньою. Однією з причин цього є використовуваний порядок обчислення матеріальної шкоди від порушення авторського права. Науковці доводять, що матеріальною шкодою від порушення авторського права слід уважати вартість конкретного майнового права, що належить суб'єктові авторського права і суміжних прав, порушеного винною особою [76, с. 140]. Ця матеріальна шкода за своїм змістом є свого роду упущеною вигодою та полягає в сумі грошових коштів, які б мав одержати суб'єкт авторського права і суміжних прав за продаж (відчуження) належного йому того чи іншого майнового права [231]. У цивільно-правовому контексті ці висновки є послідовними, але їх беззастережне перенесення на сферу кримінальної юстиції, а особливо на сферу протидії "комп'ютерному піратству", призводить до вкрай неґативних наслідків. Проблема полягає в тому, що вартість легального програмного забезпечення є дуже високою, а отже, для настання кримінальної відповідальності достатньо, наприклад, незаконного використання одного або двох програмних продуктів. Разом із тим, цілком очевидно, що метою включення до складу злочину, передбаченого ч. 1 ст. 176, такої ознаки, як "значна шкода" було відмежування злочинних посягань від тих, які не є достатньо суспільно небезпечними. Однак через зазначене тлумачення змісту розгляданої шкоди чітке й прозоре відмежування на підставі цієї ознаки дійсно суспільно небезпечних посягань на авторські права розробників програмного забезпечення від посягань, які такими не є, практично не-

можливе. У свою чергу це призводить до падіння ефективності кримінально-правової протидії "комп'ютерному піратству", оскільки до сфери кримінальної юстиції потрапляють діяння, які не можна визнавати суспільно небезпечними. У подібних випадках застосування кримінального покарання не треба розглядати як ефективний засіб подолання "комп'ютерного піратства" в Україні. Означену тезу було підтверджено під час дослідження практики використання національного законодавства про кримінальну відповідальність за порушення авторського права на програмне забезпечення (додаток 5).

Крім того, що зазначений порядок обчислення шкоди не надає можливості чіткого відмежування суспільно небезпечних видів порушення авторського права на програмне забезпечення, доволі спірною видається і його справедливість. По-перше, зрозуміло, що відсутність або значне скорочення обсягів ринку неліцензійного програмного забезпечення не приведе до пропорційного збільшення легального ринку. Це зумовлено тим, що вартість легального програмного забезпечення в сотні разів перевищує вартість контрафактного. Тому якщо в певної особи відсутня можливість придбати дешеву контрафактну продукцію, це зовсім не означає, що вона купуватиме легальну. Наприклад, вироком Бахчисарайського районного суду Автономної Республіки Крим від 18 травня 2011 року в справі №1-204/2011 засуджено особу, яка за 25 гривень продала диск з програмним забезпеченням (6 примірників) компанії "Graphisoft R&D". У вироку зазначається: "З урахуванням того, що стала ринкова вартість 6 примірників комп'ютерних програм "Graphisoft" складає 204762 грн., підсудна своїми діями заподіяла автору комп'ютерних програм – компанії "Graphisoft R&D" – матеріальну шкоду на вказану суму" [183]. Риторичне питання: чи готова особа замість 25 гривень витратити на придбання програмного забезпечення 204 тисячі гривень? По-друге, несправедливо говорити, що особа, яка придбаває контрафактне програмне забезпечення, отримує ідентичну леґальній продукцію. Користувачі контрафактних програмних засобів, як правило, не мають доступу до мережевих сервісів

підтримки й оновлення забезпечення, виникають інші складнощі використання програми, зумовлені відсутністю можливості спілкування з розробником програмного забезпечення, яке доступне тільки леґальним користувачам. Крім цього, зазначений підхід до визначення шкоди від порушення авторського права на програмне забезпечення порушує й низку гіпотетичних питань. Наприклад, якщо один і той самий диск з контрафактним забезпеченням особа А. продала особі Б., через певний час особа Б. продала його особі В., а остання продала його Г., то яку шкоду заподіяно правовласнику?

Отже, сприйняття правозастосовувачем доволі спірного підходу до визначення матеріальної шкоди від порушення авторського права призводить до падіння ефективності кримінально-правової протидії у цій сфері. Однак на цьому не закінчуються неґативні соціальні наслідки такої практики. Так, в умовах, коли переважна більшість користувачів комп'ютерної техніки використовують неліцензійне програмне забезпечення, а закон не містить чіткої й прозорої відповіді на питання відмежування суспільно небезпечних порушень авторського права від тих, які такими не є, можна обґрунтовано прогнозувати зростання проявів корупції у відповідній сфері діяльності правоохоронних органів. Принагідно зауважимо, що, за результатами всеукраїнського дослідження, проведеного на початку 2011 року "Майкрософт Україна", державні установи країни: адміністрації, податкова, правоохоронні органи й інші – використовують понад 70 відсотків нелеґального програмного продукту "Майкрософт" [49].

Викликає занепокоєння і той факт, що серед досліджених судових рішень 33% (34 вироки) містять у резолютивній частині положення щодо зобов'язання обвинувачених відшкодувати матеріальні збитки. При цьому збитки обчислено в спосіб, що, як ми зазначали та продемонстрували, не може бути сприйнятий без заперечень. У зв'язку з цим дозволимо собі дещо ненаукове, однак достатньо інформативне порівняння, що випливає з аналізу дослідженої сукупності вироків: сума всіх підтверджених судами цивільно-правових зобов'язань засу-

джених осіб перед правовласниками (у переважній більшості американськими компаніями) у 4,75 разу перевищує сукупну суму штрафів, призначених дослідженою сукупністю вироків.

Останнє зауваження актуалізує питання прагматичності використання засобів кримінально-правової протидії не законному використанню програмного забезпечення. Розглянута сукупність вироків абсолютно чітко фіксує, що значна частина конкретних рішень пов'язана з похідними проявами цього явища, тому істотно на нього не впливає. Ідеться про вироки категорій "встановлення" та "використання". Дії, яким у цих вироках дається кримінально-правова оцінка, зумовлені функціонуванням ринку неліцензійного програмного забезпечення, тому протидія переважно їм навіть теоретично не зможе забезпечити бажаного соціального результату.

Проблема орієнтації кримінально-правового впливу полягає також у тому, що серед досліджених рішень відсутні відомості про засудження осіб, які вчиняють так званий "злам" програмного забезпечення. Для того щоб продавати неліцензійне програмне забезпечення, його необхідно певним чином змінити, нейтралізувати програмні засоби захисту від порушення авторського права. Видається, що діяльність таких осіб становить реальну небезпеку, вони є "виробниками" на "чорному ринку" програмного забезпечення. Однак, як свідчить практика, кримінально-правові засоби спрямовані здебільшого проти "посередників" і "кінцевих користувачів". Достатньо красномовною є й характеристика застосовуваних покарань. Так, у досліджених випадках переважно використовувалися штраф та позбавлення волі (по 47 разів, або по 45,6% від загальної кількості судових рішень). При цьому серед випадків застосування покарання у вигляді позбавлення волі у 93,6% використовувалося звільнення від покарання з випробуванням, а серед випадків застосування покарання у вигляді штрафу у 89,3% він дорівнював мінімальній межі санкції ч. 1 ст. 176 КК.

Неможливо не звернути уваги й на той факт, що, за оцінками експертів, основним джерелом "постачання" неліцензійного програмного забезпечення стає мережа Інтернет [257, 49],

продаж дисків з програмним забезпеченням – принципова застаріла форма "комп'ютерного піратства". Водночас серед досліджених вироків лише в одному [180] (менше 1%) ідеться про кваліфікацію дій особи, яка використовувала Інтернет для розповсюдження неліцензійного програмного забезпечення. При цьому у 9 вироках прямо зазначається, що підсудні отримували з мережі Інтернет неліцензійне програмне забезпечення, яке потім розповсюджували або використовували. Обґрунтованим буде й припущення про те, що аналогічна ситуація мала місце і в переважній більшості випадків, коли "винна особа при невстановлених обставинах отримала екземпляр контрафактного програмного забезпечення".

Таким чином, одним із можливих напрямів подальшого наукового розроблення проблем кримінально-правової охорони інформаційної безпеки є підвищення ефективності кримінально-правової протидії посяганням на інтелектуальну власність узагалі та "комп'ютерному піратству" зокрема. Потребує вдосконалення порядок обчислення матеріальної шкоди від таких посягань, який на сьогодні істотно знижує ефективність відповідних кримінально-правових засобів. Існує потреба додаткових кримінологічних досліджень, метою яких є диверсифікація засобів протидії порушенням авторського права.

Наступною проблемою, на яку необхідно звернути увагу, є кримінально-правове забезпечення процесів інформатизації в Україні. У роботі неодноразово підкреслювалося, що доступ до інформації сьогодні набуває значення прав та основних свобод людини. Одним із важливих напрямів державної політики у зв'язку з цим стає інформатизація – "сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки" [104]. Отже, оскільки інформатизація – це процес, який забез-

печує підвищення можливостей реалізації інформаційних потреб громадян, суспільства, країни, її обґрунтовано можна розглядати в контексті такої складової забезпечення інформаційної безпеки, як формування інформаційного ресурсу. Чому ми ставимо питання кримінально-правового забезпечення інформатизації? Проблема в тім, що динаміка цього надважливого суспільного процесу в Україні є вкрай незадовільною, не зважаючи на значні адресні витрати державного бюджету. Саме тому, як видається, виникла потреба наукового аналізу можливостей використання засобів кримінальної юстиції для забезпечення ефективного використання державних ресурсів у сфері інформатизації.

Звернімося до фактів. У світовому рейтингу країн за розвитком інформаційно-комунікаційних технологій Україна посідає 90-те місце. При цьому ми поступаємося Перу (89-те місце) і Пакистану (88-ме місце). Російська Федерація з її великою територією та значно більшою інфраструктурою державних органів перебуває на 77-му місці. Окремо слід зазначити динаміку нашої країни в цьому рейтингу – у 1992 році Україна була на 9-му місці [145].

Важливим показником інформатизації в країні є розвиток систем так званого "електронного уряду", який у найзагальнішому розумінні являє собою створення й функціонування інформаційних систем, що об'єднують всі органи державної влади в єдине інформаційне поле. Цим досягається зниження операційних витрат, відмова від дорогого паперового документообігу, скорочення управлінського апарату, розширення можливостей громадян в отриманні офіційної інформації, скорочення часу, необхідного для реєстрації господарюючих суб'єктів, ліцензування, подання різноманітних звітів до державних органів тощо. Із 1998 року, коли було прийнято Закон "Про національну програму інформатизації", на цю мету було витрачено близько 800 млн. дол. Але паперовий документообіг у всіх установах зберігається в повному обсязі, а кількість держслужбовців зросла приблизно на 45% [39]. Не досягнуто й од-

ного з найбільш очікуваних соціальних результатів інформатизації – зниження рівня корупції [40].

Недостатній рівень інформатизації негативно позначається й на розвиткові електронної комерції. Тому унікальні переваги електронної торгівлі як для бізнесу, так і для кінцевого споживача реалізуються далеко не повністю [66, 377]. У цілому експертна оцінка фактичного рівня інформатизації невтішна: "Відсутність єдиної державної політики та координації призвела до повного хаосу в електронних системах управління. Кожне відомство винаходить … власні технічні завдання з розробки, свої правила функціонування. Бази даних не сумісні не лише між собою, а й навіть між різними підрозділами всередині установ" [38].

Такі оцінки підтверджуються й офіційними документами. Так, 5 жовтня 2009 року Рахункова палата подала на ім'я прем'єр-міністра Ю. Тимошенко звіт за №04-2118 "Про результати аудиту діяльності органів державної влади і функціонування державних реєстрів", у якому, зокрема, зазначалося: "Діяльність центральних органів виконавчої влади зі створення та забезпечення функціонування електронних державних реєстрів є безсистемною, неконтрольованою і неефективною. Соціально-економічного ефекту від формування електронних інформаційних ресурсів з метою забезпечення прозорості, відкритості та ефективності роботи органів державної влади не досягнуто. Широкого доступу громадян до державних електронних реєстрів не забезпечено" [39]. Згідно з доповідною запискою про виконання Національної програми інформатизації за №65/05-09, підготовленою для керівництва Кабінету Міністрів Держкомітетом інформатизації у 2009 році, 50% коштів державного бюджету на виконання проектів інформатизації було спрямовано органами державної влади на закупівлю обчислювальної техніки та інших технічних засобів, 31% – на створення й модернізацію існуючої інфраструктури і тільки 2,7% – на створення інформаційних ресурсів і розроблення програмного забезпечення. "Ураховуючи те, що середня забезпеченість органів виконавчої влади комп'ютерною технікою станом на кінець 2007 року склала 126%, наведені факти свідчать про нераціональне використання бюджетних коштів" [39].

Зрозуміло, що зазначене коло питань потребує самостійного дослідження. Проте уважаємо за доцільне сформулювати певні орієнтири подальшого наукового пошуку. По-перше, навряд чи є необхідність у формулюванні низки спеціальних кримінально-правових заборон. Наявні кримінально-правові засоби можуть бути достатньо задовільними. Ідеться про закони про кримінальну відповідальність за зловживання або перевищення повноважень (ст.ст. 364, 364-1, 365, 365-1). Однак, по-друге, їх використання для розв'язання сформульованого завдання потребує спеціального дослідження для встановлення чітких та операціональних критеріїв визначення заподіяної шкоди. Необхідним є наукове обґрунтування методу аналізу того, наскільки певне рішення службової особи щодо розроблення й використання відомчої інформаційної системи сприяє розв'язанню завдань інформатизації або якою є ефективність витрачених коштів. При цьому остання має визначатися не класичним шляхом – збільшення матеріальних активів певної установи, якість та вартість придбаної техніки або виконаних робіт, а з урахуванням того, наскільки відповідні витрати сприяли створенню загального інформаційного поля, забезпечили економію коштів, які витрачаються на утримання управлінського апарату, допомогли виконанню завдань, що стоять перед певною установою.

Останньою проблемою, на яку необхідно звернути увагу, є кримінально-правова протидія зловживанням у сфері збирання персональних даних. До питання охорони таких даних ми зверталися в попередній главі під час аналізу правових засобів забезпечення доступу до інформації. Однак у сфері такої складової інформаційної безпеки, як формування інформаційних ресурсів, правовий захист персональних даних має інший вимір. Він пов'язаний із тим, що створення надпотужних баз пер-

сональних даних може через розширення можливостей органів державної влади створити загрозу демократичному розвиткові країни та забезпечити умови для специфічних зловживань у комерційній сфері. У першій главі ці аспекти загроз інформатизації суспільства розглядалися в контексті концепції рефлексивної модернізації Е. Гідденса.

Певного коментаря потребує таке питання: чому збирання персональних даних є настільки важливим, що вимагає нормативної регуляції та в чому полягає небезпека збирання таких даних із порушенням установленого порядку? Тут можна цілком погодитися з А.В. Пазюком, який зазначає, що неправомірне збирання інформації завдає шкоди сформованому суспільством уявленню про індивіда, його соціальній "масці". Джерелом такого уявлення є інформація, яку індивід явно чи не явно демонструє суспільству [259]. Те, що певну інформацію про себе суб'єкт приховує від оточуючих, є таким само природним, як і, наприклад, носіння одягу. Це аксіома суспільного буття, а тому посягання на таке право людини можна сміливо називати посяганням на засади існування суспільства. У свою чергу питання про незаконне збирання персональних даних набуло актуальності, гостроти та певного рівня суспільної небезпечності саме у зв'язку з появою сучасних інформаційних технологій. Ці технології дозволяють накопичувати величезні обсяги інформації, швидко орієнтуватися в ній, моментально отримувати інформацію про всі аспекти життя конкретної людини. Зрозуміло, що за умов такої технічної бази відсутність законодавчих обмежень збирання персональної інформації може призвести до створення тотальних інформаційних систем персональних даних, а отже, до тотального контролю над поведінкою індивідів. Проблематика, пов'язана зі створенням таких інформаційних систем, отримала в західній науковій і публіцистичній літературі назву "проблема Великого брата" [402, 409, 413]. Слід визнати, що назва є вельми влучною, адже на сучасному рівні розвитку та впровадження інформаційних технологій відомий роман Джорджа Оруела вже

не здається фантастичним, а описані в ньому події – це яскрава ілюстрація в тому числі й небезпеки, яку може створити неконтрольоване накопичення персональних даних. Саме тому аналіз законодавчих механізмів захисту персональних даних є вельми актуальним завданням.

Законом України "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних" від 2 червня 2011 року передбачено зміну редакції статті 182 КК та доповнення Кодексу про адміністративні правопорушення низкою статей. Зазначена стаття КК передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або за незаконну зміну такої інформації, крім випадків, передбачених іншими статтями КК. Доцільність установлення спеціальної кримінальної відповідальності за використання та розповсюдження персональних даних повертає нас до питань, розглянутих у попередній главі. Так само спірною є необхідність криміналізації їх знищення та зміни, оскільки існують норми про відповідальність за знищення або підробку документів, знищення або порушення цілісності комп'ютерних даних. Крім того, нова редакція ст. 182 передбачає відповідальність тільки за вищеперелічені дії і лише в частині другій пов'язує її з настанням певних наслідків. Ураховуючи наведені вище аргументи щодо значення суспільно небезпечних наслідків незаконних дій з інформацією як провідного критерію необхідності застосування заходів кримінальної юстиції, уважаємо, що в цьому випадку порушено вимогу легітимації кримінально-правової заборони. Практика використання такої норми з великою ймовірністю може призвести до застосування кримінально-правових заходів у випадках, які не відносяться до суспільно небезпечних, чим, знову ж таки, може бути спричинено зниження ефективності кримінально-правової протидії посяганням у сфері інформаційної діяльності з персональними даними. Проте ці питання ми вже розглянули. Що сто-

сується збирання персональних даних, то суспільно небезпечні види таких дій повністю охоплюються запропонованою в попередній главі нормою про відповідальність за незаконне отримання доступу до інформації.

Розглянемо, наскільки обґрунтованим є встановлення кримінальної відповідальності за незаконне зберігання персональних даних незалежно від настання суспільно небезпечних наслідків (ч. 1 ст. 182 КК). Порядок зберігання персональних даних передбачено Законом України "Про захист персональних даних" від 1 червня 2010 року. У загальних рисах він полягає в тому, що накопичення (зберігання) персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих відомостей до бази персональних даних. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них. Таким чином, під незаконним зберіганням персональних даних слід розуміти вчинення таких дій з порушенням установлених законом вимог, зокрема, щодо повідомлення про включення до бази або забезпечення цілісності, доступності та конфіденційності даних.

Хоча наведене визначення не охоплює всієї сукупності можливих випадків, його цілком достатньо для аналізу доцільності використання кримінально-правових засобів забезпечення законності зберігання персональних даних. Зрозуміло, що встановлення кримінальної відповідальності за такі дії є необґрунтованим з позицій дотримання такого принципу криміналізації, як суспільна небезпечність. На користь цього додає аргументів і те, що означеним законом передбачено адміністративну відповідальність за: неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються (ч. 1 ст. 188-39 КУпАП); неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних

даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних (ч. 2 ст. 188-39 КпАП); ухилення від державної реєстрації бази персональних даних (ч. 4 ст. 188-39 КпАП); недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них (ч. 5 ст. 188-39 КпАП). По суті, названі діяння є окремими видами незаконного зберігання персональних даних. Отже, відкритим, через відсутність чітких законодавчих критеріїв, залишається й питання відмежування злочинного зберігання персональних даних від незлочинного.

Однак сказане не означає, що зберігання персональних даних не може бути суспільно небезпечним. Видається, що як суспільно небезпечні такі дії можуть розглядатися в тих випадках, коли виступають видами зловживання або перевищення повноважень (ст.ст. 364, 364-1, 365, 365-1) чи недбалості (ст. 367). По-перше, саме з суб'єктами означених посягань можна пов'язувати вчинення дійсно небезпечних видів зберігання або збирання даних. По-друге, відповідальність за ці злочини пов'язана з настанням певних наслідків, тому використання для протидії незаконному зберіганню персональних даних саме цих законів про кримінальну відповідальність дозволить не тільки чітко розмежовувати адміністративні проступки та злочини, але й забезпечить ефективність кримінально-правової протидії, оскільки до сфері кримінальної юстиції потраплятимуть дійсно суспільно небезпечні діяння. Зрозуміло, що таке рішення потребує спеціального дослідження незаконного зберігання персональних даних як виду зловживання чи перевищення повноважень або службової недбалості, установлення чітких критеріїв і методів оцінки заподіяної шкоди.

Таким чином, наступним напрямом наукового пошуку у сфері кримінально-правового забезпечення інформаційної безпеки має стати дослідження можливостей використання законів про кримінальну відповідальність за перевищення повноважень та зловживання ними, недбалість для протидії суспіль-

но небезпечним видам незаконного зберігання персональних даних.

Висновки до шостої глави

Проведений аналіз кримінально-правових засобів забезпечення формування інформаційного ресурсу дозволяє зробити такі висновки:

1. Якщо порушення у сфері використання інформаційних технологій або забезпечення доступу до інформації унеможливлюють реалізацію інформаційної потреби, то в разі порушення інформаційної безпеки у сфері формування ресурсу суб'єкт отримує можливість реалізувати інформаційну потребу, але внаслідок порушення така реалізація призводить до настання певних наслідків через соціальну дезорієнтацію суб'єкта.

2. Дослідження методом контекстної законодавчої оцінки суспільної небезпечності діяння дозволило встановити, що в цілому система кримінально-правових засобів забезпечення формування інформаційного ресурсу є обґрунтованою, однак спостерігається певне завищення суворості санкцій за окремі дії з порнографічними предметами.

3. Кількісні та якісні показники формування національного інформаційного ресурсу свідчать про значний потенціал можливих суспільно небезпечних наслідків. Однак розширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення "суспільно небезпечної інформації" є недоцільними через прогнозовану неефективність і декларативність таких норм, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Разом із цим, з розвитком технологій медіатизації, психології та соціології формулювання подібних норм, можливо, стане дійсністю.

4. Одним із можливих напрямів подальшого наукового розроблення проблем кримінально-правової охорони інформаційної безпеки є підвищення ефективності кримінально-правової протидії посяганням на інтелектуальну власність узагалі та "комп'ютерному піратству" зокрема. Потребує вдосконалення порядок обчислення матеріальної шкоди від таких посягань, який на сьогодні істотно знижує ефективність відповідних кримінально-правових засобів. Існує потреба додаткових кримінологічних досліджень, метою яких є диверсифікація засобів протидії порушенням авторського права.

5. Необхідним є наукове обґрунтування методу аналізу того, наскільки певне рішення службової особи у сфері інформатизації є ефективним з позицій витрачених коштів та отриманих результатів. При цьому метод має враховувати те, наскільки відповідні витрати сприяли створенню загального інформаційного поля, забезпечили економію коштів, які витрачаються на утримання управлінського апарату, допомогли виконанню завдань, що стоять перед певною установою.

6. Одним із напрямів наукового пошуку у сфері кримінально-правового забезпечення інформаційної безпеки має стати дослідження можливостей використання законів про кримінальну відповідальність за перевищення та зловживання повноваженнями, недбалість для протидії суспільно небезпечним видам незаконного зберігання персональних даних.

Післямова

Здійснене дослідження кримінально-правової охорони інформаційної безпеки дозволяє зробити такі висновки:

1. Як об'єкт кримінально-правової охорони інформаційна безпека являє собою систему суспільних відносин щодо забезпечення реалізації інформаційних потреб громадян, суспільства, держави, яка включає: 1) відносини щодо забезпечення доступу до інформаційних ресурсів; 2) відносини щодо формування інформаційного ресурсу; 3) відносини щодо забезпечення функціонування інформаційних технологій як засобів доступу до інформаційного ресурсу та його формування.

2. Кожній із зазначених складових інформаційної безпеки відповідають специфічні соціальні потреби, які зумовлюють необхідність кримінально-правової охорони. Так, необхідність захисту відносин у сфері використання інформаційних технологій зумовлена значенням, яке відіграє використання останніх в організації та здійсненні певних видів людської діяльності, кількість яких постійно збільшується через розширення сфери застосування комп'ютерної техніки. Відносини інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу потребують кримінально-правової охорони з огляду на наявну актуальну суспільну потребу, що, з одного боку полягає в необхідності забезпечення вільного доступу до інформаційних ресурсів якомога більшій кількості членів суспільства, а з іншого – актуалізує проблему ґарантування встановлених обмежень доступу до певних видів інформації. Формування інформаційного ресурсу потребує кримінально-правових засобів охорони з огляду на потенційну можливість іс-

тотних порушень соціальної стабільності шляхом зловживань у цій сфері.

3. Загальною рисою суспільних відносин інформаційної безпеки, які потребують кримінально-правової охорони, є те, що їх значення походить від значимості тих суспільних відносин, у межах яких виникає інформаційна потреба. Саме значення суспільних відносин визначає значення певних відносин інформаційної безпеки, а також доцільність та інтенсивність відповідних заходів кримінально-правової охорони.

4. У зв'язку з тим, що інформаційна безпека являє собою систему суспільних відносин, які потребують кримінально-правового захисту, характеризуються специфічним, властивим саме цій групі відносин змістом чинників суспільної небезпечності посягань на них, обґрунтовано доцільність включення інформаційної безпеки до системи родових об'єктів злочинів, передбачених КК України; на цій підставі запропоновано замінити назву розділу XVI Особливої частини КК України такою – "Злочини у сфері інформаційної безпеки" та об'єднати в ньому норми про відповідальність за злочини у сфері використання інформаційних технологій, забезпечення доступу до інформації та формування інформаційного ресурсу.

5. Ураховуючи, що кримінально-правова охорона інформаційної безпеки забезпечується великою кількістю законів про кримінальну відповідальність, запропоновано метод контекстного дослідження законодавчої оцінки суспільної небезпечності злочинів, сутність якого полягає в тому, що кожен злочин розглядається в контексті інших з позицій порівняння та співставлення видів і розмірів покарань, що можуть бути за нього призначені. Контекстна законодавча оцінка суспільної небезпечності, на відміну від існуючих методів порівняння, забезпечує можливість аналізу кожної кримінально-правової санкції в порівнянні з генеральною сукупністю, що дозволяє з великою вірогідністю прогнозувати значну ефективність методу, наближення законодавчих оцінок суспільної небезпечності певних посягань до їх фактичної, об'єктивної небезпеки. Достатньо перспективним видається використання розглянутого ме-

тоду в законотворчій роботі, певний розвиток якого можна забезпечити й компаративістським кримінально-правовим дослідженням.

6. Ключовою позицією в побудові механізму кримінально-правової охорони суспільних відносин у сфері використання комп'ютерної техніки та мереж електрозв'язку є сутність суспільної небезпечності відповідних посягань. Вона не є самостійною та визначається головним чином соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це й визначає суспільну небезпечність конкретного посягання у сфері використання інформаційних технологій.

7. Стосовно кримінально-правової охорони відносин інформаційної безпеки у сфері використання інформаційних технологій установлено:

- чинне законодавство про кримінальну відповідальність передбачає певну систему кримінально-правових засобів охорони суспільних відносин у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку, однак аналіз відповідних норм КК свідчить про те, що зазначена специфіка суспільної небезпечності врахована не повною мірою, а також спостерігається порушення низки принципів криміналізації;

- при криміналізації злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку був порушений принцип суспільної небезпечності: через відсутність у законодавчих визначеннях злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку чітких критеріїв суспільної небезпечності під кримінально-правову заборону та, відповідно, до сфери впливу кримінальної юстиції потрапляють не тільки діяння, які дійсно є суспільно небезпечними, але й ті, які такими не є; таке положення різко негативно відбивається на ефективності кримінально-

правової охорони інформаційної безпеки у сфері використання інформаційних технологій;

- порушений принцип визначеності та єдності термінології. У ст.ст. 361 – 363-1 при формулюванні ознак злочинних діянь використовується термінологія, яка різниться з тією, що використана при формулюванні ознак суміжних адміністративних правопорушень, *відсутність єдності* термінології значно зменшує ефективність відповідних норм як кримінального законодавства, так і адміністративного;

- норми розділу XVI містять терміни, які *неоднаково визначаються* як на рівні законодавства, так і на рівні наукового тлумачення, що звужує можливості його використання для охорони відповідних суспільних відносин;

- використання в диспозиціях зазначених норм переліку технічних засобів обробки інформації створює небезпеку "технологічної залежності" законодавства;

- чинна редакція ст. 361-2 дозволяє говорити як про надлишковість заборони, що в ній сформульована, так і про формування цією нормою певних прогалин у законодавстві; надлишковість стосується криміналізації діянь, які не можна визнавати суспільно небезпечними в контексті інших норм щодо відповідальності за незаконні дії з інформацією з обмеженим доступом; прогалини пов'язані з невдалим формулюванням ознак предмета, які значно звужують можливості норми, роблять кримінально-правові засоби, передбачені нею, такими, що не відповідають сучасним потребам протидії злочинам у сфері використання інформаційних технологій;

- конструкція об'єктивної сторони ст. 361 КК України зумовлює прогалини, що полягають у неможливості притягнення до кримінальної відповідальності осіб, які заподіюють зазначені в нормі суспільно небезпечні наслідки без вчинення передбаченого в нормі діяння;

- певні прогалини створює законодавче визначення суб'єкта злочину, передбаченого ст. 363 КК, яке не відповідає можливим формам об'єктивної сторони цього посягання; крім того, неефективність розгляданої норми зумовлена недоліками

законодавчого регулювання використання засобів захисту інформації;

- прогалини мають місце при формулюванні кримінально-правової заборони масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК). Вони полягають у тому, що відповідальність за розповсюдження спаму пов'язана з наслідками, які є абсолютно нетиповими для подібних дій, а отже, переважна більшість випадків розповсюдження спаму не підпадає під ознаки злочину, передбаченого цією нормою. Недосконалим, таким, що зменшує ефективність кримінально-правової охорони, є також матеріально-правове регулювання множинного розсилання телекомунікаційних повідомлень;

- установлено порушення принципу повноти складу; воно полягає як у формулюванні занадто громіздких законодавчих визначень, які ускладнюють установлення змісту ознак конкретних складів злочинів (ст. 361 КК передбачає відповідальність за два абсолютно самостійні склади злочинів), так і в недостатній визначеності складів конкретних комп'ютерних злочинів у диспозиціях відповідних кримінально-правових норм (відсутність чітких положень щодо змісту суб'єктивної сторони злочинів, передбачених ст.ст. 361 – 363-1 КК, недостатньо конкретне формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 362 КК);

- певне зменшення ефективності кримінально-правових засобів охорони інформаційних суспільних відносин зумовлене *недоліками диференціації відповідальності залежно від заподіяної шкоди* та *відсутністю* в нормах досліджуваного розділу спеціальної вказівки на можливість так званої *змішаної повторності;*

- дослідження відповідності національного кримінального законодавства про злочини у сфері використання інформаційних технологій принципу міжнародно-правової необхідності та допустимості криміналізації дозволяє казати про надлишковість зобов'язань, узятих на себе Україною при ратифікації Конвенції про кіберзлочинність та необхідність внесення нових застережень до Закону України "Про ратифікацію Конвенції про кіберзлочинність".

8. Для розв'язання зазначених проблемних аспектів пропонується низка законотворчих пропозицій, що знайшли відображення в проекті нової редакції розділу XVI КК України (додаток 10). Для врахування динамічності досліджуваних злочинів необхідним видається нормативне закріплення вимоги періодичного аналізу тенденцій розвитку злочинів у сфері використання інформаційних технологій, чинників їх суспільної небезпечності, соціальних потреб у відповідних кримінально-правових заборонах та ефективності їх застосування в форматі засідань відповідних комітетів Верховної Ради України за участі представників правоохоронних і судових органів.

9. Дослідження кримінально-правової охорони суспільних відносин забезпечення доступу до інформації дозволило зробити такі висновки:

- сутність порушень інформаційної безпеки у сфері забезпечення доступу до інформаційного ресурсу полягає в тому, що ускладнення чи унеможливлення реалізації інформаційної потреби зумовлюється порушенням установленого режиму доступу до певного ресурсу або неправомірним обмеженням доступу до певної інформації;

- межі кримінально-правового регулювання у сфері забезпечення доступу до інформаційного ресурсу визначаються інтенсивністю наслідків, які настають через обмеження можливості реалізації інформаційної потреби відповідних суб'єктів;

- дослідження чинної системи кримінально-правових засобів забезпечення обмеженого доступу до інформації з використанням методу контекстної законодавчої оцінки суспільної небезпечності дозволило встановити такі її вади: 1) очевидна невідповідність суспільної небезпечності низки діянь, передбачених КК, інтенсивності санкцій відповідних норм; 2) непослідовність законодавчих рішень у питанні встановлення кримінальної відповідальності за спеціальні види незаконного отримання або надання доступу до інформації, при цьому особливо слід відзначити необґрунтоване підвищення санкцій за несанкціонований доступ у разі його вчинення з використанням інформаційних технологій; 3) непослідовна законодав-

ча оцінка схожих за змістом ознак, що характеризують суб'єкт посягання; 4) спірні законодавчі рішення в питанні формулювання ознак кваліфікованих посягань на відносини щодо забезпечення обмеженого доступу до інформації; 5) неузгодженість використовуваної термінології;

- аналіз кримінально-правових засобів забезпечення обмеженого доступу до інформації на предмет відповідності сучасним проявам суспільно небезпечної поведінки у сфері отримання та надання незаконного доступу до інформації дозволяє стверджувати про фрагментарність та несистемність законодавства в цій сфері;

- сформульовано пріоритетні завдання вдосконалення системи кримінально-правових засобів забезпечення обмеженого доступу до інформації: 1) подолання фрагментарності кримінально-правової охорони; 2) пошук загальних підходів до законодавчої оцінки суспільної небезпечності окремих видів незаконного отримання або надання доступу; 3) розвиток системи як засобу протидії формуванню ринку незаконних інформаційних послуг;

- для наближення законодавчих оцінок суспільної небезпечності посягань у сфері обмеженого доступу до їх фактичних чинників, створення передумов для більш раціонального використання засобів кримінальної юстиції в зазначеній сфері та забезпечення стабільності законодавства про кримінальну відповідальність в умовах подальшої інформатизації суспільства запропоновано зміни до КК, які передбачають: доповнення КК загальними нормами про незаконне надання доступу та його отримання; скасування низки норм, що передбачають окремі види порушень обмеженого доступу до різноманітних видів інформації;

- обґрунтовано, що як просту форму кримінально караного надання доступу до інформації доцільно криміналізувати незаконне надання доступу до таємної, службової або конфіденційної інформації, якщо це спричинило істотне порушення реалізації прав, свобод, законних інтересів. До кваліфікуючих ознак незаконного надання доступу до інформації пропо-

нується відносити: повторність; вчинення злочину групою осіб за попередньою змовою; вчинення злочину особою, яка має правомірний доступ до інформації у зв'язку з займаною посадою або спеціальними повноваженнями; використання засобів масової інформації або інших інформаційних технологій, що забезпечують доступ до інформації значної кількості осіб; вчинення злочину з корисливою метою; спричинення тяжких наслідків;

- запропоновано визначення простої форми злочинного отримання доступу до інформації як отримання незаконного доступу до таємної, службової або конфіденційної інформації, вчинене шляхом подолання технічних, програмних або організаційних засобів захисту інформації; до кваліфікуючих ознак незаконного отримання доступу до інформації пропонується відносити: повторність; вчинення злочину групою осіб за попередньою змовою; використання технічних або програмних засобів, призначених для незаконного отримання доступу до інформації; вчинення злочину з метою надання незаконного доступу до інформації;

- передбачена чинним законодавством система кримінально-правових засобів забезпечення надання доступу до інформації визнана обґрунтованою та достатньою, такою, що дозволяє забезпечити ефективний захист відносин у сфері надання доступу до інформації, однак її ефективність залежить від якості правового регулювання інформаційної діяльності.

10. Дослідження кримінально-правової охорони формування інформаційного ресурсу дозволило встановити таке:

- якщо порушення у сфері використання інформаційних технологій або забезпечення доступу до інформації унеможливлюють реалізацію інформаційної потреби, то в разі порушення інформаційної безпеки у сфері формування ресурсу суб'єкт отримує можливість реалізувати інформаційну потребу, але внаслідок порушення така реалізація призводить до настання певних наслідків, через соціальну дезорієнтацію суб'єкта, неадекватне сприйняття ним дійсності;

- дослідження методом контекстної законодавчої оцінки суспільної небезпечності діяння дозволило встановити, що в цілому система чинних кримінально-правових засобів забезпечення формування інформаційного ресурсу є обґрунтованою, однак спостерігається певне завищення суворості санкцій за окремі дії з порнографічними предметами;

- кількісні та якісні показники формування національного інформаційного ресурсу свідчать про значний потенціал можливих суспільно небезпечних наслідків, однак розширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення "суспільно небезпечної інформації", є недоцільними через прогнозовану неефективність і декларативність таких норм, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації.

11. У ході дослідження виявилося можливим сформулювати перспективні напрями подальших наукових досліджень кримінально-правової охорони інформаційної безпеки:

- підвищення ефективності кримінально-правової протидії посяганням на інтелектуальну власність узагалі та "комп'ютерному піратству" зокрема, яке передбачає вдосконалення порядку обчислення матеріальної шкоди від таких посягань, який на сьогодні істотно знижує ефективність відповідних кримінально-правових засобів, проведення додаткових кримінологічних досліджень, метою яких є диверсифікація засобів протидії порушенням авторського права;

- наукове обґрунтування методу аналізу шкоди, заподіяної зловживанням або перевищенням повноважень у сфері інформатизації, який повинен ураховувати, наскільки відповідні витрати сприяли створенню загального інформаційного поля, забезпечили економію коштів, які витрачаються на утримання управлінського апарату, допомогли виконанню завдань, що стоять перед певною установою;

- дослідження можливостей використання законів про кримінальну відповідальність за перевищення, зловживання повноваженнями та недбалість для охорони прав громадян щодо доступу до інформації та протидії суспільно небезпечним видам незаконного зберігання персональних даних.

12. Викладені положення знайшли відображення у відповідному проекті Закону щодо змін та доповнень до Кримінального кодексу України та Кодексу України про адміністративні правопорушення (додаток 10).

Список використаних джерел

1. Автоматизовані системи. Терміни та визначення : ДСТУ 2226-93. – Вид. офіц. – Вперше ; введ. 1994-07-01. – К. : Держспоживстандарт України, 1994. – 47 с.

2. Азаров, Д. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д.С. Азаров // Право України. – 2000. – № 12. – С. 69 – 73.

3. Азаров, Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) / Д.С. Азаров. – К.: Атіка, 2007. – 304 с.

4. Азаров, Д.С. Кваліфікуючі ознаки складів злочинів: вибрані риторичні питання / Д.С. Азаров, А.В. Калуп // Теоретичні та прикладні проблеми кримінального права України: матеріали міжнародної науково-практичної конференції, м. Луганськ, 20 – 21 травня 2011 р. [редкол.: Г.Є. Болдарь, А.О. Данілевський, О.О. Дудоров та ін.] ; МВС України, Луганський державний університет внутрішніх справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2011. – С. 6 – 11.

5. Азаров, Д.С. Нові зміни до розділу XVI Особливої частини Кримінального кодексу України – нові проблеми / Д.С. Азаров // Юридичний вісник України. – 2005. – № 6. – С. 28 – 32.

6. Азаров, Д.С. Про розмежування злочинів, передбачених статтями 361 і 362 Кримінального кодексу України / Д.С. Азаров // Кримінальне право України. – № 3. – 2006. – С. 32 – 39.

7. Актуальні проблеми інформаційної безпеки України (аналітична доповідь УЦЕПД) // Національна безпека і оборона. – 2001. – № 1. – С. 2 – 60.

8. Ализар, А. Спам приносит только пользу [Электронный ресурс] // Вебсайт интернет-издания "Вебпланета". – Режим доступа: http://www.webplanet.ru/news/internet/2004/3/3/spamm.html

9. Американские следователи не нашли улик против Ассанджа [Электронный ресурс] // ПРАВО.ru. – 10.02.2011. – Режим доступа : http://www.pravo.ru/interpravo/news/view/48103/

10. Аналіз стану здійснення судочинства судами загальної юрисдикції в 2008 р. [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу: http://www.scourt.gov.ua/clients/vs.nsf/0/9DDE825F47D1FAF3C225766A0041BF8D?OpenDocument&CollapseView&RestrictToCategory=9DDE825F47D1FAF3C225766A0041BF8D&Count=500&)

11. Аналіз стану здійснення судочинства судами загальної юрисдикції в 2009 р. [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу: http://www.scourt.gov.ua/clients/vs.nsf/0/09F805995C5F5CA6C2257752002A196D?OpenDocument&CollapseView&RestrictToCategory=09F805995C5F5CA6C2257752002A196D&Count=500&)

12. Аналітичний огляд стану комп'ютерної злочинності та інформаційної безпеки в Україні у 2000 році // Національне бюро Інтерполу в Україні. – К., 2001. – 26 с.

13. Андрушко, П.П. Коментар до розділу XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку" Особливої частини Кримінального кодексу України / П.П. Андрушко // Законодавство України. – № 1. – 2006. – С. 32 – 54

14. Антонов, С. Компьютерные преступления в банковской сфере / С. Антонов // Юридическая практика. – 1997. – № 8. – С. 7.

15. Арістова, І.В. Розбудова правової держави в Україні: правовий механізм забезпечення права на доступ до інформації в суспільстві знань / І.В. Арістова // Правова інформатика. – 2010. – № 1. – С. 3 – 13.

16. Армянский хакер потряс всех масштабностью своей деятельности [Электронный ресурс] // Центр исследования ком-

пьютерной преступности. – 05.11.2010. – Режим доступа : http://www.crime-research.ru/news/05.11.2010/7003/

17. Ашманов, И. Спам 2004: подробный аналитический отчет [Электронный ресурс] / Игорь Ашманов, Анна Власова, Алексей Тутубалин // Официальный сайт альянса разработчиков программного обеспечения SiliconTaiga. – Режим доступа : http://www.silicontaiga.ru/home.asp?artId=3169.

18. Балдицын, В.В. Охранительные правоотношения в сфере обеспечения информационной безопасности современной России (теоретико-правовой аспект) : дис. канд. юрид. наук : 12.00.01 / Василий Вячеславович Балдицын ; [Северо-западная академия государственной службы]. – СПб., 2000. – 178 с.

19. Балобанова, Д.О. Теорія криміналізації : дис. ... канд. юрид. наук: 12.00.08 / Балобанова Дар'я Олександрівна ; Одеська національна юридична академія. – Одеса, 2007. – 208 с.

20. Батурин, Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юридическая литература, 1991. – 157 с.

21. Белл, Д. Прихід постіндустріального суспільства / Д. Белл // Сучасна зарубіжна соціальна філософія. – К., 1996. – С. 194 – 251.

22. Бергер, П. Социальное конструирование реальности : трактат по социологии знания / П. Бергер, Т. Лукман ; пер. Е. Руткевич. – М. : Медиум, 1995. – 333 с.

23. Берзін, П.С. Злочинні наслідки в механізмі кримінально-правового регулювання : автореф. дис. ... д-ра юрид. наук : 12.00.08 / Берзін Павло Сергійович ; Київ. нац. ун-т ім. Т. Шевченка. – К., 2010. – 35 с.

24. Бєгун, А.В. Інформаційна безпека : навчальний посібник / А.В. Бєгун. – К.: КНЕУ, 2008. – 280 с.

25. Бидашко, Е.А. Компьютерные преступления: миф или реальность? / Е.А. Бидашко, Н.Л. Волкова // Науковий вісник Дніпропетровського юридичного інституту МВС України. – 2001. – № 1 (14). – С. 160 – 168.

26. Біленчук, П.Д. Комп'ютерна злочинність : навчальний посібник / Петро Дмитрович Біленчук, Володимир Васильович Бут, Владислав Данилович Гавловський, Михайло Васильович Гуцалюк, Руслан Леонідович Колпак. – К.: Атіка, 2002. – 240 с.

27. Богдановская, И.Ю. Законодательство о спаме: зарубежный опыт и российские перспективы / И.Ю. Богдановская, Е.К. Волчинская // Информационное право. – 2005. – № 1. – С. 31 – 34.

28. Бойченко, О.В. Інформаційна безпека в органах внутрішніх справ (організаційно-правові засади): монографія / О.В. Бойченко. – Сімферополь : ВАТ "Сімферопольська міська друкарня", 2009. – 288 с.

29. Борзенко, А. Украденное "я" / Андрей Борзенко [Электронный ресурс] // Итоги.ru. – 2011. – № 01 (760). – Режим доступа: http://www.itogi.ru/pda/hitech-business/2011/1/160664.html.

30. Борисов, В.І. Основні напрямки розвитку Особливої частини законодавства України про кримінальну відповідальність / В.І. Борисов // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13 – 14 жовтня 2011 р. / редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 280 – 283.

31. Ботвінкін, О. Проблеми забезпечення національної безпеки в інформаційній сфері / О. Ботвінкін // Юридичний журнал. – 2007. – № 2. – С. 58 – 63.

32. Братель, О. Поняття та зміст доктрини інформаційної безпеки / О. Братель // Право України. – 2006. – № 5. – С. 36 – 41.

33. Брусничкин, Г. Информационная безопасность предпринимателя / Г. Брусничкин // Мир безопасности. – 2004. – № 4. – С. 8 – 10.

34. Бугера, О. Засоби масової інформації: проблема вдосконалення діяльності щодо запобігання протиправної поведінки неповнолітніх / О. Бугера // Підприємництво, господарство і право. – 2005. – № 7. – С. 70 – 73.

35. Бугера, О.І. Проблеми використання засобів масової інформації для запобігання злочинів серед неповнолітніх: дис. ... канд. юрид. наук: 12.00.08 / Бугера О.І. ; Національний педа-

гогічний ун-т ім. М.П. Драгоманова. – К., 2006. – 224 арк. – Арк. 208 – 224.

36. Бутузов, В.М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науково-практичний коментар / В.М. Бутузов, С.Л. Остапец, В.П. Шеломенцев. – К. : Друкарня МВС України, 2005. – 86 с.

37. Бутузов, В.М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науково-практичний коментар / В.М. Бутузов, С.Л. Остапец, В.П. Шеломенцев. – К. : Друкарня МВС України, 2005. – 86 с.

38. Бутусов, Ю. Держава 2.0 чи Держава.gov? [Електронний ресурс] / Ю. Бутусов // Дзеркало тижня. – 2010. – № 31. – Режим доступу : http://dt.ua/articles/60954

39. Бутусов, Ю. Електронна соціальна карточна гра. Посібник із розпилення мільярдів [Електронний ресурс] / Ю. Бутусов // Дзеркало тижня. – 2010. – № 43. – Режим доступу : http://dt.ua/articles/61519

40. Бутусов, Ю. Михайло Бродський: "За державні документи бізнес платить приватним структурам вісім мільярдів на рік"[Електронний ресурс] / Ю. Бутусов // Дзеркало тижня. – 2010. – № 37. – Режим доступу: http://dt.ua/articles/61191

41. В Белоруссии хищения путем использования компьютерных технологий составляет 93% всех преступлений в сфере высоких технологий [Электронный ресурс] // Центр исследования компьютерной преступности. – 23.09.2010. – Режим доступа : http://www.crime-research.ru/news/23.09.2010/6957/

42. В Египте Twitter оказался вне закона [Электронный ресурс] // Первый информационный портал "ОБОЗ.ua - Обозреватель". – 26.01.2011. – Режим доступа : http://mobilnik.ua/news/30520.html

43. В интернет попали СМС абонентов четырех сотовых операторов [Электронный ресурс] // Центр информационной безопасности beazpeka.com – 19.07.2011. – Режим доступа : http://www.bezpeka.com/ru/news/2011/07/19/sms-leak.html

44. В Лондоне растет безграмотное поколение – исследование [Электронный ресурс] // Факты и комментарии. – 01.06.2011. – Режим доступа: http://fakty.ua/133847-v-londone-rastet-pokolenie-ne-sposobnoe-prochest-elementarnye-slova

45. В Одессе поймали хакера, похитившего данные 190 тыс. пользователей [Электронный ресурс] // РИА "Новости" Украина. – 16.03.2011. – Режим доступа: http://rian.com.ua/incedents/20110316/78680949.html

46. В США "русский хакер" Федоров получил 10 месяцев тюрьмы [Электронный ресурс] // NEWSru.com. – 06.01.2011. – Режим доступа: http://www.newsru.com/world/06jan2011/feodorov.html

47. В Турции хакеры атакуют сайты членов правительства [Электронный ресурс] // Центр исследования компьютерной преступности. – 01.09.2010. – Режим доступа : http://www.crime-research.ru/news/01.09.2010/6937/

48. В Украине готовят закон о борьбе с интернет-агрессией [Электронный ресурс] // Украинский Центр Информационной Безопасности. – 10.06.2011. – Режим доступа : http://www.bezpeka.com/ru/news/2011/06/10/ukraine-internet-agression-law.html

49. В Україні "квітне" програмне піратство – експерти [Електронний ресурс] // Українська правда. – 02.02.2011. – Режим доступу: http://life.pravda.com.ua/technology/2011/02/2/71380/

50. Вам спам мешает? [Электронный ресурс] // Журнал "Деньги". – 2010. – № 43 (800). – Режим доступа : http://www.kommersant.ru/doc.aspx?fromsearch=600378e1-e0fb-42e3-b978-139ba8b5748e&docsid=1524322

51. Вартанова, Е.Л. Саморегулирование в информационном обществе / Е.Л. Вартанова // Вестник МГУ. Серия 10. Журналистика. – 2006. – № 3. – С. 8 – 19.

52. Вебер, А.Б. Устойчивое развитие как социальная проблема: (Глобальный контекст и российская ситуация) / А.Б. Вебер / РАН. Ин-т социол. – М. : Изд-во Ин-та социол., 1999. – 122 с.

53. Великий енциклопедичний юридичний словник : [за ред. акад. НАН України Ю.С. Шемшученка]. – К. : ТОВ "Видавництво юридична думка", 2007.– 992 с.

54. Вехов, В. Проблема определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ / В. Вехов // Уголовное право. – 2004. – № 4.– С. 15-17.

55. Винер, Н. Кибернетика или управление и связь в животном и машине / Норберт Винер. – М.: Советское радио, 1968. – 328 с.

56. Виртуальные источники информации. "Белый" и "черный" рынки информационных ресурсов сыска. [Электронный ресурс] // Частное охранное предприятие ЧОП "Чёрный Ворон". – 08.01.2011. – Режим доступа: http://чоп-воронеж.рф/informations/166–lr-lr-4.html.

57. Вовчик-Блакитна, Л. Мы не рабы, мы – куклы? [Электронный ресурс] / Л. Вовчик-Блакитна // Зеркало недели. – 2006. – № 47. – Режим доступу : http://zn.ua/articles/48603

58. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / Александр Григорьевич Волеводз. – М. : Юрлитинформ, 2002. – 496 с.

59. Волобуєв, А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки / А.Ф. Волобуєв // Вісник Луганського інституту внутрішніх справ. – 1998. – № 2. – С. 179 – 185.

60. Воройский, Ф.С. Систематизированный толковый словарь по информатике [вводный курс по информатике и вычислительной технике в терминах] / Ф.С. Воройский. – М. : Либерия, 1998. – 375 с.

61. Воронов, К. Хакер заплатит по счетам RBS WorldPay / Константин Воронов [Электронный ресурс] // Коммерсантъ (Новосибирск). – 2011. – № 8 (4546). – Режим доступа : http://kommersant.ru/doc-y.aspx?DocsID=1570217.

62. Воры проникли в компьютерную сеть Национального банка // Голос Украины. – 1998. – № 217 (1963). – С. 3.

63. Гавловський, В.Д. Щодо проблем боротьби із злочинами, що вчинюються з використанням комп'ютерних технологій / В.Д. Гавловський, В.С. Цимбалюк //Уряду України. Президенту, законодавчій, виконавчій владі. "Боротьба з контрабандою: проблеми та шляхи їх вирішення": Аналітичні розробки, пропозиції наукових і практичних працівників [керівн. авт. кол. А.І. Комарова, О.О. Крикун]. – К., 1998. – С. 148 – 154.

64. Гавриленко І. Комп'ютерна злочинність // Юридичний вісник України. – 1997. – № 28. – С. 4.

65. Гавриш, С.Б. Криминализация экологических деликтов: оптимальная модель / С.Б. Гавриш // Проблеми держави і права: тематичний збірник наукових праць. – К.: УМКВО, 1992. – С. 96 – 103.

66. Галковська, Т. Всі пішли в онлайн! "Дикий" ринок електронної комерції планують поставити в чіткі законодавчі рамки [Електронний ресурс] / Т. Галковська // Дзеркало тижня. – 2010. – № 16. – Режим доступу: http://dt.ua/articles/59943

67. Гальперин, И.М. Наказание: социальные функции, практика применения / И.М. Гальперин. – М. : Юрид. лит., 1983. – 206 с.

68. Гилстер, П. Новый Навигатор Internet / Пол Гилстер. – К. : Диалектика, 1996. – 496 с.

69. Гнатенко, Е.А. Понятие общественной опасности: философский и правовой подходы / Е.А. Гнатенко // Практична філософія та правовий порядок: [збірка наукових статей]. – Х. : Центр Освітніх Ініціатив, 2000. – С. 195 – 196.

70. Голубєв, В.О. Правові проблеми захисту інформаційних технологій / В.О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35 – 40.

71. Горбулін, В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок; Інститут проблем національної безпеки. – К. : Інтертехнологія. – 2009. – 136 с.

72. Горпинюк, О.П. Кримінально-правова охорона інформаційного аспекту приватності в Україні [Текст] : автореф.

дис. ... канд. юрид. наук : 12.00.08 / Горпинюк О.П. ; Львів. держ. ун-т внутр. справ. – Л., 2011. – 19 с.

73. Гриців, М.І. Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / М.І. Гриців, В.В. Антощук [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу : http://www.scourt.gov.ua/

74. Грищук, В.К. До питання про соціальну зумовленість кримінальної відповідальності за суспільно небезпечні діяння у сфері господарської діяльності / В.К. Грищук // Відповідальність за злочини у сфері господарської діяльності : матер. наук.-практ. конференції / Ред. кол.: В.В. Сташис (голов. ред.) та ін. – Х. : Кроссроуд, 2006. – С. 15 – 18.

75. Грищук, В.К. Проблеми кодифікації кримінального законодавства України / В.К. Грищук. – Львів : 1993. – 137 с.

76. Гулкевич, В. Д. Кримінально-правова охорона авторського права і суміжних прав: дис. ... канд. юрид. наук : 12.00.08 / Гулкевич Володимир Дмитрович ; Львів. нац. ун-т ім. І. Франка. – Л., 2008. – 218 арк.

77. Гуторова, Н.О. Проблеми кримінально-правової охорони державних фінансів України: дис. ... д-ра юрид. наук: 12.00.08 / Наталія Олександрівна Гуторова; [Національний ун-т внутрішніх справ]. – Х., 2001. – 459 с.

78. Гуцалюк, М. Координація боротьби з комп'ютерною злочинністю / М.В. Гуцалюк // Право України. – 2002. – № 5. – С. 121 – 126

79. Гуцалюк, М.В. Інформаційна безпека України: нові загрози та організація протидії / М.В. Гуцалюк // Правова інформатика. – 2004. – № 3. – С. 39 – 43.

80. Данилов-Данильян, В. Что может и чего не может рыночная экономика / В. Данилов-Данильян, И. Рейф // Наука и жизнь. – 2010. – № 9. – С. 2 – 8.

81. Даніл'ян, В.О. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз): автореф. дис... канд. філос. наук : 09.00.03 / Вадим Олегович

Даніл'ян ; [Харківський ун-т повітряних сил ім. Івана Кожедуба]. – Х., 2006. – 19 с.

82. Дем'яненко, Ю.І. Кримінальна відповідальність за порушення недоторканності приватного життя : дис. ... канд. юрид. наук : 12.00.08 / Дем'яненко Ю.І. ; Нац. юрид. акад. України ім. Ярослава Мудрого. – Х., 2008. – 215 арк. – Бібліогр. : С. 199 – 215.

83. Денисов Д. Информационная "вскрытность"/ Дмитрий Денисов [Электронный ресурс] // Российское разведывательное агентство "Разведка в сфере бизнеса". – 10.07.2006. – Режим доступа : http://www.a-rsb.ru/index.php?go=News&in=view&id=197\\

84. Дмитренко, М.А. Політична система України: розвиток в умовах глобалізації та інформаційної революції / М.А. Дмитренко; Національний педагогічний університет імені М.П. Драгоманова, Інститут оперативної діяльності та державної безпеки. – К. : Знання України, 2008. – 544 с.

85. Дорош, Л.В. Теоретико-прикладні проблеми якості кримінального законодавства України / Л.В. Дорош // Питання боротьби зі злочинністю : зб. наук. пр. / редкол.: В.І. Борисов та ін. – Х. : Право, 2009. – Вип. 18. – С. 15 – 44.

86. Дрьомов, С. Комп'ютерна інформація як предмет злочину, передбаченого ст. 362 Кримінального кодексу України / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 4. – С. 129 – 132.

87. Дрьомов, С. Кримінально-правова характеристика перехоплення комп'ютерної інформації як форми об'єктивної сторони злочину, передбаченого статтею 362 КК України / С. Дрьомов // Юридичний журнал. – 2006. – № 6. – С. 54 – 56.

88. Дрьомов, С. Несанкціоноване знищення інформації як форма об'єктивної сторони складу злочину, передбаченого ст. 362 КК України / С. Дрьомов, Т. Рендель // Вісник прокуратури. – 2006. – № 9 (63). – С. 90 – 94.

89. Дрьомов, С. Сутність копіювання як форми несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої

інформації / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 9.– С. 144 – 147.

90. Дрьомов, С. Умисел при вчиненні несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК України) / С. Дрьомов // Підприємництво, господарство і право. – 2005. – № 7. – С. 115 – 119.

91. Дубов, Д. Інформаційна безпека в умовах впровадження електронного урядування / Д. Дубов // Вісник книжкової палати. – 2006. – № 7. – С. 34 – 38.

92. Дюжев, Д.В. Інформаційне суспільство: соціально-правова парадигма суспільного розвитку : автореф. дис. ... канд. філос. наук : 09.00.03 / Дмитро Володимирович Дюжев ; [Донецький національний університет]. – Донецьк, 2004. – 18 с.

93. Еременко Ю. Диплом юриста хакеру не помеха / Ю. Еременко // Луганская правда. – 2007. – № 16. – С. 3.

94. Єрмоленко, А.М. Комунікативна практична філософія / А.М. Єрмоленко. – К. : Лібра, 1999. – 488 с.

95. Жалинский А.Э. Уголовное право в ожидании перемен : теоретико-инструментальный анализ / Альфред Эрнестович Жалинский. – М. : Проспект, 2008. – 400 с.

96. Жданова, И. Кто остается на обочине "Украинского прорыва"? [Электронный ресурс] / И. Жданова // Зеркало недели. – 2008. – № 6. – Режим доступу: http://zn.ua/articles/52782

97. Задорожня, Л. Щодо законодавчого врегулювання деяких аспектів прав громадян на інформацію / Л. Задорожня // Правова інформатика. –2005. – № 1. – С. 7 – 18.

98. Закон України "Про внесення змін до деяких законодавчих актів України щодо гуманізації відповідальності за правопорушення у сфері господарської діяльності" від 15 листопада 2011 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/4025-17

99. Закон України "Про державну службу спеціального зв'язку та захисту інформації України" від 23.02.2006 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3475-15

100. Закон України "Про державну таємницю" від 21.01.1994 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3855-12

101. Закон України "Про доступ до судових рішень" від 22.12.2005 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3262-15

102. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/80/94-вр

103. Закон України "Про інформацію" від 02.11.1992 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

104. Закон України "Про національну програму інформатизації" від 04.02.1998 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=74%2F98-%E2%F0

105. Закон України "Про страхування" від 07.03.1996 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=85%2F96-%E2%F0

106. Закон України "Про телекомунікації" від 18.11.2003 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280-15

107. Засновник WikiLeaks продав право на автобіографію за $1,5 млн [Електронний ресурс] // NEWSru.com. – 26.12.2010. – Режим доступу : http://newsru.com/world/ 26dec2010/psd.html.

108. Згуровський, М.З. Загальні тенденції розвитку інформаційного суспільства у глобальному контексті: трансформації світового устрою / М.З. Згуровський // Інформаційне суспільство. Шлях України. – К., 2004. – С. 104 – 114.

109. Зернецкая, О. Интернет-ловушка для молодежи [Электронный ресурс] / О. Зернецкая // Зеркало недели. – 2007. – № 11. – Режим доступу : http://zn.ua/articles/49507

110. Зинченко, Н.И. Обеспечение безопасности личности, общества и государства: концептуально-теоретический аспект / Н.И. Зинченко // Социально-гуманитарное знание. – 2006. – № 6. – С. 175 – 188.

111. Иванов, А.Г. Нужны ли "мертвые" нормы в уголовном праве / А.Г. Иванов // Советское государство и право. – 1988. – № 9. – С. 89 – 90.

112. Иноземцев, В.Л. Расколотая цивилизация: системные кризисы индустриальной эпохи / В.Л. Иноземцев // Вопросы философии. – 1999. – № 5. – С. 3 – 18

113. Ільченко, С.Ю. Проблемний аспект кваліфікації діяння за ознаками складу злочину, передбаченого ст. 361-1 Кримінального кодексу України / С.Ю. Ільченко // Кримінальне право України. – 2006. – № 5.– С. 11 – 18.

114. Кадченко, В. В Киеве злоумышленники установили в торговом центре фальшивый банкомат / Виталий Кадченко [Электронный ресурс] // Официальный сайт Первого канала. – 18.01.2011. – Режим доступа : http://www.1tv.ru/news/world/169103

115. Калининградский хакер украл 2 млн руб. из банков Ростова, Махачкалы и Екатеринбурга [Электронный ресурс] // REGNUM-Балтика. – 13.01.2011. – Режим доступа : http://www.newspb.ru/allnews/1364286/

116. Калмыков, Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : дис. ... канд. юрид. наук: 12.00.08 / Дмитрий Александрович Калмыков. – Ярославль, 2005. – 219 с.

117. Калюжный, Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) :

автореф. дис. … д-ра юрид. наук: 12.00.02 / Ростислав Андреевич Калюжный ; [АН Украины, Институт государства и права им. В.М. Корецкого]. – К., 1992. – 47 с.

118. Камлюк В. Ботнеты / Виталий Камлюк [Электронный ресурс] // Лаборатория Касперского. – Режим доступа : http://www.securelist.com/ru/analysis?pubid=204007610

119. Карчевский, Н.В. Проблемы гармонизации украинского и международного законодательства о компьютерных преступлениях / Н.В. Карчевский [Электронный ресурс] // Официальный сайт Центра исследования компьютерной преступности. – Режим доступа : http://www.crime-research.ru/articles/karchevsky08

120. Карчевський, М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж: монографія / М.В. Карчевський ; МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; [Наук. ред. Л.М. Кривоченко]. – Луганськ: РВВ ЛАВС, 2002. – 144 с.

121. Карчевський, М.В. Проблеми гармонізації українського та міжнародного законодавства про комп'ютерні злочини / М.В. Карчевський // Вісник Луганського державного університету внутрішніх справ. – 2005. – № 4. – С. 122 – 133.

122. Касперський, І. Суспільна значимість як підстава поширення інформації з обмеженим доступом / І. Касперський, А. Марущак // Право України. – 2006. – № 4. – С. 107 – 110.

123. Кастельс, М. Информационная эпоха: экономика, общество и культура / Мануэль Кастельс [Электронный ресурс] // Библиотека Гумер. – Режим доступа : http://www.gumer.info/bibliotek_Buks/Polit/kastel/09.php.

124. Кендюхов, О. Суспільство споживання як національна трагедія України [Електронний ресурс] / О. Кендюхов // Дзеркало тижня. – 2011. – № 1. – Режим доступу: http://dt.ua/articles/73290

125. Кибератака на информационные сети государственных структур [Электронный ресурс]// Новости сайта

Центра исследования компьютерной преступности. – 16.04.2009. – Режим доступа : http://www.crime-research.ru/news/16.04.2009/5797/

126. Киберпреступность страшнее финансового кризиса [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 03.12.2008. – Режим доступа : http://www.crime-research.ru/news/03.12.2008/5056/

127. Киви, Б. В Боевой червь Stuxnet / Берд Киви [Электронный ресурс] // Компьютерра-Онлайн. – 29.09.2010. – Режим доступа : http://www.computerra.ru/own/kiwi/565316/?n

128. Китай: в стране жертвой Stuxnet стали около 1000 предприятий [Электронный ресурс] // CyberSecurity. – 30.09.2010. – Режим доступа : http://www.cybersecurity.ru/crypto/104229.html

129. Книженко, О.О. Санкції у кримінальному праві : монографія / О.О. Книженко. – Х. : НікаНова, 2011. – 336 с.

130. Коваленко, В. Сучасна масова комунікація: носій добра чи криміногенний фактор? / В. Коваленко // Право України. – 2008. – № 4. – С. 84 – 89.

131. Козубський, В.О. Інформаційна безпека держави: Кримський регіон : автореф. дис. … канд. політ. наук: 23.00.02 / Валентин Олексійович Козубський ; [Таврійський національний університет ім. В.І. Вернадського] – Сімферополь, 2005. – 19 с.

132. Колодій, І.М. Інформаційна безпека: деякі проблеми визначення поняття / І.М. Колодій // Держава і право. – 2008. – Вип. 40. – С. 300 – 305.

133. Колодюк, А.В. Інформаційне суспільство: сучасний стан та перспективи розвитку в Україні : дис. … канд. політ. наук: 23.00.03 / А.В. Колодюк ; [Київський національний ун-т ім. Тараса Шевченка; Інститут журналістики]. – К., 2004. – 234 с.

134. Колодюк, А.В. Цифровий розподіл – нова форма соціального розмежування в умовах глобалізації / А.В. Колодюк // Вісник державної Академії керівних кадрів культури. – 2004. – № 4. – С. 124 – 129.

135. Компьютерные преступления: их предупреждение и выявление [Текст] : учеб. пособие для студ. вузов / В.Ю. Захарченко [и др.]. – Изд. 2-е перераб., доп. – Донецк, 2008. – 204 с.

136. Компьютерные террористы: новейшие технологии на службе преступного мира / [авт.-сост. Т.И. Ревяко]. – Минск : Литература, 1997. – 640 с.

137. Комюніке секретаря Європейського суду з прав людини стосовно рішення у справі "Сегерштед-Віберг та інші проти Швеції" / Європейський суд з прав людини // Юридична Україна. – 2006. – № 10. – С. 99 – 103.

138. Конах, В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США) : автореф. дис. … канд. політ. наук: 21.01.01 / Вікторія Костянтинівна Конах [Національний інститут стратегічних досліджень]. – К., 2005. – 20 с.

139. Копырюлин, А.Н. Квалификация неправомерного доступа к компьютерной информации / А.Н. Копырюлин // Уголовный процесс. – 2007. – № 11. – С. 3 – 7.

140. Коржанський, М.Й. Проблеми кримінального права : монографія / М.Й. Коржанський. – Дніпропетровськ: Юрид. акад. МВС, 2003. – 200 с.

141. Кормич, Б.А. Інформаційна безпека: організаційно-правові основи : навч. посібн. / Борис Анатолійович Кормич. – К.: Кондор, 2004. – 384 с.

142. Кормич, Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук: 12.00.07 / Борис Анатолійович Кормич. – Одеса, 2004. – 427 с.

143. Кормич, Б.А. Функція держави щодо захисту інформаційної безпеки / Б. А. Кормич // Держава і право. – 2002. – Вип. 18. – С. 103 – 108.

144. Коробеев, А.И. Советская уголовно-правовая политика: проблемы криминализации и пенализации : монография / А.И. Коробеев. – Владивосток : Издательство Дальневосточного университета, 1987. – 270 с.

145. Котляр, А. Україна посідає місце [Електронний ресурс] / А. Котляр // Дзеркало тижня. – 2011. – № 29. – Режим доступу : http://dt.ua/articles/86389

146. Красненкова, Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами : дис. ... канд. юрид. наук: 12.00.08 / Е.В. Красненкова. – М., 2006. – 188 с.

147. Кривоченко, Л.Н. Классификация преступлений / Людмила Николаевна Кривоченко. – Х. : Вища школа. – 1983. – 129 с.

148. Кримінальна справа № 1-714/09 // Архів Київського районного суду м. Харкова.

149. Кримінальна справа № 1-79/2010 // Архів Переяслав-Хмельницького міськрайонного суду Київської області.

150. Кримінальна справа № 1-0473/2008 // Архів Павлоградського міськрайонного суду Дніпропетровської області.

151. Кримінальна справа № 1-101/10 // Архів Іванівського районного суду Херсонської області.

152. Кримінальна справа № 1-101/2009 // Архів Миколаївського районного суду Львівської області.

153. Кримінальна справа № 1-103/2010 // Архів Крюківського районного суду м. Кременчука Полтавської області.

154. Кримінальна справа № 1-133/10 // Архів Ленінського районного суду м. Кіровограда.

155. Кримінальна справа № 1-154/2008 // Архів Голованівського районного суду Кіровоградської області.

156. Кримінальна справа № 1-156/08 // Архів Голованівського районного суду Кіровоградської області.

157. Кримінальна справа № 1-162/2009 // Архів Корольовського районного суду м. Житомира.

158. Кримінальна справа № 1-1918/2010 // Архів Приморського районного суду м. Одеси.

159. Кримінальна справа № 1-200/2010 // Архів Прилуцького міськрайонного суду Чернігівської області.

160. Кримінальна справа № 1-221/2008 // Архів Сарненського районного суду Рівненської області.

161. Кримінальна справа № 1-222/2010 // Архів Центрально-Міського районного суду м. Макіївки Донецької області.

162. Кримінальна справа № 1-223/07 // Архів Придніпровського районного суду м. Черкаси.

163. Кримінальна справа № 1-232/10 // Архів Червонозаводського районного суду м. Харкова.

164. Кримінальна справа № 1-235/2008 // Архів Першотравневого районного суду м. Чернівці.

165. Кримінальна справа № 1-326/2008 // Архів Дергачевського районного суду Харківської області.

166. Кримінальна справа № 1-378/2008 // Архів Крюківського районного суду м. Кременчука Полтавської області.

167. Кримінальна справа № 1-39/2008 // Архів Жидачівського районного суду Львівської області.

168. Кримінальна справа № 1-395/10 // Архів Приморського районного суду м. Одеси.

169. Кримінальна справа № 1-43/09 // Архів Кіровського районний суд м. Кіровограда.

170. Кримінальна справа № 1-468/11 // Архів Святошинського районного суду м. Києва.

171. Кримінальна справа № 1-502/10 // Архів Джанкойського міськрайонного суду Автономної республіки Крим.

172. Кримінальна справа № 1-555/11 // Архів Новомосковського міськрайонного суду Дніпропетровської області.

173. Кримінальна справа № 1-56/2007 // Архів Косівського районного суду Івано-Франківської області.

174. Кримінальна справа № 1-569/09 // Архів Соснівського районного суду м. Черкаси.

175. Кримінальна справа № 1-57/08 // Архів Кіровського районний суд міста Кіровограда.

176. Кримінальна справа № 1-670/2010 // Архів Суворовського районного суду м. Одеси.

177. Кримінальна справа № 1-738/2007 // Архів Рівненського міського суду Рівненської області.

178. Кримінальна справа № 1-740/10 // Архів Соснівського районного суду м. Черкаси.

179. Кримінальна справа № 1-77/2011 // Архів Куп'янського міськрайонного суду.

180. Кримінальна справа № 1-789/10 // Архів Ленінського районного суду м. Луганська.

181. Кримінальна справа № 1-81/2007 // Архів Корольовського районного суду м. Житомира.

182. Кримінальна справа №1-196/10 // Архів Авдіївського міського суду Донецької області.

183. Кримінальна справа №1-204/2011 // Архів Бахчисарайського районного суду Автономної Республіки Крим.

184. Кримінальна справа №1-296/2008 // Архів Харцизького міського суду Донецької області.

185. Кримінальна справа №1-299/11 // Архів Свердловського міського суду Луганської області.

186. Кримінальна справа №1-543/10 // Архів Калінінського районного суду м. Донецька.

187. Кримінальна справа №1-809/2010 // Архів Тернопільського міськрайонного суду Тернопільської області.

188. Кримінальне право України. (Особлива частина) : підручник / Кол. авторів А. В. Байлов, О.А. Васильєв, О.О. Житний та ін..; за заг. ред. О.М. Литвинова; наук. ред. серії О.М. Бандурка. – Х. : Вид-во ХНУВС, 2011. – 572 с.

189. Кримінальне право України. (Особлива частина) : підручник / Кол. авторів А.В. Байлов, О.А. Васильєв, О.О. Житний, та ін..; за заг. ред. О.М. Литвинова; наук. ред. серії О.М. Бандурка. – Х. : ХНУВС, 2011. – 572 с.

190. Кримінальне право України. Загальна частина: підруч. для студ. вищ. навч. закл. / Ю.В. Баулін, В.І. Борисов, Л.М. Кривоченко, В.А. Ломако, М.І. Панов, В.В. Сташис, В.Я. Тацій, В.П.Тихий, В.І. Тютюгін; [за ред. проф. В. В. Сташиса, В.Я. Тація] ; Нац. юрид. акад. України ім. Ярослава Мудрого ; 4-е вид., перероб. і допов. – Х. : Право, 2010. – 456 с.

191. Кримінальне право України. Особлива частина: підруч. для студ. вищ. навч. закл. / Г.М. Анісімов, Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш, С.В. Гізімчук, Ю.В. Гродецький, Н.О. Гуторова, Л.В. Дорош, І.О. Зінченко, В.І. Касинюк; [за ред. проф. В.В. Сташиса, В.Я. Тація] ; Нац. юрид. акад. України ім. Ярослава Мудрого ; 4-е вид., перероб. і допов. – Х. : Право, 2010. – 606 с.

192. Кримінальне право України: Особлива частина : підруч. / За заг. ред. Є.Л. Стрельцова – Х.: Одіссей, 2009. – 496 с.

193. Кримінальний кодекс України: Науково-практичний коментар / Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш та ін.; За заг. ред. В.В. Сташиса, В.Я. Тація. – К. : Ін Юре, 2003. – 1196 с.

194. Кримінальний кодекс України : Науково-практичний коментар / Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш та ін. ; За заг. ред. В.В. Сташиса, В.Я. Тація. – Вид. 4-е, допов. – Х.: ТОВ "Одіссей", 2008. – 1208 с.

195. Кузина, С. Интернет съедает наш мозг / С. Кузина // Комсомольская правда в Украине. – 2009. – 20 января. – С. 15.

196. Кузнецов, Н.А. Информационное взаимодействие как объект научного исследования / Н.А. Кузнецов, Н.Л. Мусхелишвили, Ю.А. Шрейдер // Вопросы философии. – 1999. – № 1. – С. 77 – 87.

197. Кузнецова, Н.Ф. Значение преступных последствий для уголовной ответственности / Нинель Федоровна Кузнецова. – М. : Государственное издательство юридической литературы, 1958. – 219 с.

198. Кураков, Л.П. Информация как объект правовой защиты / Л.П. Кураков, С.Н. Смирнов. – М. : Гелиос АРВ, 1998. – 239 с.

199. Курушин, В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М. : Новый Юрист, 1998. – 256 с.

200. Кушакова-Костицька, Н.В. Проблемні питання законодавчого регулювання спаму згідно з кримінальним законодавством України / Н.В. Кушакова-Костицька // Кримінальний кодекс України 2001 р.: проблеми застосування і перспективи удосконалення. Прогалини у кримінальному законодавстві. Міжнародний симпозіум, 12 – 13 вересня 2008 року. Тези і реферати доповідей, тексти повідомлень. – Львів, 2008. – С. 108 – 112.

201. Лаборатория PandaLabs опубликовала отчет о результатах расследования ситуации на черном IT-рынке [Электронный ресурс] // ITnews – Новости Информационных Технологий. – 25.01.2011. – Режим доступа : http://itnews.com.ua/58666.html

202. Лазарев, А.Ю. Проблемы формирования информационного общества в России / А.Ю. Лазарев // Информационное право. – 2008. – № 3. – С. 8 – 9.

203. Лайон, Д. Інформаційне суспільство: проблеми та ілюзії / Д. Лайон // Сучасна зарубіжна соціальна філософія. – К., 1996. – С. 362 – 380.

204. Лащук, Є.В. Предмет злочину в кримінальному праві України : автореф. дис. ... канд. юрид. наук: 12.00.08 / Лащук Єфрем Вікторович ; Національна академія внутрішніх справ України. – К., 2005. – 20 с.

205. Левашова, Ю. Компания "Доктор Веб" подвела итоги борьбы с киберпреступностью / Юлия Левашова [Электронный ресурс] // Официальный сайт Центра исследования компьютерной преступности. – 06.12.2010. – Режим доступа: http://www.crime-research.ru/news/06.12.2010/7028/

206. Левашова, Ю. СБУ Украины завершила спецоперацию по пресечению группировки кибермошенников / Юлия Левашова [Электронный ресурс] // Официальный сайт Центра исследования компьютерной преступности. – 24.10.2010. – Режим доступа: http://www.crime-research.ru/news/24.10.2010/6986/

207. Левашова, Ю. В Евросоюзе стремительно растет уровень киберпреступности / Юлия Левашова [Электронный ресурс] // Официальный сайт Центра исследования

компьютерной преступности. – 12.01.2011. – Режим доступа : http://www.crime-research.ru/news/12.01.2011/7066/

208. Лихова, С. Актуальні питання вдосконалення кримінально-правових норм, спрямованих на захист недоторканності приватного життя (статті 162, 163, 182 Кримінального кодексу України) / С. Лихова // Підприємництво, господарство і право. – 2005. – № 7. – С. 98 – 104.

209. Лихова, С.Я. Злочини проти громадянських, політичних та соціальних прав і свобод людини і громадянина за Кримінальним кодексом України (теоретико-правове дослідження) : дис... д-ра юрид. наук: 12.00.08 / Лихова С. Я. ; Київський національний ун-т ім. Тараса Шевченка. – К., 2006. – 29 с. – С. 416 – 471.

210. Ліпкан, В.А. Адміністративно-правові основи забезпечення національної безпеки України: автореф. дис. … д-ра юрид. наук: 12.00.07 / Володимир Анатолійович Ліпкан ; [Київський національний університет внутрішніх справ]. – К., 2008. – 34 с.

211. Ліпкан, В.А. Національна безпека України: кримінально-правова охорона : навч. посіб. / Ліпкан В.А., Діорділа І.В. – К.: КНТ, 2007. – 292 с.

212. Лісовий, В. "Комп'ютерні" злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86 – 88.

213. Логвиненко, Н.Ф. Современные методы и средства защиты компьютерной информации от утечки по электрическим каналам / Н.Ф. Логвиненко, С.Л. Емельянов, В.В. Носов, В.И. Писаревский // Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвузівської науково-практичної конференції (22 грудня 2000 року). – Донецьк : Донецький інститут внутрішніх справ, 2001. – С. 190 – 199.

214. Лопатин, В.Н. Актуальные проблемы становления и развития теории информационного права / В.Н. Лопатин // Информационное право. – 2005. – № 3. – С. 4 – 7.

215. Лопатин, В.Н. Информационная безопасность России : дис. … д-ра юрид. наук: 12.00.01 / В.Н. Лопатин. – СПб., 2000. – 436 с.

216. Лопатин, В.Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации: Проект / В.Н. Лопатин. – М. : Издание Государственной Думы, 1998. – 159 с.

217. Лопашенко, Н.А. Основы уголовно-правового воздействия: уголовное право, уголовный закон, уголовно-правовая политика / Н.А. Лопашенко. – СПб. : Юридический центр Пресс, 2004. – 329 с.

218. Лужецький, В.А. Інформаційна безпека : навч. посіб. / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця : УНІВЕРСУМ – Вінниця, 2009. – 240 с.

219. Лукина, Н.П. Информационное общество: состояние и перспективы социально-философского исследования / Н.П. Лукина [Электронный ресурс] // Открытый междисциплинарный электронный журнал "Туманитарная информатика". – № 1. – Режим доступа : http://huminf.tsu.ru/e-jurnal/magazine/1/lukina.htm.

220. Мазуренко, О. Комп'ютерна інформація, як предмет злочинів, передбачених Розділом XVI КК України / О. Мазуренко, Н. Розенфельд // Право України. – 2004. – № 6. – С. 80 – 83.

221. Макаренко, Є.А. Проблема безпеки в інформаційному суспільстві / Є.А. Макаренко // Інформаційне суспільство. Шлях України. – К., 2004. – С. 177 – 185.

222. Малько, А.В. Эффективность правового регулирования / А.В. Малько // Правоведение. – 1990. – № 6. – С. 61 – 67.

223. Мальковская, И.А. Профиль информационно-коммуникативного общества (обзор зарубежных теорий) / И.А. Мальковская // Социологические исследования. – № 2. – 2007. – С. 76 – 85.

224. Маруховський, О.О. Політичні аспекти зарубіжних концепцій інформаційного суспільства : автореф. дис. ... канд. політ. наук: 23.00.01 / Маруховський Олег Олександрович ; [НАН України; Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса]. – К., 2008. – 20 с.

225. Марущак, А. До питання про забезпечення безпеки інформаційного простору та інформаційних ресурсів / А. Марущак // Юридичний радник. – Х., 2009. – № 4. – С. 64 – 67.

226. Марущак, А. Зміст поняття "забезпечення доступу до інформації" / А. Марущак //Право України. – 2008. – № 5. – С. 99 – 104.

227. Марущак, А.І. Інформаційне право: доступ до інформації : навч. посіб. для студ. ВНЗ / А.І. Марущак. – К.: КНТ, 2007. – 531 с.

228. Марущак, А.І.Визначення поняття "доступ до інформації" / А.І. Марущак // Правова інформатика. – 2006. – № 3. – С. 69 – 75.

229. Матеріали круглого столу "Інформаційна безпека України: сутність та проблеми", Київ, червень 1998 року [Електронний ресурс] // Офіційний сайт Національного інституту стратегічних досліджень. – Режим доступу : http//www.niss.gov.ua/book/panorama/index.htm

230. Мей К. Інформаційне суспільство: скептичний погляд / К. Мей ; пер. М. Войцицька. – К.: К.І.С., 2004. – 220 с.

231. Мельник, О.М. Цивільно-правова охорона інтелектуальної власності в Україні : дис. ... д-ра юрид. наук: 12.00.03. / О.М. Мельник ; Національний університет внутрішніх справ. – Х., 2004. – 403 с. – Бібліогр.: С. 372 – 403. – С. 34.

232. Миколенко, О.М. Теоретичні основи дослідження шкоди, заподіяної злочином : дис... канд. юрид. наук: 12.00.08 / Олена Миколаївна Миколенко ; Одеський національний ун-т ім. І.І. Мечникова. – Одеса, 2005. – 220 с.

233. Мироненко, В. Хакеры отключили "Аэрофлот" от платежной системы / Владимир Мироненко [Электронный ресурс] // 3DNews – Daily Digital Digest. – 20.07.2010. – Режим доступа : http://www.3dnews.ru/news/Hakeri-otklyuchili-Aeroflot-ot-platezhey

234. Михеева, М.Р. Проблема правовой защиты персональных данных / М.Р. Михеева [Электронный ресурс] // Владивостокский центр исследования организованной

преступности. – Режим доступа : http://www.crime.vl.ru/index.php?p=1115&more=1&c=1&tb=1&pb=1.

235. Міхайліна,Т.В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : автореф. дис. … канд. юрид. наук: 12.00.08 / Тетяна Вікторівна Михайліна ; [Державний науково-дослідний інститут МВС України]. – К., 2011. – 20 с.

236. Музика, А.А. Законодавство про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення / А.А. Музика, Д.С. Азаров. – К. : Вид. Паливода А.В., 2005. – 118 с.

237. Музика, А.А. Кримінально-правові ризики: постановка наукової проблеми / А.А. Музика // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13 – 14 жовтня 2011 р. / редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 98 – 103.

238. На долю общепита пришлось наибольшее количество проникновений в 2010 году [Электронный ресурс] // Хакер.ru. – 21.01.2011. – Режим доступа : http://www.xakep.ru/post/54587/default.aspt

239. На тесте по математике каждый третий не справился с теоремой Пифагора [Электронный ресурс] // Комсомольская правда в Украине. – 29.07.2011 – Режим доступа : http://kp.ua/daily/ 290711/293003/

240. Набруско, В. Станет ли Украина хозяином в собственном информационном пространстве? [Электронный ресурс] / В. Набруско // Зеркало недели. – 2008. – № 34. – Режим доступа : http://zn.ua/articles/54742

241. Навроцький, В.О. Основи кримінально-правової кваліфікації: навчальний посібник / В.О. Навроцький. – К. : Юрінком Інтер, 2006. – 704 с.

242. Навроцький, В.О. Спеціальні і казуїстичні кримінально-правові норми та прогалини у кримінальному законі / В.О. Навроцький // Кримінальний кодекс України 2001 р.: проблеми застосування і перспективи удосконалення. Прогалини у кримінальному законодавстві. Міжнародний симпозіум, 12 – 13 вересня 2008 року. Тези і реферати доповідей, тексти повідомлень. – Львів, 2008. – С. 132 – 136.

243. Нагорна, Л. Символічний простір інформаційного суспільства: зорові аберації віртуальності / Л. Нагорна // Політичний менеджмент. – № 2. – 2009. – С. 3 – 11.

244. Назаренко, С. Інформаційно-психологічна безпека в політиці / С. Назаренко // Віче. – К., 2003. – № 2. – С. 47 – 50.

245. Назаров, М.М. Средства массовой коммуникации и российское общество на пороге XXI века / М.М. Назаров // Социально-гуманитарные знания. – 1999. – № 5. – С. 11 – 21.

246. Наказ Міністерства аграрної політики України "Про організаційні заходи щодо захисту інформації з обмеженим доступом" від 11 грудня 2002 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

247. Наказ Міністерства аграрної політики України "Про організацію роботи з технічного захисту інформації в Міністерстві аграрної політики України" від 16 серпня 2000 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

248. Наказ Міністерства економіки та з питань європейської інтеграції України "Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства" від 23 квітня 2002 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

249. Наказ Міністерства фінансів України "Про забезпечення захисту інформації шляхом обмеження доступу до приміщень, у яких розміщене серверне та комутаційне обладнан-

ня" від 20 липня 2004 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

250. Наказ Міністерства фінансів України "Про затвердження Положення про роботу із засобами обчислювальної техніки та про доступ до інформаційних ресурсів Міністерства фінансів України" від 1 квітня 2003 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

251. Науково-практичний коментар до Кримінального кодексу України / За ред. М.І. Мельника, М.І. Хавронюка. – 8-е вид., перероб. і доп. – Х. : Фактор, 2011. – 1280 с.

252. Нерсесян, А.С. Кримінально-правова охорона прав інтелектуальної власності: дис. ... канд. юрид. наук: 12.00.08 / Нерсесян Армен Сабірович ; НАН України, Інститут держави і права ім. В.М. Корецького. – К., 2008. – 208 с.

253. Новая философская энциклопедия: в 4 т. / Ин-т философии РАН; Нац. обществ.-науч. фонд; Предс. науч.-ред. совета В.С. Степин [Электронный ресурс] // Официальный сайт Института философии РАН. – Режим доступа : http://iph.ras.ru/elib/1431.html

254. Орлов, С.О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах: дис. ... канд. юрид. наук: 12.00.08 / С.О. Орлов [Національний університет внутрішніх справ]. – Х., 2004. – 213 с.

255. Орлов, Ю.Ю. Реалізація вимог міжнародної Конвенції про кіберзлочинність у законодавстві України / Ю.Ю. Орлов // Науковий вісник Національної академії внутрішніх справ. – 2011. – № 6. – С. 3 – 9.

256. Основания уголовно-правового запрета. Криминализация и декриминализация / П.С. Дагель, Г.А. Злобин, С.Г. Келина, Г.Л. Кригер и др. ; [под ред. В.Н. Кудрявцева и А.М. Яковлева] – М. : Наука, 1982. – 304 с.

257. Особливості піратства в Україні [Електронний ресурс] // Zaxid.NET. – 17.03.2010. – Режим доступу : http://zaxid.net/home/showSingleNews.do?osoblivosti_piratstva_v_ukrayini&objeobje=1098424

258. Павликова, М.М. Парадоксы информационного общества / М.М. Павликова // Вестник Московского государственного университета. – Сер. 10. Журналистика. – № 1. – 2008. – С. 82 – 91.

259. Пазюк, А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: дис. ... канд. юрид. наук: 12.00.11 / Пазюк Андрій Валерійович ; Київський національний ун-т ім. Тараса Шевченка. – К., 2004. – 205 с.

260. Панарин, И. Технология информационной войны / И. Панарин. – М.: КСП+, 2003. – 319 с.

261. Панченко, П.Н. Уголовно-правовые вопросы криминализации общественно опасных деяний / П.Н. Панченко // Актуальные проблемы криминализации и декриминализации общественно опасных деяний. Сборник научных трудов. – Омск, 1980. – С. 3 – 16.

262. Паньо Е.М. Сито со слишком большими дырочками [Электронный ресурс] / Е. Паньо, Т. Паньо // Зеркало недели. – 2006. – № 24. – Режим доступу : http://zn.ua/articles/47040

263. Пархоменко, О.В. Інформаційно-знаннєве суспільство: проблеми, особливості / О. В. Пархоменко // Науково-технічна інформація. – 2010. – № 1. – С. 3 – 6.

264. Першиков, В.И. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков. – М.: Финансы и статистика, 1991. – 543 с.

265. Петров, С.А. Особенности квалификации хищений, совершенных с использованием компьютерной техники / С.А. Петров // Российский следователь. – 2008. – № 15. – С. 22 – 24.

266. Петрова, Н. Норма запретительная превращается в... разрешительную / Н. Петрова [Электронный ресурс] // Официальный сайт еженедельника "2000". – Режим доступа : http://2000.net.ua/2000/forum/38095.

267. Пинаев, А.А. Уголовно-правовая борьба с хищениями / А.А. Пинаев. – Х. : Вища школа, 1975.

268. Плетнева, Д.А. О реализации принципа индивидуализации ответственности при построении санкций квалифицирующих составов / Плетнева Д.А. // Держава і право: проблеми становлення і стратегія розвитку: зб. матеріалів міжнар. наук.-практ. конф., 15 – 16 травня 2010 року / Сумська філія Харківського національного університету внутрішніх справ. – Суми: ФОП Ляпощенко Л.Г., 2010. – С. 241 – 244.

269. Плохой І.І. Поняття громадського порядку / І.І. Плохой // Форум права. – 2009. – № 3. – С. 500 – 505 [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2009-3/09piipgp.pdf, с. 504

270. Плугатир М.В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук: 12.00.08 / Плугатир Максим Віталійович ; Державний науково-дослідний інститут МВС України. – К., 2010. – 18 с.

271. Подоляка А.М. Правове регулювання охорони громадського порядку : монографія / А.М. Подоляка. – Х. : Золота миля. – 2008. – 352 с.

272. Половина американских школьников не смогла показать на карте свою страну [Электронный ресурс] // Факты и комментарии. – 2011. – 19 июля. – Режим доступа : http://fakty.ua/136687-polovina-amerikanskih-shkolnikov-ne-mogut-pokazat-na-karte-svoyu-stranu

273. Полуэхтова, И.А. Телевидение как механизм социального контроля / И.А. Полуэхтова// Вестник Московского университета. – Серия 18. Социология и политология. – 1998. – № 1. – С. 49 – 60.

274. Пономаренко, Ю.А. Основні проблеми пеналізації злочинів у законотворчій практиці / Ю.А. Пономаренко // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-

практ. конф., 13 – 14 жовтня 2011 року / редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 211 – 216.

275. Пономаренко, Ю.А. Щодо структури вчення про пеналізацію злочинів / Ю.А. Пономаренко // Правові засади підвищення ефективності боротьби зі злочинністю в Україні : матеріали наук. конф., 15 травня 2008 року / Редкол.: В.І. Борисов та ін. – Х.: Право, 2008. – С. 39 – 40

276. Постанова Верховної Ради України № 2498-III від 7 червня 2001 року "Про підсумки парламентських слухань "Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України" [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

277. Постанова Кабінету Міністрів України "Про державну комп'ютеризовану систему моніторингу сплати податків, зборів (обов'язкових платежів)" від 25 серпня 2004 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

278. Постанова Кабінету Міністрів України "Про Єдину державну інформаційну систему у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму" від 10 грудня 2003 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

279. Постанова Кабінету Міністрів України "Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління" 3 серпня 2005 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

280. Постанова Кабінету Міністрів України "Про затвердження Порядку ведення Єдиного державного реєстру судових рішень" № 740 від 25 травня 2006 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=740-2006-%EF

281. Постанова Кабінету Міністрів України "Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади" від 10 вересня 2003 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

282. Постанова Кабінету Міністрів України "Про затвердження Порядку підключення до глобальних мереж передачі даних" від 12 квітня 2002 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

283. Постанова Кабінету Міністрів України "Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»" від 24 лютого 2003 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

284. Постанова Кабінету Міністрів України "Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади" від 4 січня 2002 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua.

285. Постанова Національного банку України "Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті" від 21 січня 2004 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua.

286. Постанова Пленуму Верховного Суду України "Про судову практику у справах про злочини проти власності" від 06.11.2009 р. № 10 [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0010700-09

287. Постанова Правління Пенсійного фонду України "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, в Пенсійному фонді України та його органах" від 27 червня 2002 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

288. Постанова Правління Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України № 55 від 29 липня 2004 року "Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, у виконавчій дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України і її робочих органах" [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

289. Потрубач, Н.Н. Проблемы информационной безопасности / Н.Н. Потрубач // Дискуссии, мнения, предложения. – М., 1998. – С. 264 – 271.

290. Правовая информатика и кибернетика : учебник / Г.А. Атанесян, О.А. Гаврилов, П. Дёри, А.Г. Каблуков, А.К. Караханьян, И. Ковачич, К. Ковачичне, В.В. Крылов, А. Малиновский, М.Г. Мальковский, Г.О. Матюшкин, Я. Петцель, Н.С. Полевой, Л.Д. Самыгин, Д.Д. Хан-Магомедов, И. Ханец, С.И. Цветков, Н.П. Яблоков ; [под ред. Н.С. Полевого]. – М. : Юридическая литература, 1993. – 528 с.

291. Правовое обеспечене информационной безопасности: учеб. пособ. для студ. высш. учеб. заведений / С.Я. Казанцев, О.Э. Згадзай, Р.М. Оболенский и др.; [под ред. С.Я. Казанцева]. – М. : Академия, 2005. – 240 с.

292. Приговор спамеру [Электронный ресурс] // Официальный сайт юридической фирмы "Интернет и право". – Режим доступа : www.internet-law.ru/intlaw/spam/spamer.htm.

293. Приговор Центрального районного суда г. Барнаула по делу Гуляева Р.Г. от 21 ноября 2003 года [Электронный документ]. – Режим доступа : http://www.internet-law.ru/intlaw/crime/samara.htm

294. Приходько, О. Дети в Интернете: реальные риски виртуальных погружений [Электронный ресурс] / О. Приходько // Зеркало недели. – 2009. – № 12. – Режим доступа : http://zn.ua/articles/56562

295. Пугачев, В.П. Информационно-финансовый тоталитаризм: российский эксперимент по американскому сценарию / В.П. Пугачев // Вестн. Моск. ун-та. Сер. 12. Полит. науки. – М., 1999. – № 4. – С. 3 – 32.

296. Радутний, О. Е. Кримінальна відповідальність за незаконне збирання, використання та розміщення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : автореф. дис. ... канд. юрид. наук : 12.00.08 / Радутний Олександр Едуардович ; Національна юридична академія України ім. Ярослава Мудрого. – Х., 2002. – 21 с.

297. Радутний, О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) [Текст] : дис. ... канд. юрид. наук : 12.00.08 / Радутний Олександр Едуардович ; Національна юридична академія України ім. Ярослава Мудрого. – Х., 2002. – 204 с. – С. 183 – 199.

298. Расследование неправомерного доступа к компьютерной информации / под ред. Н.Г. Шуруханова. – М. : Щит – М., 1999. – 254 с.

299. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України (справа № 1-9/2012) від 20 січня 2012 року [Електронний ресурс] // Офіційний сайт Конституційного суду України. – Режим доступу: http://www.ccu.gov.ua/uk/doccatalog/list?currDir=167724

300. Розанова, Ю.М. Телебачення і держава : теоретичні моделі взаємодії і російська практика / Ю.М. Розанова // Вісник Московського університету. – Серія 18. Соціологія і політологія. – 1999. – № 4. – С. 107 – 122.

301. Розенфельд, Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. ... канд. юрид. наук: 12.00.08 / Наталія Андріївна Розенфельд ; [Інститут держави і права ім. В.М. Корецького НАН України]. – К., 2003. – 222 с.

302. Розпорядження Державної комісії з регулювання ринків фінансових послуг України № 4122 від 3 червня 2005 року "Про затвердження Вимог до програмного забезпечення та спеціального технічного обладнання кредитних спілок, пов'язаного з наданням фінансових послуг" [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

303. Росінчук, Т. Антиутопія інформаційного суспільства / Т.А. Росінчук // Соціальна психологія. – № 1. – 2008. – С. 85 – 95.

304. Ростовские киберпреступники шокировали американцев [Электронный ресурс] // Центр исследования компьютерной преступности. – 14.12.2010. – Режим доступа : http://www.crime-research.ru/news/14.12.2010/7039/.

305. Рудик, М.В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом: дис. ... канд. юрид. наук: 12.00.08 / Михайло Вікторович Рудик ; [Харківський національний університет внутрішніх справ]. – Х., 2007. – 229 с.

306. Румынский хакер взломал сайт ВМС Великобритании [Электронный ресурс] // Курсквеб.Ру. – 09.11.2010. – Режим доступа : http://kurskweb.ru/news/technology/15249.html

307. Сабитов, Р.А. Общественная опасность как критерий криминализации / Р.А. Сабитов // Актуальные проблемы

криминализации и декриминализации общественно опасных деяний : Сборник научных трудов. – Омск, 1980. – С. 17 – 28.

308. Савінова, Н.А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н.А. Савінова. – К., 2012. – 340 с.

309. Савченко, А.В. Удосконалення кримінальної відповідальності за шахрайські посягання в Україні: Європейський досвід / А.В. Савченко // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13 – 14 жовтня 2011 року / редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 117 – 121.

310. Сайт WikiLeaks заробив за рік 1 млн євро [Електронний ресурс] // NEWSru.com. – 24.12.2010. – Режим доступу : http://newsru.com/finance/ 24dec2010/wikileaks.html

311. Сайтарлы, Т. Компьютерная преступность бьет по налогам [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 10.08.2004. – Режим доступа : http://www.crime-research.ru/news/10.08.2004/1336

312. Сайтарлы, Т. Право граждан на неприкосновенность частной жизни не имеет достаточного правового обеспечения [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 21.01.2005. – Режим доступа : http://www.crime-research.ru/news/21.01.2005/1772

313. Сащук, Г.М. Безпекові імперативи телевізійного простору України: автореф. дис. … канд. політ.наук: 23.00.03 / Ганна Миколаївна Сащук ; [Київський національний університет імені Тараса Шевченка Інститут журналістики] – К., 2005. – 16 с.

314. Свиридов, С. "Капкан" для хакера / С. Свиридов // Комсомольская правда. – 2002. – 10 сентября. – С. 5.

315. Системи оброблення інформації. Основні положення. Терміни та визначення : ДСТУ 2938-94. – Вид. офіц. – Введ. 1996-01-01– К. : Держспоживстандарт України, 1996. – 20 с.

316. Сіленко, А.О. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства / А.О. Сіленко // Політичний менеджмент. – 2007. – № 3.– С. 96 – 112.

317. Скалацький, В. М. Інформаційне суспільство: сучасні теорії та моделі (соціально-філософський аналіз) : автореф. дис. ... канд. філос. наук: 09.00.03 / Вячеслав Миколайович Скалацький ; [Київський національний ун-т ім. Тараса Шевченка]. – К., 2006. – 17с.

318. Скляренко, О.А. Сучасні проблеми інформаційної безпеки України в умовах внутрішніх трансформацій / О.А. Скляренко // Актуальні проблеми міжнародних відносин. – 2006. – Випуск 64 (Частина І). – С. 125 – 131.

319. Соснін, О.В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук: 23.00.02 / Олександр Васильович Соснін ; [Одеська національна юридична академія]. – Одеса, 2005. – 36 с.

320. Спирина, С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации : автореф. дис. ... канд. юрид. наук: 12.00.08 / С.Г. Спирина ; [Волгоградская академия МВД России]. – Волгоград, 2001. – 16 с.

321. Справа "Класс та інші проти Німеччини" (Case of Klass and Othersv. Germany) [Електронний ресурс] // Українська правнича фундація. – Режим доступу : http://eurocourt.in.ua/Article.asp?AIdx=532.

322. Справа "Мікулич проти Хорватії" (Case of Mikulich v. Croatia) [Електронний ресурс] // Українська правнича фундація. – Режим доступу : http://eurocourt.in.ua/Article.asp?AIdx=472.

323. Стан та перспективи розвитку інформаційної сфери України: збірник матеріалів з питань становлення інформаційного суспільства в Україні / за матеріалами Рубана І.А., Семенченко А.І., Трояна П.І., Макарової В.С., Задорожньої Л.М., Брижко В.М.; упоряд. та редагування Брижка В.М., Гладківської О.В., Швеця М.Я. – К.: ТОВ "Пан Тот", 2009. – 116 с. – (Додаток до наукового журналу "Правова інформатика").

324. Старіш, О.Г. Системологія : підручник / О.Г. Старіш. – К. : Центр навчальної літератури, 2005. – 240 с.

325. Стрельцов, Є.Л. Доктринальне визначення необхідних "збудників" процесів криміналізації та декриміналізації, педалізації та депеналізації / Є.Л. Стрельцов // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13 – 14 жовтня 2011 року / редкол. : В.Я. Таційй (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 78 – 82.

326. Суд обязал спамера заплатить Facebook $360,5 млн [Электронный ресурс] // IPLIFE.com.ua. – 31.01.2011. – Режим доступа : http://www.iplife.com.ua/news/sud-spamer-facebook

327. Сэлинджер, Дж. Д. Над пропастью во ржи : повесть. Рассказы: Пер. с англ. / Дж. Д. Сэлинджер. – Х. : Фолио, 1998. – 399 с. – (Вершины. Мастера). – С. 100 – 101.

328. Тарарухин, С.А. Квалификация преступлений в следственной и судебной практике / С.А. Тарарухин. – К.: Юринком, 1995. – 208 с.

329. Таций, В.Я. Объект и предмет преступления в советском уголовном праве / В.Я. Таций. – Х.: Вища школа: Изд-во при ХГУ, 1988. – 198 с.

330. Тацій, В.Я. Десять років Кримінальному кодексу України: здобутки і проблеми застосування / В.Я. Тацій // Право України. – 2011. – № 9. – С. 5 – 19.

331. Тер-Акопов, А.А. Безопасность человека : Теоретические основы социально-правовой концепции / А.А. Тер-Акопов, Междунар. независимый экол.-политолог. ун-т (МНЭПУ). – М. : Изд-во МНЭПУ, 1998. – 196 с.

332. Типовой договор на предоставление услуг доступа к сети Интернет ООО ТРК "Бриз" [Электронный ресурс]. – Режим доступа : www.breezein.net/Ru/internet/dogovor/

333. Типовой договор хостинга ООО [Электронный ресурс]. – Режим доступа : www.anz.ru/content/31.htm

334. Титкова, О.И. Уголовно-правовая характеристика мошенничества (по материалам судебной практики Республики Карелия) : дис. … канд. юрид. наук: 12.00.08 / Ольга Игоревна Титкова. – М., 2004. – 152 с.

335. Тихомиров, О.О. Забезпечення інформаційної безпеки як функція держави [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.01 / Тихомиров О. О. ; Національна академія внутрішніх справ. – К., 2011. – 19 с.

336. Трегубов, В. Пост ДАІ на шляхах Інтернету [Електронний ресурс] / В. Трегубов // Дзеркало тижня. – 2012. – № 6. – Режим доступу : http://dt.ua/POLITICS/post_dai_na_shlyahah_internetu-97470.html

337. Уголовный кодекс Австралии 1995 г. – СПб. : Юридический центр Пресс, 2002. – 388 с.

338. Уголовный кодекс Австрии. – СПб. : Юридический центр Пресс, 2004. – 352 с.

339. Уголовный кодекс Бельгии. – СПб. : Юридический центр Пресс, 2004. – 561с.

340. Уголовный кодекс Голландии. – СПб. : Юридический центр Пресс, 2001. – 510 с.

341. Уголовный кодекс Дании. – СПб.: Юридический центр Пресс, 2001. – 230 с.

342. Уголовный кодекс Латвийской республики. – СПб. : Юридический центр Пресс, 2001. – 313 с.

343. Уголовный кодекс Литовской республики. – СПб. : Юридический центр Пресс, 2003. – 470 с.

344. Уголовный кодекс Республики Беларусь [Электронный ресурс] // Эталонный банк данных правовой информации Республики Беларусь. – Режим доступа : http://www.pravo.by/webnpa/

345. Уголовный кодекс Республики Польша. – СПб. : Юридический центр Пресс, 2001. – 234 с.

346. Уголовный кодекс Украины : Научно-практический комментарий / Отв. ред. С.С. Яценко, В.И. Шакун. – К. : Правові джерела, 1998. – 1088 с.

347. Уголовный кодекс Украины. Комментарий / Под ред. Ю.А. Кармазина и Е.Л. Стрельцова. – Х. : ООО "Одиссей", 2001. – 960 с.

348. Уголовный кодекс Украины: Научно-практический комментарий / Отв. ред. С.С. Яценко. – 3-е изд., испр. и доп. – К. : А.С.К., 2004. – 1096 с.

349. Уголовный кодекс Украины: Научно-практический комментарий / Отв. ред. Е.Л. Стрельцов. – Издание четвертое, перераб. и доп. – Х. : Одиссей, 2007. – 872 с.

350. Уголовный кодекс Федеративной Республики Германии. – СПб. : Юридический центр Пресс, 2003. – 524 с.

351. Уголовный кодекс Эстонской республики. – СПб.: Юридический центр Пресс, 2001. – 262 с.

352. Уголовный кодекс Японии. – СПб. : Юридический центр Пресс, 2002. – 226 с.

353. Угроза кибертерроризма будет только возрастать [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 27.12.2008. – Режим доступа : http://www.crime-research.ru/news/27.12.2008/5106/

354. Указ Президента України "Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України" від 6 жовтня 2000 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу : http://zakon1.rada.gov.ua.

355. Указ Президента України № 1119/2010 від 17 листопада 2010 року "Про рішення Ради національної безпеки і оборони України "Про виклики та загрози національній безпеці України у 2011 році" [Електронний ресурс] // Офіційний сайт Ради національної безпеки і оборони України. – Режим доступу : http://www.rainbow.gov.ua/documents/277.html

356. Уколов Р. Базы данных / Роман Уколов [Электронный ресурс] // Независимая газета. – 06.04.2005. – Режим доступа : http://www.ng.ru/events/2005-04-06/6_bases.html

357. Украина: потери от вирусных атак в первом полугодии 2004 г. составили около 45 млн. евро [Электронный ресурс] // Новости сайта Центра исследования ком-

пьютерной преступности. – 30.07.2004. – Режим доступа : http://www.crime-research.ru/news/30.07.2004/1320.

358. Україна в 2005 – 2009 рр.: стратегічні оцінки суспільно-політичного та соціально-економічного розвитку : монографія / за заг. ред. Ю.Г. Рубана. – К. : НІСД, 2009. – 655 с.

359. Управление "К" выявило с начала года 7,5 тыс. преступлений в IT-сфере [Электронный ресурс] // РИА НОВОСТИ. – 23.11.2010. – Режим доступа : http://www.rian.ru/inquest/20101123/300003609.html

360. Ухвала колегії суддів судової палати у кримінальних справах апеляційного суду Хмельницької області від 26 грудня 2006 року [Електронний ресурс] // Єдиний державний реєстр судових рішень. – Режим доступу : http://www.reyestr.court.gov.ua/

361. Уэбстер, Ф. Теории информационного общества / Фрэнк Уэбстер ; [пер. с англ. М.В. Арапова, Н.В. Малыхиной; под. ред. Е.Л. Вартановой]. – М. : Аспект Пресс, 2004. – 400 с.

362. Фарбер, И.Е. Правосознание как форма общественного сознания / И.Е. Фарбер. – М. : Юрид. лит., 1963. – 206 с.

363. Федотов, О.А. Предмет злочинного посягання за злочинами у сфері комп'ютерних технологій / О.А. Федотов // Економіка, фінанси, право. – 2010. – № 2. – С. 37 – 39.

364. Фефелов, П.А. Общественная опасность преступного деяния / П.А. Фефелов // Советское государство и право. – 1977. – № 5. – С. 135 – 138.

365. Філософський словник / за ред. В.І. Шинкарука. – К., 1973. – 600 с.

366. Фролов, В.С. "Думающее" оружие / В.С. Фролов. – М. : Знание, 1991. – 62 с.

367. Хакер, устроивший порнопоказ в Москве, приговорен к 6 годам заключения [Электронный ресурс] // SecurityLab.ru. – 23.03.2011. – Режим доступа : http://www.securitylab.ru/news/405193.php

368. Хакери атакували кібер-поліцію Італії [Електронний ресурс] // BBCUkrainian. – 25.07.2011. – Режим доступу : http://www.bbc.co.uk/ukrainian/science/2011/07/110725_hackers_italy_it.shtml.

369. Хакеры взломали базу данных McDonald's [Электронный ресурс] // Bfm.ru. – 13.12.2010. – Режим доступа : http://www.bfm.ru/news/2010/12/14/hakery-vzlomali-bazu-dannyh-mcdonald-s.html#text

370. Хакеры взломали страницу Николя Саркози в Facebook [Электронный ресурс] // Постсовет. – 24.01.2011. – Режим доступа : http://www.postsovet.ru/blog/russia/62037.html

371. Хакеры добрались до официального Twitter КНДР [Электронный ресурс] // Автоволк новости. – 10.01.2011. – Режим доступа : http://www.autovolk.ru/modules.php?name=News&file=view&news_id=28322

372. Хакеры замаскировали троянский вирус под "Камасутру" [Електронний ресурс] // UBR – Український бізнес ресурс. – 14.01.2011. – Режим доступа : http://ubr.ua/ukraine-and-world/technology/hakery-zamaskirovali-troianskii-virus-pod-kamasutru--74135

373. Хакеры заразили полмиллиона "твиттерян" [Электронный ресурс] // Государственный интернет-канал "Россия". – 21.09.2010. – Режим доступа : http://www.vesti.ru/doc.html?id=394129.

374. Харламова, Е. "Незолотая" молодежь резвится в Сети / Елена Харламова [Электрооный ресурс] // Компьютер и право. – 2010. – № 44. – Режим доступа : http://www.kv.by/index2010442502.htm

375. Харламова, С. О. Кримінальна відповідальність за незаконні дії з відомостями, що становлять комерційну або банківську таємницю : дис. ... канд. юрид. наук: 12.00.08 / Харламова Світлана Олегівна ; Київський національний ун-т внутрішніх справ. – К., 2007. – 221 арк. – Арк. 188 – 206.

376. Харченко, В. Б. Кримінально-правова охорона прав на об'єкти інтелектуальної власності в Україні: перспективи розвитку та гармонізації з європейським законодавством [Текст] : автореф. дис. ... д-ра. юрид. наук : 12.00.08 / Харченко В.Б. ; Харківський національний університет внутрішніх справ. – Х., 2011. – 36 с.

377. Худицький, В. Електронний шлагбаум. Підприємці не хочуть звітувати перед державою через електронних посередників [Електронний ресурс] / В. Худицький // Дзеркало тижня. – 2010. – № 4. – Режим доступу : http://dt.ua/articles/59133

378. Цимбалюк, В.С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) / В.С. Цимбалюк // Підприємництво, господарство і право. – 2004. – № 3. – С. 88 – 91.

379. Чубукова, С.Г. Основы правовой информатики (юридические и математические вопросы информатики) : учеб. пособ. – Изд. второе, испр., доп. / С.Г. Чубукова, В.Д. Элькин ; [под ред. д-ра юрид. наук, проф. М.М. Рассолова, проф. В.Д. Элькина] – М. : Юридическая фирма "КОНТРАКТ", 2007. – 287 с.

380. Чуприй, Л. Пленники информационного пространства / Л. Чуприй // Зеркало недели. – 2010. – № 21. – С. 13.

381. Швець, В.Д. Законодавча реалізація кримінально-правової політики: аналіз законопроектної діяльності Верховної Ради України V скликання з питань кримінального права / В.Д. Швець, В.М. Грицак, Я.І. Василькевич, В.О. Гацелюк ; [вступне слово проф. Мельника М.І.] – К. : Атіка, 2008. – 244 с.

382. Швець, В.Д. Практика внесення змін і доповнень до КК України: здобутки та прорахунки / В.Д. Швець // 10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн : матеріали міжнар. наук.-практ. конф., 13 – 14 жовтня 2011 року / редкол. : В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2011. – С. 35 – 40.

383. Швець, М. Україна на шляху до інформаційного суспільства / Швець М., Калюжний Р., Цимбалюк В., Гавловський В., Брижко В.// Правова інформатика. – К., 2003. – № 1. – С. 90 – 98.

384. Шевченко, Є.В. Злочини з похідними наслідками в кримінальному праві : дис. ... канд. юрид. наук: 12.00.08 / Євген Валерійович Шевченко ; Національна юридична академія України ім. Ярослава Мудрого. – Х., 2001. – 201 арк. – С. 182 – 194.

385. Шинкаренко, І.Р. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія : монографія / І.Р. Шинкаренко, В.О. Голубєв, М.В. Карчевський, І.Ф. Хараберюш; МВС України, Донецький юридичний інститут Луганського державного університету внутрішніх справ. – Донецьк : РВВ ЛДУВС, 2007. – 266 с.

386. Шуберт, Л. Об общественной опасности преступного деяния [Текст] / Л. Шуберт ; пер. со словац. Р.П. Разумова ; ред. М.А. Гельфер. – М. : Госюриздат, 1960. – 239 с.

387. Юдін, О.К. Інформаційна безпека держави : навчальний посібник / О.К. Юдін, В.М. Богуш. – Х. : Консум, 2005. – 576 с.

388. Яременко, О. Офіційна державна інформація в Україні: поняття та право на доступ / О. Яременко // Право України. – 2005. – № 8. – С. 89 – 92.

389. Яременко, О. Правове регулювання доступу до офіційної правової інформації в Україні / О. Яременко // Правова інформатика. – 2006. – № 1. – С. 12 – 17.

390. "Черный" рынок конфиденциальной информации [Электронный ресурс] // @Astera. – 24.11.2008. – Режим доступа : http://www.astera.ru/news/?id=63659

391. A Strong Britain in an Age of Uncertainty: The National Security Strategy [Electronic resource] // The Stationery Office (TSO). – Mode of access: http://www.official-documents.gov.uk/document/cm79/7953/7953.pdf

392. Aglietta, M. A Theory of Capitalist Regulation: the US experience / Michel Aglietta. – London : New Left Books, 1979. – 390 p.

393. Baudrillard, J. In the Shadow of the Silent Majorities, or, The End of the Social and Other Essays / Jean Baudrillard. – New York: Semiotext(e), 1983. – 123 p.

394. Bell, D. The Coming of Post-Industrial Society: A Venture in Social Forecasting / Daniel Bell. – New York:Basic Books, 1973. – 507 p.

395. Brzezinsky, Z. Between two Ages. American's Role in the Technotronic Era / Zbigniew Brzezinski. –New York : Viking Press, 1970. – 334 p.

396. Castells, M. End of Millennium. Vol. 3 of The Information Age:Economy, Society and Culture / Manuel Castells. – Oxford: Blackwell, 1998. – 418 p.

397. Castells, M. The Power of Identity. Vol. 2 of The Information Age: Economy, Society and Culture / Manuel Castells. – Oxford: Blackwell, 1997. – 461 p.

398. Castells, M. The Rise of the Network Society. Vol. 1 of The Information Age: Economy, Society and Culture / Manuel Castells. – Oxford: Blackwell, 1996. – 556 p.

399. Complaint against Sanford Wallace, Adam Arzoomanian, Scott Shaw (Filing fee $ 350.00, receipt number 54611004760.). Filed byFacebook, Inc.. (gm, COURT STAFF) (Filed on 2/24/2009) (Additional attachment(s) added on 3/5/2009: # 1 Civil Cover Sheet) (gm, COURT STAFF) [Electronic resource] // The Justia Federal District Court Filings & Dockets site. – Modeof access: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/1/0.pdf

400. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). Public Law 108-187 [Electronic resource]. – Mode of access: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

401. Default Judgment in favor of Facebook, Inc. against Sanford Wallace. Signed by Judge Jeremy Fogel on 10/29/2009 [Electronic resource] // The Justia Federal District Court Filings & Dockets site. – Modeof access: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/92/

402. Dice, M. Big Brother: The Orwellian Nightmare Come True / Mark Dice– The Resistance Manifesto, 2011. – 326 p.

403. Giddens, A. Social Theory and Modern Sociology /Anthony Giddens.–Cambridge: Polity, 1987.– 310 p.

404. Giddens, A. The Nation State and Violence, Vol. 2 of A Contemporary Critique of Historical Materialism /Anthony Giddens. – Cambridge: Polity, 1985. – 380 p.

405. Habermas, J. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society [translated by Thomas Burger with the assistance of Fre derick Lawrence]/ Jurgen Habermas. – Cambridge, Massachusetts : MIT Press, 1989.– 301 p.

406. Idictment USA v. Robert Alan Soloway and Newport Internet Marketing Corporation [Electronic resource] // Mortgagespam site. – Mode of access: http://www.mortgagespam.com/soloway/Indictmentfiled.pdf

407. Israeli Citizen Arrested in Israel for Hacking United States and Israeli Government Computers (March 18, 1998) [Electronic resource] // Computer Crime & Intellectual Property Section of United States Department of Justice site. – Mode of access : http://usdoj.gov/criminal/cybercrime /ehudpr.html

408. Jonscher, C. Wired Life: who are we in the digital age? / Charles Jonscher. – NewYork: Bantam, 1999.– 293 p.

409. Kirwan, N. Big Brother: Who Is Watching / Natasha Kirwan – Pocket Issue Limited, 2008. – 96 p.

410. Lipietz,A. Mirages and Miracles: The Crises of Global Fordism / Alain Lipietz. – London : Verso, 1987.– 226 p.

411. Machlup, F. The Production and Distribution of Knowledge in the United States / Fritz Machlup. – Princeton, NJ: Princeton University Press, 1962. – 416 p.

412. Markoff, J. Malware Aimed at Iran Hit Five Sites, Report Says / John Markoff // The New York Times. – 11.02.2011. – Mode of access: http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=1&ref=stuxnet

413. Martin, S. Bits, bytes, and big brother: federal information control in the technological age / Shannon E. Martin. – Greenwood Publishing Group, 1995. – 166 p.

414. Monthly Websense Email Security Threat Brief "In The Mail", August 2010, Volume 3, Issue 8 [Electronic resource] // Websense Security Labs site. – Mode of access:

http://securitylabs.websense.com/content/Assets/report-in-the-mail-aug-10-en.pdf

415. Morozov, E. Living with the Streisand Effect [Electronic resourse] / E. Morozov // The New York Times site. – Mode of access: http://www.nytimes.com/2008/12/26/opinion/26iht-edmorozov.1.18937733426.html

416. Mulgan, G. Communication and Control: Networks and the New Economies of Communication / Geoff Mulgan. – Cambridge: Polity Press, 1991. – 302 p.

417. Porat, M. The Information Economy: Sources and Methods for Measuring the Primary Information Sector (Detailed Industry Reports) / Marc Uri Porat. – Washington, DC: US Department of Commerce, Office of Telecommunications, 1977. – 180 p.

418. Schiller, H. Who Knows: Information in the Age of the Fortune 500 / Herbert I.Schiller. – Norwood, NJ: Ablex, 1981. – 187 p.

419. Schjolberg,S. "The Legal Framework – Unauthorized Access to Computer Systems. Penal Legislation in 44 Countries" [Electronic resource] / Stein Schjolberg // Moss District Court site. – Mode of access : http://www.mosstingrett.no/info/legal.html.

420. SonyPictures хранит пароли пользователей в открытом виде [Электронный ресурс] // Центр информационной безопасностиbeazpeka.com – 06.06.2011. – Режим доступа : http://www.bezpeka.com/ru/news/2011/06/06/sonypictures-lulzsec.html

421. Sophos: Мир вошел в "третью эпоху" киберпреступности [Электронный ресурс] // Открытые системы. – 20.01.2011. – Режим доступа : http://www.osp.ru/news/thematic/2011/0120/13005261/

422. The National Information Infrastructure Protection Act of 1996 Legislative Analysis By The Computer Crime and Intellectual Property Section United States Department of Justice [Electronic resource] // Computer Crime & Intellectual Property Section of United States Department of Justice site. – Mode of access : http://www.usdoj.gov/criminal/cybercrime/1030_anal.html.

423. The Register of Known Spam Operations (ROKSO) database [Electronic resource]// The Spamhaus Project site. – Mode of access: http://www.spamhaus.org/statistics/spammers.lasso

424. The World's Worst Spammers [Electronic resource] // The Spamhaus Project site. – Mode of access: http://www.spamhaus.org/statistics/spammers.lasso

425. U.S. National Information Infrastructure Protection Act of 1996 [Electronic resource] // Electronic privacy information center. – Mode of access: http://epic.org/security/1996_computer_law.html

426. Yiannopoulos, M. What is 'The Streisand Effect'? [Electronic resourse] / Yiannopoulos M. // The Daly Telegraph site. – Mode of access: http://blogs.telegraph.co.uk/technology/miloyiannopoulos/8248311/What_is_The_Streisand_Effect/

Додатки

Додаток 1

Реальні та потенційні загрози інформаційній безпеці України та заходи протидії їм
(систематизація положень Доктрини інформаційної безпеки України, затвердженої Указом Президента України № 514/2009 від 8 липня 2009 року)

	Зовнішньополітична сфера	Сфера державної безпеки
Загрози	1) поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; 2) прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем; 3) зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;	1) негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України; 2) використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками; 3) несанкціонований доступ до інформаційних ресурсів органів державної влади; 4) розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

Продовження таблиці

Заходи протидії	1) удосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном; 2) організаційно-технічне, інформаційне та ресурсне сприяння держави вітчизняним засобам масової інформації, що формують у світовому інформаційному просторі позитивний імідж України; 3) посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України в разі повноправного її партнерства з державами — членами ЄС та НАТО; 4) інтеграція в міжнародні інформаційно-телекомунікаційні системи та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету; 5) гарантування своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації;	1) залучення засобів масової інформації до забезпечення неухильного додержання конституційних прав і свобод людини й громадянина, захисту конституційного устрою, удосконалення системи політичної влади з метою зміцнення демократії, духовних і моральних засад суспільства; підвищення ефективності функціонування органів державної влади; 2) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; 3) розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп'ютерними системами і мережами;
	Військова сфера	**Внутрішньополітична сфера**
Загрози	1) порушення встановленого регламенту збирання, обробки, зберігання та передачі інформації з об-	1) недостатня розвиненість інститутів громадянського суспільства, недосконалість партійно-політичної системи, непро-

	меженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України; 2) несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони; 3) реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України; 4) перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління; 5) інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;	зорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю; 2) негативні інформаційні впливи, у тому числі з застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість; 3) поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;
Заходи протидії	1) проведення систематичного аналізу застосування засобів, форм і способів інформаційної боротьби у військовій сфері, визначення напрямів забезпечення інформаційної безпеки держави; 2) удосконалення законодавства з питань інформаційної безпеки, координації діяльності органів державної влади та органів	1) створення дієвої та прозорої системи громадського контролю за діяльністю органів державної влади й органів місцевого самоврядування, громадсько-політичних структур, зокрема через створення системи суспільного телебачення і радіомовлення України; 2) поліпшення взаємодії органів державної влади з громадськими організаціями у сфері боротьби з проявами обмеження

	військового управління під час вирішення завдань забезпечення інформаційної безпеки; 3) удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами та зброєю, від несанкціонованого доступу; 4) удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави; 5) підготовка спеціалістів з питань інформаційної безпеки у військовій сфері;	конституційних прав і свобод людини й громадянина та маніпулювання масовою свідомістю;
	Економічна сфера	**Соціальна та гуманітарна сфери**
Загрози	1) відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій; 2) недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель; 3) несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах; 4) використання неліцензованого і несертифіко-	1) відставання України від розвинених держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури; 2) недодержання прав людини й громадянина на одержання інформації, необхідної для захисту їхніх соціально-економічних прав; 3) поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської та національної гідності; 4) тенденція до витіснення з інформаційного простору та молодіжної культури українсь-

	ваного програмного забезпечення, засобів і комплексів обробки інформації; 5) недостатній рівень розвитку національної інформаційної інфраструктури;	ких мистецьких творів, народних традицій і форм дозвілля; 5) послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства; 6) відставання рівня розвитку українського кінематографу, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвинених держав;
Заходи протидії	1) підтримка вітчизняних виробників високотехнологічної продукції, насамперед комп'ютерно-телекомунікаційних засобів і технологій; 2) формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів; 3) гармонізація законодавства України з питань інформаційної безпеки в економічній сфері з міжнародними нормами та стандартами; 4) розроблення та вдосконалення методів і засобів захисту інформації; 5) забезпечення сталого розвитку національного медіа-ринку під час впровадження в Україні цифрового телерадіомовлення; 6) посилення державного контролю за додержанням вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації;	1) формування та реалізація державної політики національного духовного та культурного відродження, яка відповідає ін.-тересам Українського народу і визначає чіткі критерії та пріоритети формування інформаційної політики в соціальній сфері; 2) запобігання монополізації національного інформаційного простору; 3) удосконалення законодавчого регулювання діяльності засобів масової інформації, зокрема, з метою підтримки діяльності, спрямованої на формування оптимістичної морально-психологічної атмосфери в суспільстві, популяризації національних культурних цінностей, сприяння соціальній стабільності й злагоді; 4) державна підтримка вітчизняного виробника інформаційної продукції;

	7) комплексна інформатизація процесів формування, розподілення і контролю за використанням бюджетних коштів; 8) удосконалення системи статистичної звітності з метою підвищення оперативності, достовірності й релевантності звітної інформації;	
	Науково-технологічна сфера	**Екологічна сфера**
Загрози	1) зниження наукового потенціалу в галузі інформатизації та зв'язку; 2) низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку; 3) відтік за кордон наукових кадрів і суб'єктів права інтелектуальної власності; 4) недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки; 5) неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;	1) приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру; 2) недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій; 3) низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.
Заходи протидії	1) забезпечення технологічної конкурентоспроможності України у сфері інформатизації та зв'язку; 2) розвиток міжнародного науково-технічного співробітництва у сфері забезпечення захисту інформації в міжнародних телекомунікаційних системах;	1) проведення комплексного аналізу екологічного стану територій та їх виробничого потенціалу з метою вироблення інформаційної політики щодо впровадження концепції сталого розвитку; 2) застосування сучасних аерокосмічних, комп'ютерно-телекомунікаційних та геоінформа-

	3) удосконалення системи охорони та захисту права інтелектуальної власності; 4) науково-технологічний супровід формування і розвитку в Україні інформаційного суспільства з урахуванням вимог забезпечення інформаційної безпеки України; 5) розширення можливостей доступу громадян до світового інформаційного простору, зокрема до наукової та науково-технічної інформації;	ційних засобів і технологій для комплексного моніторингу, профілактики та своєчасного реагування на надзвичайні ситуації; 3) створення бази даних екологічно безпечних технологій і продукції, їх розробників, виробників і постачальників, результатів маркетингових досліджень екологічного ринку; 4) підвищення рівня інформатизації галузі страхування для акумулювання коштів на відшкодування збитків від надзвичайних ситуацій, а також на довгострокове інвестування заходів із мінімізації ризиків життєдіяльності й господарювання.

Додаток 2

Таблиця 1

Елементи формальної системи представлення законодавчої оцінки суспільної небезпечності злочину

Номер елементу	Зміст і форма подання відомостей
1	наявність можливості застосування покарання у вигляді довічного позбавлення волі (можливі значення: 1 – передбачено в санкції; 0 – не передбачено в санкції);
2	верхня межа покарання у вигляді позбавлення волі (значення в роках);
3	нижня межа покарання у вигляді позбавлення волі (значення в роках);
4	верхня межа покарання у вигляді тримання в дисциплінарному батальйоні військовослужбовців (значення в роках);
5	нижня межа покарання у вигляді тримання в дисциплінарному батальйоні військовослужбовців (значення в роках);
6	верхня межа покарання у вигляді обмеження волі (значення в роках);
7	нижня межа покарання у вигляді обмеження волі (значення в роках);
8	верхня межа покарання у вигляді арешту (значення в місяцях);
9	нижня межа покарання у вигляді арешту (значення в місяцях);
10	верхня межа покарання у вигляді службових обмежень для військовослужбовців (значення в роках);
11	нижня межа покарання у вигляді службових обмежень для військовослужбовців (значення в роках);
12	верхня межа покарання у вигляді виправних робіт (значення в роках);
13	нижня межа покарання у вигляді виправних робіт (значення в роках);
14	верхня межа покарання у вигляді громадських робіт (значення в годинах);
15	нижня межа покарання у вигляді громадських робіт (значення в годинах);
16	верхня межа основного покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю (значення в роках);
17	нижня межа основного покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю (значення в роках);

Продовження таблиці

18	верхня межа основного покарання у вигляді штрафу (значення в неоподатковуваних мінімумах доходів громадян);
19	нижня межа основного покарання у вигляді штрафу (значення в неоподатковуваних мінімумах доходів громадян);
20	наявність можливості застосування додаткового покарання у вигляді конфіскації майна (можливі значення: 2 – передбачено як обов'язкову; 1 – передбачено як факультативну; 0 – не передбачено в санкції);
21	верхня межа додаткового покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю (значення в роках);
22	нижня межа додаткового покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю (значення в роках);
23	перемінна, що характеризує додаткове покарання у вигляді позбавлення права обіймати певні посади або займатися певною діяльністю як обов'язкове або факультативне (можливі значення: 2 – передбачено як обов'язкове; 1 – передбачено як факультативне)
24	верхня межа додаткового покарання у вигляді штрафу (значення в неоподатковуваних мінімумах доходів громадян);
25	нижня межа додаткового покарання у вигляді штрафу (значення в неоподатковуваних мінімумах доходів громадян);
26	перемінна, що характеризує додаткове покарання у вигляді штрафу як обов'язкове або факультативне (можливі значення: 2 – передбачено як обов'язкове; 1 – передбачено як факультативне);
27	наявність можливості застосування спеціальної конфіскації (можливі значення: 2 – передбачена як обов'язкова; 1 – передбачена як факультативна; 0 – не передбачені в санкції).

Додаток 3

Порядок сортування відомостей щодо змісту кримінально-правових санкцій залежно від етапів реалізації методу контекстної законодавчої оцінки суспільної небезпечності посягання

Етапи реалізації методу	Порядок ранжирування заборон, що входять до певної групи (послідовність елементів формальної системи, за якою проводиться сортування)
Етап 1. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено довічне позбавлення волі.	1, 20, 21, 22, 23, 24, 25, 26, 27, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 2. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено позбавлення волі.	2, 20, 21, 22, 23, 24, 25, 26, 27, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 3. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено тримання в дисциплінарному батальйоні військовослужбовців.	4, 20, 21, 22, 23, 24, 25, 26, 27, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 4. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено обмеження волі.	6, 20, 21, 22, 23, 24, 25, 26, 27, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 5. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено арешт.	8, 20, 21, 22, 23, 24, 25, 26, 27, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 6. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено службові обмеження для військовослужбовців	10, 20, 21, 22, 23, 24, 25, 26, 27, 11, 12, 13, 14, 15, 16, 17, 18, 19
Етап 7. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено виправні роботи.	12, 20, 21, 22, 23, 24, 25, 26, 27, 13, 14, 15, 16, 17, 18, 19

Продовження таблиці

Етап 8. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено громадські роботи.	14, 20, 21, 22, 23, 24, 25, 26, 27, 15, 16, 17, 18, 19
Етап 9. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено позбавлення права обіймати певні посади або займатися певною діяльністю.	16, 20, 24, 25, 26, 27, 17, 18, 19
Етап 10. Ранжирування санкцій злочинів, за вчинення яких найбільш суворим основним покаранням визначено штраф.	18, 20, 21, 22, 23, 27, 19

Додаток 4

Досвід законодавчого регулювання масового розповсюдження повідомлень електрозв'язку в США

Одним з найбільш прогресивних нормативно-правових актів у сфері регулювання масового розповсюдження повідомлень електрозв'язку є Федеральний Закон Сполучених Штатів Америки під назвою Controlling the Assault of Non-Solicited, Pornography and Marketing Act (CAN-SPAM Act) від 16 грудня 2003 року [1]. У зв'язку з цим його дослідження в контексті наукового аналізу питання кримінально-правової охорони інформаційної безпеки є доцільним.

Перед тим як перейти до розгляду ознак складів злочинів, передбачених цим нормативним документом, необхідно зробити деякі термінологічні уточнення. Предметом передбачених законом злочинів є комерційні повідомлення електронної пошти (commercial electronic mail message), що визначаються як повідомлення електронної пошти, головною метою яких є комерційна реклама або пропозиція конкретних товарів чи послуг (включаючи зміст платних інтернет-сайтів). При цьому в законі зазначається, що до комерційної пошти не відносяться повідомлення про трансакції або відносини (transactional or relationship message). Останні являють собою повідомлення, метою яких є: 1) підтвердження комерційної трансакції отримувача; 2) повідомлення про гарантійне чи сервісне обслуговування продуктів або послуг, придбаних отримувачем; 3) повідомлення отримувача про статус або баланс його фінансового рахунку чи про іншу подібну інформацію стосовно позик, триваючих комерційних відносин тощо; 4) забезпечення отримувача інформацією щодо його трудових відносин; 5) забезпечення отримувача інформацією про доставку товарів чи послуг, які він замовив.

Важливим для формулювання ознак досліджуваних складів злочинів є також термін "header information", який можна перекласти як "інформація, що міститься в заголовку повідом-

лення". До цих відомостей CAN-SPAM Act відносить дані щодо джерела, призначення та маршрутизації електронного листа, а також будь-які інші дані, що дозволяють ідентифікувати особу, яка "ініціювала" повідомлення. Ініціювання повідомлення визначається як його передавання, спричинення початку процесу передавання або забезпечення виконання подібних дій іншими особами. Метою такого складного формулювання є виключення зі сфери дії закону провайдерів інтернет-послуг, які здійснюють транспортування передачі (routine conveyance) – передачу, маршрутування, ретрансляцію, керування або зберігання шляхом автоматичного технічного процесу повідомлень електронної пошти, для яких інші особи визначили адреси отримувачів. Транспортування передачі не є ініціюванням повідомлення за визначенням, закон розділяє ці поняття для того, щоб ідентифікувати діяльність саме відправника повідомлень, відокремити її від роботи провайдера послуг Інтернет, який забезпечує фактичне передавання повідомлення.

Також закон оперує терміном "захищений комп'ютер" (protected computer), він визначається у федеральному законі щодо захисту національної інфраструктури (U.S. National Information Infrastructure Protection Act of 1996) [2]. До захищених відносяться: 1) комп'ютери, які використовуються фінансовими установами або урядом США виключно або від їх імені чи для виконання їх завдань, і діяння, яке утворює злочин, чинить вплив на таке використання; 2) комп'ютери, які використовуються в комерційній або комунікаційній діяльності, що здійснюється між штатами або на міжнародному рівні, включаючи комп'ютери, що перебувають поза межами США, які використовуються в спосіб, що впливає на таку комерційну або комунікаційну діяльність. Нарешті, множинними (multiple) повідомлення слід уважати тоді, коли їх кількість перевищує 100 за 24 години, 1000 – протягом 30 днів чи 10000 – протягом року.

Отже, відповідно до CAN-SPAM Act діяння, вчинені під час комерційної діяльності, що відбувається між штатами або є міжнародною, або діяння, вчинені для забезпечення такої ді-

яльності третіх осіб, треба вважати федеральними злочинами, коли вони становлять:

1) несанкціонований доступ до захищеного комп'ютера та умисне ініціювання передачі множинних комерційних повідомлень електронної пошти з такого комп'ютера або через нього (18 U.S.C. 1037 (a)(1));

2) використання захищеного комп'ютера для передавання або перенаправлення комерційних повідомлень електронної пошти з метою введення в оману отримувачів або інтернет-провайдерів стосовно джерела таких повідомлень (18 U.S.C. 1037 (a)(2));

3) істотне викривлення інформації, що міститься в заголовку множинного повідомлення, та умисне ініціювання передавання таких повідомлень (18 U.S.C. 1037 (a)(3));

4) реєстрацію з використанням істотно викривленої інформації стосовно ідентифікації особи, що реєструється, п'яти або більше облікових записів електронної пошти чи облікових записів мережевих користувачів, або двох чи більше доменних імен та умисне ініціювання передавання множинних комерційних повідомлень електронної пошти з будь-якої комбінації таких облікових записів або доменних імен (18 U.S.C. 1037 (a)(4));

5) представлення себе шляхом обману особою або законним представником особи, на яку зареєстровано п'ять або більше IP-адрес (цифрових ідентифікаторів певних комп'ютерів в мережі Інтернет), та умисне ініціювання передачі множинних комерційних повідомлень електронної пошти з таких адрес (18 U.S.C. 1037 (a)(5)).

Закон передбачає такі кваліфікуючі ознаки перелічених посягань: 1) вчинення означених дій для подальшого здійснення злочину, передбаченого федеральним законодавством або законами певного штату; 2) вчинення означених злочинів після вчинення будь-якого з посягань, передбачених розділом 1030 Зводу законів Сполучених Штатів (федеральний кримінальний закон про "комп'ютерні" злочини), або будь-якого злочину, передбаченого законодавством певного штату, пов'язаного з передачею множинних комерційних повідомлень електронної пошти або несанкціонованим доступом до комп'ютерної системи; 3) вчинення злочину, передбаченого U.S.C. 1037 (a)(4) з використанням більш ніж 20 облікових записів електронної пошти або облікових записів мережевих користувачів або більш ніж 10 доменних імен, реєстрація яких пов'язана з фальсифікацією; 4) вчинення множинного розсилання в розмірі 2500 листів за день або 25000 за 30 днів, або 2500000 листів за рік; 5) втрати однієї або більше осіб унаслідок вчинення означених злочинів складають 5000 $ США або більше протягом одного року; 6) у результаті вчинення означених злочинів особа, яка його вчинила, отримала протягом одного року майно або будь-які майнові переваги, сума яких у грошовому вираженні дорівнює або перевищує 5000 $ США; 6) означені злочини було вчинено групою осіб і винна особа виконувала роль організатора або керівника.

Як приклад застосування норм цього закону розглянемо кваліфікацію масового розсилання повідомлень електронної пошти, запропоновану в обвинувальному вироку в справі США проти Роберта Соловея та Ньюпорт Інтернет Маркетинг (USA v. Robert Alan Soloway and Newport Internet Marketing Corporation) [3]. Головною метою діяльності обвинуваченого було отримання майна шляхом обману. Для цього Роберт Соловей розмістив на багатьох сайтах рекламу програмного забезпечення та послуг створеної ним корпорації Ньюпорт Інтернет Маркетинг. Ці послуги полягали в організації леґального масового розсилання реклами шляхом електронної кореспонденції. Усі відомості про наявність бази даних леґально отриманих адрес електронної пошти, працездатність запропонованого програмного забезпечення, наявність послуг цілодобової технічної підтримки та повернення вартості програмного забезпечення в разі неотримання замовником гарантованого прибутку не відповідали дійсності. Крім цього, використовуючи незаконно отримані електронні адреси, Роберт Соловей здійснював масове розсилання комерційних повідомлень електронної пошти, у яких рекламував послуги та програмні продукти Ньюпорт Інтернет Маркетинг. За даними обвинувачен-

ня, таких повідомлень налічувалися десятки мільйонів. При цьому адреси, які він використовував для фальсифікації реального джерела повідомлень, належали, як правило, тим особам, які внаслідок введення в оману придбали рекламоване ним програмне забезпечення. Приховування джерела повідомлень здійснювалося з використанням спеціального програмного забезпечення, яким він фальсифікував дані заголовків повідомлень. Така фальсифікація чинилася шляхом залишення поля "Звідки" (From) порожнім або заповнення його неіснуючою адресою чи адресою, що належала іншій особі. Також для приховування реальної адреси відправника Роберт Соловей використовував близько 2000 так званих проксі-серверів (proxy servers) спеціальних мережевих служб, які дозволяють переадресовувати та перенаправляти потоки електронної пошти та змінювати відомості про джерело повідомлення. Обвинувачення окремо містить характеристику шкоди, заподіяну через масове розсилання повідомлень електронної пошти. У цьому випадку вона головним чином пов'язується з певними ускладненнями легального використання електронної пошти особами, яким належали використовувані зловмисником електронні адреси. У деяких випадках це виявлялося в припиненні обслуговування електронних адрес цих осіб провайдерами інтернет-послуг. Такий захід провайдери Інтернет вправі застосовувати своїм рішенням, оскільки масове розсилання є порушенням загальних правил надання доступу до мережі. Отже, реальні володарі адрес, які використовував Роберт Соловей, несли відповідальність за розсилання, які він організовував. Для тих із них, хто здійснює господарську діяльність в Інтернеті, подібні заходи завдавали істотних збитків. В інших випадках володарі використовуваних злочинцем адрес отримували на свої електронні поштові скриньки численні повідомлення про те, що пошту не доставлено (у тих випадках, коли програма Роберта Соловея надсилала листи на ті адреси, які вже не існували). Ці повідомлення були численними, займали багато місця на серверах, а їх видалення спричинило втрати як часу, так і грошей.

У контексті досліджуваного закону дії Роберта Соловея були кваліфіковані як використання захищеного комп'ютера (такими в цій справі були сервери крупних провайдерів та проксі-сервери, що використовувалися для організації зв'язку між штатами) для передавання або перенаправлення комерційних повідомлень електронної пошти з метою введення в оману отримувачів стосовно джерела таких повідомлень (18 U.S.C. 1037 (a)(2)), а також як істотне викривлення інформації, що міститься в заголовку множинного повідомлення, та умисне ініціювання передавання таких повідомлень (18 U.S.C. 1037 (a)(3)). Крім цього, йому були інкриміновані шахрайство, крадіжка ідентифікаційних відомостей та відмивання грошей. Цей приклад, як видається, дає достатньо чіткі аргументи для визначення характеру суспільної небезпечності розповсюдження спаму. Будучи засобом вчинення інших злочинів або певним видом недобросовісної реклами, він спричиняє специфічні наслідки й у сфері використання інформаційних технологій. Ці наслідки полягають у значному ускладненні або навіть узагалі в позбавленні можливості користуватися електронною поштою. У свою чергу, суспільну небезпечність розповсюдження спаму як самостійного посягання у сфері використання інформаційних технологій визначають збитки осіб, які викликані цим ускладненням або неможливістю використання електронної пошти.

CAN-SPAM Act не обмежується засобами кримінально-правового впливу на суспільні відносини, він передбачає також інші заходи правового захисту для осіб, які використовують комерційну електронну пошту (Sec. 5. Other protections for users of commercial electronic mail). Якщо перелічені вище діяння відносяться до 18 титулу Зводу Законів США, який має назву "Злочини та Кримінальний процес", то норми, що передбачають інші заходи правового захисту, відносяться до 15 титулу "Комерція та торговельна діяльність". Такі заходи полягають у встановленні ознак діянь, які слід уважати незаконними та за вчинення яких, відповідно, може наставати цивільна або господарська відповідальність. Ці діяння поділяються на

дві групи: вимоги до передачі сигналів (Requirements for transmition of messages); кваліфіковані порушення,що відносяться до комерційної електронної пошти (Aggravated violations relating to commercial electronic mail).

До діянь першої групи закон відносить:

1) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти або повідомлень про трансакції чи відносини, які містять істотно сфальсифіковану інформацію в заголовку або таку інформацію заголовку, що вводить в оману (під останньою розуміється інформація, яка є технічно правильною, тобто листи дійсно відправлялися з адреси, яка в них зазначена, але можливість надсилання листів з цієї адреси отримана шляхом обману, наприклад, через використання троянської програми) (15 U.S.C. 7704 (a)(1));

2) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, що містить опис предмета (subject heading), сформульований таким чином, щоб ввести в оману отримувача (15 U.S.C. 7704 (a)(2));

3) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить посилання на функціонуючу електронну адресу чи інший подібний механізм, що дозволяє відмовитися від подальшого отримання подібної кореспонденції (15 U.S.C. 7704 (a)(3));

4) ініціювання передачі комерційного повідомлення електронної пошти особі, яка в установленому порядку відмовилася від отримання подібної кореспонденції (15 U.S.C. 7704 (a)(4));

5) ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить чіткої та зрозумілої вказівки на те, що повідомлення є рекламою або особа має можливість відмовитися від отримання такої кореспонденції в подальшому або без вказівки на дійсну фізичну поштову адресу відправника (15 U.S.C. 7704 (a)(5)).

До кваліфікованих порушень, таких, що мають обтяжуючі ознаки, належать:

1) так звані "атаки збору врожаю" та "словникові атаки" (address harvesting and dictionary attacks), які полягають у використанні для розсилання електронних адрес, отриманих шляхом автоматизованої обробки сайтів, у інформаційному наповненні яких спеціально зазначається, що особа, котра оперує сайтом, не надає, не продає, не передає іншим чином представлені на сайті електронні адреси для надсилання на них комерційної інформації, або у використанні для розсилання електронних адрес, отриманих у результаті автоматизованого підбору та перестановок імен, символів, цифр тощо (15 U.S.C. 7704 (b)(1));

2) створення множинних облікових записів електронної пошти для подальшого розсилання комерційних повідомлень електронної пошти шляхом використання засобів автоматизації (15 U.S.C. 7704 (b)(2));

3) ретрансляція повідомлень електронної пошти або повідомлень про трансакції чи відносини, які містять істотно сфальсифіковану інформацію в заголовку або таку інформацію заголовку, що вводить в оману через захищений комп'ютер, доступ до якого отримано несанкціоновано (15 U.S.C. 7704 (b)(3));

4) направлення без спеціального маркування комерційних повідомлень електронної пошти, які містять відомості сексуального характеру, на захищений комп'ютер (15 U.S.C. 7704 (b)(4)).

Прикладом застосування цих засобів правової охорони суспільних відносин у сфері використання електронної пошти може слугувати судове рішення в широковідомому цивільному процесі соціальної мережі Facebook проти так званого "короля спаму" Сенфорда Уоллеса та його спільників. Відповідно до рішення окружного суду Північного округу Каліфорнії Уоллес був зобов'язаний виплатити компенсацію позивачеві в розмірі 710 737 650 доларів США [4]. Аналіз позовної заяви в цій справі дає можливість установити, що свої матеріальні претензії Facebook обґрунтовувала в тому числі й порушенням норм досліджуваного закону, які об'єднані в розглянутому вище розділі. Зокрема, представники Facebook доводили, що Уоллес розповсюджував спам серед користувачів мережі. При цьому розсилання комерційних повідомлень він здійснював від імені інших клієнтів Facebook, незаконно використовуючи їх облікові запи-

си. Ураховуючи те, що в соціальних мережах обмін повідомленнями можливий тільки після взаємної згоди користувачів, дії Уоллеса призводили до того, що клієнти отримували повідомлення рекламного характеру нібито від своїх друзів, колег та ін. Отже, використовуваний механізм розповсюдження спаму значно ускладнював його ідентифікацію, заподіював шкоду користувачам мережі, чим зумовлював втрату репутації та довіри до Facebook. У позовній заяві дії Уоллеса були представлені також як направлення на захищений комп'ютер повідомлень комерційного характеру із заголовками, що вводять в оману (15 U.S.C. 7704 (a)(1)); ініціювання передачі на захищений комп'ютер комерційного повідомлення, що містить оманливий опис предмета (15 U.S.C. 7704 (a)(2)); ініціювання передачі на захищений комп'ютер комерційного повідомлення електронної пошти, яке не містить посилання на функціонуючу електронну адресу чи інший подібний механізм, що дозволяє відмовитися від подальшого отримання подібної кореспонденції (15 U.S.C. 7704 (a)(3)), тощо [5].

Здійснений огляд федерального закону США щодо регулювання відносин у сфері користування комерційною електронною поштою дає змогу зробити кілька важливих висновків.

По-перше, особливу увагу американський законодавець приділяє правовому регулюванню саме комерційної електронної пошти. У такий спосіб вирішується дуже важлива проблема протидії спаму. На законодавчому рівні фіксується класифікація нормативних підходів до масових розсилань залежно від їх змісту. Якщо шляхом масового розсилання здійснюється розповсюдження комп'ютерних вірусів, порнографії чи створюються умови для подальшого вчинення шахрайства, таке розсилання однозначно визнається злочинним і отримує правову оцінку в контексті відповідних законів. Це положення фіксується CAN-SPAM Act у параграфі (c) четвертого розділу. Водночас, якщо масове розсилання являє собою поширення повідомлень рекламного характеру, дії осіб, які його здійснюють, визнаються суспільно небезпечними тільки в разі порушення встановлених правил використання комерційної елек-

тронної пошти. Завдяки цьому досліджуваний нормативний акт ураховує вищевизначену особливість спаму, яка полягає в тому, що він у деяких формах є корисним суспільним явищем. Такий нормативний підхід дозволяє забезпечити баланс позитивних і негативних наслідків криміналізації, оскільки досліджуваний нормативно-правовий акт урешті-решт сприяє цивілізованому розвиткові суспільно корисного сегменту спаму.

Зазначений підхід знаходить відображення і в практиці російських правоохоронних органів. Так, у листопаді 2010 року повідомлялося про порушення кримінальної справи стосовно гендиректора ТОВ "Деспмедіа" Ігоря Гусєва (більше року перебував у Top-10 рейтингу найнебезпечніших спамерів світу, що ведеться Spamhausproject). Згідно з матеріалами справи, на які посилається журнал "Деньги", підозри на адресу Гусєва пов'язані з партнерською програмою Glavmed.com, за допомогою якої в США й Канаді здійснювалися продажі контрафактних фармацевтичних препаратів з Індії. Продукція рекламувалася через спам-розсилання. За три з половиною роки компанія Ігоря Гусєва продала препаратів на суму більше 120 мільйонів доларів США. Прибутки Гусєва від незареєстрованої підприємницької діяльності оцінюються майже у два мільйони доларів [6]. Зазначимо, що кримінально-правова оцінка його діяльності правильно давалася поза контекстом відповідальності за злочини у сфері використання інформаційних технологій. Відповідно до цілком обґрунтованої позиції правоохоронців його дії розглядались як незаконне підприємництво, пов'язане з отриманням прибутків в особливо великому розмірі, тобто злочин у сфері господарської діяльності.

По-друге, американський законодавець у питанні регулювання спаму обрав так звану модель "opt out", яка, на його думку, полягає в тому, що відправник повідомлень не має вводити в оману отримувачів стосовно змісту або джерела таких повідомлень, а отримувачі, у свою чергу, повинні мати можливість відмовитися від подальшого отримання подібної кореспонденції від певного відправника. Інша існуюча модель – "opt in" – значно жорсткіша. Відповідно де неї правомірною є тіль-

ки таке масове розсилання, що здійснюється на електронні адреси отримувачів, які її попередньо замовили.

По-третє, до передбачених американським законодавством нормативних критеріїв суспільної небезпечності направлення множинних комерційних повідомлень електронної пошти слід зараховувати: несанкціоноване використання захищених комп'ютерів, або їх використання для введення отримувачів в оману; фальсифікацію реквізитів електронних листів для унеможливлення ідентифікації відправника; використання для здійснення масових розсилань електронних поштових адрес або доменних імен, зареєстрованих з використанням фальсифікованих відомостей (у таких випадках реквізити листів не фальсифікуються, а неможливість ідентифікації відправника забезпечується шляхом спотворення даних щодо реєстрації адрес джерел повідомлення); використання чужих IP-адрес для здійснення масових розсилань від свого імені.

По-четверте, CAN-SPAM Act пропонує розгалужену систему кваліфікуючих ознак розповсюдження множинних повідомлень комерційного зв'язку. Серед них на окрему увагу заслуговує механізм визначення розміру шкоди, заподіяної масовим розповсюдженням повідомлень електронної пошти, та розміру прибутку, отриманого шляхом учинення злочинів, передбачених досліджуваним законом. Ці ознаки розглядаються в контексті певного проміжку часу. Наприклад, множинне розсилання вважатиметься кваліфікованим не просто тоді, коли злочином заподіяно шкоду в розмірі 5250 доларів, а тоді, коли сума всіх втрат потерпілого, пов'язаних з множинним розсиланням певної особи, склала понад 5000 доларів за один рік. Як видається, таке законодавче рішення найповніше відображає специфіку заподіяння шкоди від спаму. Вона, як правило, складається з великої кількості незначних втрат, які, отримуючи системний характер, із часом набувають значення, достатнього для правової оцінки.

По-п'яте, для розв'язання, або, використовуючи влучний термін з назви закону, контролювання проблеми комерційного спаму американський законодавець не обмежується норма-

ми про кримінальну відповідальність. З метою забезпечення комплексного нормативно-правового впливу CAN-SPAM Act містить також вимоги щодо оформлення комерційної електронної кореспонденції, прозорості механізму зв'язку з відправником та відмови від подальшого отримання подібних листів, законності збирання електронних поштових адрес тощо. З порушенням цих вимог може бути пов'язана цивільна відповідальність відправника повідомлень. При цьому головною рисою, що дозволяє відмежовувати злочини, передбачені CAN-SPAM Act, від цивільно-правових деліктів, є множинність розсилання. У такий спосіб, як видається, досягається ефективне розв'язання проблеми залежності якості правового впливу від небезпечності правопорушення.

Використані джерела:

1. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). Public Law 108-187 [Electronic resource]. – Modeof access:http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

2. U.S. National Information Infrastructure Protection Act of 1996 [Electronic resource] // Electronic privacy information center. – Modeof access:http://epic.org/security/1996_computer_law.html

3. Idictment USA v. Robert Alan Soloway and Newport Internet Marketing Corporation [Electronic resource] // Mortgagespam site. – Modeof access: http://www.mortgagespam.com/soloway/Indictmentfiled.pdf

4. Default Judgment in favor of Facebook, Inc. against Sanford Wallace. Signed by Judge Jeremy Fogel on 10/29/2009 [Electronic resource] // The Justia Federal District Court Filings & Dockets site. – Modeof access: http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/92/

5. Complaint against Sanford Wallace, Adam Arzoomanian, Scott Shaw (Filing fee $ 350.00, receipt number 54611004760.). Filed byFacebook, Inc.. (gm, COURT STAFF) (Filed on 2/24/2009) (Additional attachment(s) added on 3/5/2009: # 1 Civil Cover

Sheet) (gm, COURT STAFF) [Electronic resource] // The Justia Federal District Court Filings & Dockets site. – Mode of access : http://docs.justia.com/cases/federal/district-courts/california/candce/5:2009cv00798/211911/1/0.pdf

6. Вам спам мешает? [Электронный ресурс] // Журнал "Деньги". – 2010. – № 43 (800). – Режим доступа : http://www.kommersant.ru/doc.aspx?fromsearch=600378e1-e0fb-42e3-b978-139ba8b5748e&docsid=1524322

Додаток 5

Практика використання окремих кримінально-правових засобів забезпечення інформаційної безпеки (ст.ст. 176, 361 – 363-1 КК України)

І. Аналіз практики використання кримінального законодавства про відповідальність за "комп'ютерні" злочини (ст.ст. 361 – 363-1 КК)

Перш ніж перейти до результатів, зробимо кілька зауважень, що стосуються методології аналізу. По-перше, більшу частину фактичного матеріалу для дослідження було отримано з Єдиного державного реєстру судових рішень (далі – Реєстр), ведення якого, відповідно до Закону України "Про доступ до судових рішень", забезпечує Державна судова адміністрація України. Станом на грудень 2010 року Реєстр містив інформацію про 167 випадків кваліфікації дій осіб за ознаками складів злочинів, передбачених статтями 361 – 363-1 КК України. Цілком зрозуміло, що Реєстр, з огляду на час його створення, певні організаційно-технічні труднощі початкового етапу його формування й функціонування, не містить ґенеральної сукупності судових рішень зазначеної категорії. Разом із тим, наявні в законі, а також у Постанові Кабінету Міністрів України "Про затвердження Порядку ведення Єдиного державного реєстру судових рішень" від 25.05.2006 № 740 вимоги щодо організації роботи Реєстру дозволяють обґрунтовано стверджувати, що сукупність судових рішень, представлених у ньому, є репрезентативною добіркою.

По-друге, для отримання науково обґрунтованих висновків ми зробимо дворівневу класифікацію випадків застосування досліджуваних норм, ураховуючи особливості змісту ознак відповідних складів злочинів. Тобто кожне з досліджуваних судових рішень спочатку буде віднесено до однієї з груп залежно від того, з використанням якої статті розділу XVI КК воно пов'язане. Після цього для більш детального аналізу в кожній з таких груп буде виділено категорії, які об'єднуватимуть судові

рішення, що характеризуються певною специфікою змісту фактичних складів.

І по-третє, здійснивши класифікацію судових рішень на групи й категорії та використовуючи найбільш обґрунтовані та загальноприйняті положення науки кримінального права щодо змісту поняття "суспільно небезпечне діяння", спробуємо дослідити чинники суспільної небезпечності діянь, із якими пов'язані відповідні судові рішення.

Отже, досліджувані судові рішення за хронологією розподілилися таким чином: у 2005 р. – 2; 2006 р. – 2; 2007 р. – 33; 2008 р. – 31; 2009 р. – 37; 2010 р. – 62. Більш докладна інформація міститься в нижченаведеній таблиці:

Таблиця 1

Кількість випадків кваліфікації дій осіб за ст.ст. 361 – 363-1 КК України за роками

№ з/п	Номер статті розділу XVI КК України	Загальна кількість	2005	2006	2007	2008	2009	2010
1	361	99	1	2	24	21	22	29
2	361-1	15	1	-	2	3	2	7
3	361-2	13	-	-		2	4	7
4	362	40	-	-	7	5	9	19
5	363	0	-	-	-	-	-	-
6	363-1	0	-	-	-	-	-	-
7	РАЗОМ	167	2	2	33	31	37	62

Як можна побачити з таблиці, спостерігається впевнене зростання кількості випадків застосування зазначених норм. Найбільшу групу складають ті, що пов'язані з кримінальною відповідальністю за несанкціоноване втручання в роботу комп'ютерної техніки та мереж електрозв'язку (59,28%). Розгляд цих рішень дозволяє виділити такі категорії: "крадіжка машинного часу", "незаконне підключення до телевізійних

мереж", "незаконне підключення до телефонних мереж", "IP-телефонія", "використання карток-емуляторів", "втручання в роботу радіомереж", "витік", "втрата", "підробка", "блокування", "спотворення процесу обробки", "кілька наслідків".

Найбільш численну категорію несанкціонованих втручань (24,24%) складають незаконні підключення до мереж кабельного телебачення. Такі дії суди правильно кваліфікують як несанкціоноване втручання в роботу мереж електрозв'язку, яке призвело до витоку інформації [3]. Право доступу до інформації, що транслюється в мережах кабельного телебачення, особа отримує шляхом укладання угоди з певною телерадіокомпанією. Відповідно, отримання доступу до такої інформації без укладання угоди є витоком інформації за визначенням. У низці вироків за обвинуваченням осіб у подібних несанкціонованих втручаннях містяться відомості про дослідження судами доказів падіння рівня сигналу в мережі внаслідок дій винної особи. Наявність таких наслідків суди правильно додатково кваліфікували як блокування інформації [64, 65, 74]. Окрему групу в межах несанкціонованих втручань у роботу телевізійних мереж складають випадки незаконного підключення до мереж супутникового телебачення. Вони полягають в отриманні зашифрованої трансляції відповідних програм мовлення шляхом використання спеціальних пристроїв або спеціальних налаштувань тюнерів без укладання угоди з організацією, яка здійснює трансляцію таких програм. У більшості випадків подібні дії правильно кваліфікувались як несанкціоноване втручання в роботу мережі електрозв'язку, що призвело до витоку інформації [39, 37, 60].

До категорії "крадіжки машинного часу" (11,11%) ми віднесли випадки незаконного отримання доступу до інформаційних ресурсів мережі Інтернет від імені та за рахунок інших осіб, які мають право на такий доступ. Як правило, у подібних випадках винна особа використовує чужі ідентифікатори абонента комп'ютерної мережі. Суди здебільшого правильно кваліфікують подібні дії як несанкціоноване втручання, що призводить до витоку та блокування комп'ютерної інформації [90,

13, 54, 5]. Витік має місце, оскільки винна особа отримує доступ до трафіку, не маючи на це права. Інкримінування блокування зумовлене специфікою роботи комп'ютерних мереж, яка полягає в тому, що одночасна робота в мережі двох абонентів з однаковими мережевими ідентифікаторами неможлива. Унаслідок цього, коли винна особа з використанням чужих логінів і паролів здійснює доступ до певних інформаційних ресурсів, особа, яка має право доступу до них (зазвичай на підставі угоди з провайдером), позбавляється такої можливості. Залежно від технічних особливостей незаконного отримання доступу до інформаційних ресурсів провайдера, крім витоку та блокування, у деяких випадках суди додатково кваліфікували дії винних осіб як порушення порядку маршрутизації або як спотворення порядку обробки комп'ютерної інформації [81, 76].

Наступну групу складають несанкціоновані втручання в роботу телефонних мереж електрозв'язку (7,07%). Вони полягають у підключенні до телефонного номера потерпілої особи. У контексті ст. 361 КК такі дії розглядаються як несанкціоноване втручання в роботу мереж електрозв'язку, що призводить до: 1) блокування інформації абонента у вигляді неможливості користування телекомунікаційними послугами; 2) спотворення процесу обробки інформації провайдером послуг телефонного зв'язку; 3) порушення встановленого порядку маршрутизації, оскільки телекомунікаційна інформація провайдера фактично не надходила до кінцевого обладнання дійсного абонента, хоча обладнання фіксувало користування абонентом послугою [87, 29, 45].

Із несанкціонованим втручанням у роботу телефонних мереж електрозв'язку пов'язані ще дві категорії: IP-телефонія (13,13%) та використання карток-емуляторів (3,03%).

IP-телефонія являє собою протиправне, вчинене з порушенням правил надання й отримання телекомунікаційних послуг спрямовування отриманого з мережі Інтернет міжнародного телефонного трафіку в телекомунікаційну мережу загального користування України шляхом заміни оригінальних номерів ініціаторів міжнародних телефонних викликів на внутрішньодержавні телефонні номери, тобто несанкціоноване втручання в роботу мереж електрозв'язку, що призвело до підробки, спотворення процесу обробки інформації щодо міжнародного телефонного трафіку та до порушення встановленого порядку її маршрутизації [17, 38].

Усі випадки використання карток-емуляторів [22, 31, 47] пов'язані з незаконним отриманням послуг телефонного зв'язку через мережу таксофонів ВАТ "Укртелеком". Емулятор таксофонної картки ВАТ "Укртелеком" являє собою виготовлений напівпромисловим способом пристрій, функціональне призначення якого – імітувати роботу єдиної таксофонної картки ВАТ "Укртелеком". Перед процесором таксофона емулятор поводиться як одна з реально випущених таксофонних карток і за певних маніпуляцій змінює інформацію в електронному модулі та збільшує вміст лічильника. При використанні емулятора в автоматизованій Системі управління таксофонами ВАТ "Укртелеком" несанкціоновано змінюється інформація про стан лічильників реально випущених карток. Таким чином, використання подібних пристроїв обґрунтовано визнається несанкціонованим втручанням в роботу автоматизованої Системи управління таксофонної мережі ВАТ "Укртелеком", Автоматизованої системи комплексних розрахунків і мережі електрозв'язку ВАТ "Укртелеком", які об'єднані комп'ютерними мережами, що призвело до підробки інформації про стан лічильників телефонних карток та спотворення процесу обробки інформації за показниками лічильників реальних телефонних карт.

Категорія "втручання в роботу радіомереж" є нечисленною (2,02%), але достатньо специфічною, тому заслуговує на окремий розгляд [12, 93]. У цих випадках суди давали кримінально-правову оцінку діям радіоаматорів, які виходили на зв'язок у забороненому діапазоні частот. Їх дії кваліфікувались як несанкціоноване втручання в роботу мережі електрозв'язку, що призвело до блокування в ній інформації. Така кваліфікація зумовлена тим, що робота з передавання сигналу різними радіозасобами на одній і тій самій частоті призводить до ство-

рення радіоперешкод одними засобами телекомунікації іншим.

У категорії "витік" (6,06%) ми об'єднали випадки ознайомлення з певною комп'ютерною інформацією з обмеженим доступом, правова оцінка яким давалася в межах ст. 361 КК: ознайомлення зі змістом електронних поштових скриньок [55, 36, 9], розділів сайту, не призначених для загального доступу [26], відомостями щодо акаунтів користувачів мережі провайдера [80] тощо.

Втрата (4,04%) і підробка (14,14%) комп'ютерної інформації здебільшого (17 судових рішень з 18) мають місце, коли вчинення подібних діянь пов'язане з іншим злочином. Так, дії особи, котра видаляла частину придбаних покупцями товарів із накладних та вносила неправдиву інформацію через електронно-обчислювальну машину, установлену на касі, до комп'ютерної мережі торгового дому, унаслідок чого по касі утворювалися надлишки грошових коштів, що привласнювалися цією особою, були правильно кваліфіковані як привласнення, а також незаконне втручання в роботу комп'ютерної мережі, що призвело до знищення комп'ютерної інформації [60].

Кваліфікація дій осіб як несанкціоноване втручання, що призвело до спотворення процесу обробки інформації (2,02%), також зустрічається у випадках, коли "комп'ютерний" злочин пов'язаний із вчиненням іншого. Так, вироком Голосіївського районного суду м. Києва від 22 березня 2010 року в справі № 1-9/10 засуджено особу, яка змінила програмне забезпечення автоматизованого пункту обміну умовних грошових одиниць, а потім, використовуючи ці зміни, шляхом обману заволоділа майном власника цього пункту [15].

До категорії "блокування" (2,02%) ми віднесли випадки створення перешкод користування інформаційними ресурсами, які не пов'язані з описаними вище "крадіжками машинного часу" [18, 85]. Наприклад, вироком Саксаганського районного суду м. Кривого Рога від 24 липня 2008 року в справі № 1-520/08 засуджено особу, яка шляхом використання спеціальної про-

грами блокувала роботу провайдера та позбавила абонентів комп'ютерної мережі можливості доступу до інформаційних ресурсів мережі Інтернет [85].

У категорію "кілька наслідків" (11,11%) ми об'єднали випадки, що характеризуються настанням кількох наслідків із числа перелічених у диспозиції ст. 361 КК. Наприклад, вироком Рубежанського міського суду Луганської області від 11 вересня 2007 року в справі № 1-289/2007 засуджено особу, яка шляхом введення до клієнтської бази даних провайдера великої кількості довільних різноманітних відомостей (підробка) суттєво порушила його роботу та позбавила абонентів можливості доступу до Інтернету (блокування) [83].

В іншому випадку, правова оцінка якому дається у вироку Алчевського міського суду в Луганській області від 29 лютого 2008 року в справі 1-168 [4], винна особа також здійснила несанкціоноване втручання в роботу комп'ютерної мережі місцевого провайдера, але наслідки цього мали інший характер. Отримавши можливість змінювати інформацію, представлену на сайті провайдера, засуджений знищив інформацію щодо внутрішніх і зовнішніх ресурсів мережі (втрата), а також змінив стартову сторінку місцевого провайдера на зображення порнографічного характеру (підробка). Дії цієї особи були правильно кваліфіковані за сукупністю злочинів, передбачених ч. 1 ст. 301 та ч. 1 ст. 361 КК України.

Наявні в Єдиному реєстрі судових рішень відомості щодо притягнення до кримінальної відповідальності за розповсюдження або збут шкідливих програмних або технічних засобів (15 вироків, або 8,98% від загальної кількості досліджених судових рішень) ми систематизували за п'ятьма категоріями: "збут дисків", "збут технічних засобів", "розповсюдження з використанням комп'ютерних мереж", "використання вірусів для вчинення злочинів", "спеціалізовані програми для порушення авторських прав розробників програмного забезпечення".

Найчастіше (8 судових рішень, або 53,33% у групі) стаття 361-1 КК застосовувалася для притягнення до кримінальної відповідальності осіб, які здійснювали продаж дисків із запи-

саними на них шкідливими програмними засобами [58, 27, 10]. У двох випадках (13,33%) розповсюдження шкідливого програмного забезпечення здійснювалося шляхом надання доступу абонентам локальної мережі до директорії на жорсткому диску комп'ютера винної особи, що містила шкідливі програми [34, 35].

Також двічі суди приймали рішення про кримінальну відповідальність за збут шкідливих технічних засобів (13,33%). У першому випадку таку кваліфікацію отримали дії щодо збуту підробленої картки, призначеної для перегляду закритих супутникових телевізійних каналів [71]. Подібний технічний засіб було обґрунтовано віднесено до шкідливих, оскільки він дозволяє здійснювати несанкціоноване втручання в роботу мереж електрозв'язку, яке призводить до витоку інформації. Інший випадок пов'язаний зі збутом пристрою, призначеного для переривання (якщо з'єднання вже відбулося) та блокування (якщо абонент, що викликається, перебуває в зоні дії працюючого пристрою) з'єднань оператора мобільного зв'язку між абонентами [48].

В окрему категорію ми виділили випадки застосування ст. 361-1 КК, пов'язані з розповсюдженням програм, призначених для використання програмного забезпечення з порушенням авторських прав його розробників [49, 88]. Подібні програми, "кейгенератори", дозволяють обходити засоби захисту програмного забезпечення та використовувати його в повному обсязі, не маючи на це права. Ці випадки заслуговують на окрему категорію, оскільки, як видається, вони є результатом достатньо широкого та вельми спірного тлумачення терміна "шкідлива програма".

Нарешті, в одному випадку розповсюдження шкідливої програми було пов'язане з подальшим вчиненням злочинів [78]. Ідеться про судове рішення, на яке ми вже звертали увагу в контексті розгляду питань відмежування комп'ютерних злочинів від порушення права таємниці кореспонденції. Як розповсюдження шкідливої програми кваліфіковано розміщення на загальнодоступному мережевому інформаційному ресурсі

шкідливого програмного засобу під виглядом програми для роботи з аудіо-файлами. При цьому метою розповсюдження такої програми був подальший доступ до закритої інформації абонентів мережі.

Наступна група судових рішень пов'язана із застосуванням ст. 361-2 КК, яка встановлює відповідальність за розповсюдження або збут комп'ютерної інформації з обмеженим доступом. У цій групі ми виділили такі категорії: "збут дисків", "надання доступу", "розповсюдження файлів даних", "повідомлення відомостей", "кардшаринг".

Більше половини випадків застосування ст. 361-2 КК (61,54%) складають судові рішення, що стосуються кримінально-правової оцінки дій осіб, які здійснюють збут носіїв комп'ютерної інформації (дисків для лазерних систем зчитування [94,95] або жорстких дисків [98]), що містять відомості з обмеженим доступом. Предметом дій винних осіб ставали відомості щодо абонентів телефонної мережі "Укртелеком" [11], дані щодо експортно-імпортних операцій суб'єктів зовнішньоекономічної діяльності, акредитованих у Державній митній службі України [67], електронні ключі для доступу до використання програмного забезпечення [82] тощо.

Розповсюдження комп'ютерної інформації з обмеженим доступом здійснювалося також шляхом розміщення певних відомостей на загальнодоступному інформаційному ресурсі в мережі Інтернет. Так, вироком Каховського міськрайонного суду Херсонської області від 5 липня 2010 року в справі № 1-316/10 було засуджено особу, котра, не маючи дозволу ВАТ "Укртелеком", розмістила на сайті відомості щодо абонентів відповідної телефонної мережі, які мешкають в м. Каховка та Каховському районі Херсонської області [30].

Мало місце і вчинення розгляданого злочину шляхом передавання файлів даних, які містили відомості, що становлять комерційну таємницю підприємства, електронною поштою [96].

При цьому розповсюдження комп'ютерної інформації з обмеженим доступом представлено в судовій практиці не тільки як передавання певних носіїв інформації або файлів даних

чи надання віддаленого доступу до них. Наприклад, у вироку Корольовського районного суду м. Житомира від 10 серпня 2008 року в справі № 1-326/09 як розповсюдження комп'ютерної інформації розглядалося неправомірне повідомлення службовцем банківської установи іншій особі відомостей про стан карт-рахунку певного клієнта. При цьому відомості накопичувалися в автоматизованій інформаційній системі банку [41].

На окрему увагу заслуговує випадок, віднесений нами до категорії "кардшаринг". У дослідженому масиві судових рішень він зустрічається лише один раз [24], однак з великою ймовірністю можна прогнозувати збільшення частки подібних вироків. Такий прогноз обґрунтований постійним зростанням національної аудиторії супутникового телебачення та розвитком інтернет-технологій. За визначенням кардшаринг являє собою метод, завдяки якому декілька ресиверів можуть отримувати доступ до перегляду платних каналів супутникового телебачення та використовувати при цьому тільки одну карту доступу. Зазвичай обладнання, куди встановлюється придбана на законних підставах карта доступу, підключається до Інтернету та використовується як сервер, що здійснює трансляцію потоку даних та дозволяє дешифрувати супутниковий сигнал. Для того щоб мати можливість перегляду платних каналів, не маючи на це права, необхідно з'єднати ресивер з Інтернетом та здійснити підключення до трансляції відповідного сигналу дешифрування. У згаданому вироку було дано кримінально-правову оцінку діям особи, яка пропонувала іншим послуги кардшарингу. Її дії щодо організації перегляду закритого каналу було кваліфіковано як несанкціоноване втручання в роботу мереж електрозв'язку, що призвело до витоку інформації (ст. 361 КК). У свою чергу, розповсюдження потоку даних для дешифрування закритого каналу отримало кваліфікацію за ст. 361-2 КК.

Група судових рішень, що стосуються використання ст. 362 КК, є другою за кількістю (23,95%). У більшості випадків цієї групи (80%) застосування статті 362 КК пов'язане з кваліфікацією дій винних осіб у контексті вчинення інших злочинів. Ці

судові рішення ми систематизували у 6 типових категорій: "переказ грошей", "фіктивне повернення платежів", "маніпуляції з АС енергопостачальників", "введення неправдивої інформації щодо знижки", "оформлення кредитів на підставних осіб", "приховування слідів платежів".

До категорії "переказ грошей" (27,5%) ми віднесли судові рішення, пов'язані з кваліфікацією дій співробітників банківських установ, які, використовуючи доступ до електронних систем платежів, наданий їм у зв'язку з виконуваною роботою, здійснювали незаконний переказ грошей. Такі дії суди правильно кваліфікували як сукупність злочинів, передбачених ст. 191 та ст. 362 КК [52, 77, 57].

Певну варіацію привласнення, пов'язаного з незаконною зміною комп'ютерної інформації, являють собою випадки, об'єднані нами в категорію "фіктивне повернення платежів" (17,5%) [73, 56, 23]. Механізм вчинення подібних злочинів полягав у тому, що особа, яка має доступ до автоматизованої системи обліку матеріальних цінностей, отримує певні платежі, вносить відомості про них до системи, але після цього додатково вносить фіктивні відомості про те, що платіж зроблено помилково, а отже, привласнює одержані таким чином залишки. Наприклад, вироком Богунського районного суду м. Житомира від 13 травня 2010 року в справі № 1-316/2010 засуджено касира-операціоніста відділення № 13 Житомирського регіонального управління публічного акціонерного товариства комерційного банку "ПриватБанк". Перебуваючи на своєму робочому місці, вона неодноразово з метою привласнення коштів осіб, які користувалися послугами банку шляхом доступу до електронної мережі банку за допомогою персонального логіну та пароля, несанкціоновано, без згоди на те клієнтів, скасовувала, а потім знищувала інформацію, що обробляється в автоматизованій системі банку, про здійснення потерпілими платежів за навчання в Житомирському агротехнічному коледжі, після чого ці кошти привласнювала [7].

Достатньо великою є категорія "маніпуляції з АС енергопостачальників" (12,5%) [19, 20]. Такі посягання полягають у

привласненні коштів, сплачених за електроенергію, або приховуванні фактів відсутності відповідних платежів і заподіянні в такий спосіб шкоди енергопостачальним компаніям. Приклад судового рішення цієї категорії ми вже наводили в контексті розгляду ознак складу злочину, передбаченого ст. 362 КК [43].

Вироком Октябрського районного суду м. Полтави від 2 серпня 2010 року в справі № 1-9/10 засуджено чотирьох осіб за привласнення та незаконну зміну комп'ютерної інформації, вчинені особами, які мають право доступу до неї. Злочини було скоєно за таких обставин. Винні особи отримували від клієнтів кошти, які повинні були вносити до каси підприємства, на якому працювали, за постачання товарів. При внесенні даних щодо сплати клієнтами за поставлені товари до автоматизованої інформаційної системи підприємства вони незаконно збільшували відсоток знижки та привласнювали отримані внаслідок цього залишки [68]. Це судове рішення ми віднесли до категорії "введення неправдивої інформації щодо знижки".

Певної поширеності (7,5%) набули випадки, які ми віднесли до категорії "оформлення кредитів на підставних осіб" [8, 42, 97]. Такі злочини полягають у тому, що службовець банку, використовуючи наявний у нього доступ до автоматизованої інформаційної системи установи, вносить до неї неправдиві відомості щодо укладення договору кредитування з певною особою, а після цього привласнює кошти, отримані від імені цієї особи. Наприклад, вироком Богунського районного суду м. Житомира від 9 листопада 2009 року в справі № 1-468/2009 [8] засуджено особу А., котра згідно з відповідними наказами "ПриватБанку" була спеціалістом по роботі з кредитними картками Житомирського регіонального управління КБ "ПриватБанк", а також матеріально відповідальною особою, на зберіганні у якої знаходилися неактивовані кредитні картки клієнтів банку, та яка мала право доступу до електронної інформації щодо кредитних карток клієнтів банку, що обробляється у внутрішньобанківській комп'ютерній мережі – програмному комплексі "Приват 48", та зміни цієї інформації. Вона вчинила

умисні злочини за таких обставин. Перебуваючи на своєму робочому місці, використовуючи закріплений за нею логін і пароль, А. увійшла до програмного комплексу "Приват 48", де оброблялася інформація щодо електронного договору, укладеного між "ПриватБанк" і Б., на ім'я якої автоматично за банківською програмою "Конвеєр" було виготовлено неактивовану кредитну картку "Універсальна". До цього електронного договору винна особа, зловживаючи своїм службовим становищем та порушуючи вимоги відповідних внутрішніх наказів, без відома Б. умисно внесла несанкціоновані зміни, а саме: у полі "Телефон мобільний" ввела дані про номер свого мобільного телефону та зберегла ці відомості в програмному комплексі "Приват 48". Того ж дня, використовуючи власний мобільний телефон, зателефонувала до "CALL"-центру КБ "ПриватБанк" та в автоматичному режимі провела активацію кредитної картки Б. Після цього з метою погашення обов'язкового щомісячного мінімального платежу винна особа в полі "Джерело погашення" зазначеного електронного договору ввела номер своєї зарплатної картки, а також змінила в договорі інформацію про розмір кредитного ліміту картки на ім'я Б., збільшивши його з 4200 грн. до 7000 грн. Аби приховати свої злочинні дії, умисно змінила в цьому електронному договорі інформацію про номер свого мобільного телефону. У результаті цього А. отримала безпосередній доступ до грошових коштів банку, що знаходилися на активованій кредитній карточці на ім'я Б., та можливість ними розпоряджатися. У подальшому, використовуючи цю кредитну картку, умисно, зловживаючи своїм службовим становищем, заволоділа грошовими коштами банку на загальну суму 11690 грн. шляхом зняття готівки через банкомати м. Житомира.

Окрему категорію випадків застосування ст. 362 КК складають судові рішення, пов'язані з кваліфікацією дій осіб, які використовують доступ до інформаційних систем з метою приховання злочинних дій [72,21]. Прикладом може слугувати вирок Оржицького районного суду Полтавської області від 24 вересня 2007 року в справі № 1-87/2007 [72]. Відповідно до цього

судового рішення засуджено П., який, працюючи на посаді оператора-касира зали ігральних автоматів, будучи матеріально відповідальною особою та маючи вільний доступ до комп'ютера для введення ставок ігральних автоматів, ввів через управляючий комп'ютер системи "Jeckpot" грошові ставки в кредит до ігрального автомата на загальну суму 6479 грн. При цьому гроші в касу зали ігральних автоматів не вносив та не проводив введену до ігрального автомата суму через касовий апарат. Усі внесені у вигляді ставок кошти П. протягом своєї зміни програв. Після вчинення цих дій, маючи намір не повертати до каси зали ігральних автоматів грошового еквіваленту програних ставок та бажаючи приховати вчинене, він за допомогою управляючого комп'ютера знищив інформацію в системі керування ігральними автоматами.

Решта випадків використання ст. 362 КК, представлених судовими рішеннями, наявними в Єдиному реєстрі (20%), не пов'язана із вчиненням інших злочинів. Ці випадки ми розподілили за трьома категоріями залежно від особливостей об'єктивної сторони посягань: "зміна інформації" (5%), "знищення інформації" (10%) та "копіювання інформації, що призвело до витоку" (5%).

Типовим прикладом судового рішення категорії "знищення" є вирок Лисичанського міського суду Луганської області від 10 липня 2009 року в справі № 1-460/2009. Ним було засуджено особу, котра, маючи намір помститися за своє звільнення, але ще перебуваючи на посаді, яка передбачає право доступу до автоматизованої системи підприємства, знищила в ній файли зі службовою документацією [53].

Прикладом судового рішення категорії "копіювання інформації, що призвело до витоку" може слугувати вирок Крюківського районний суду м. Кременчука Полтавської області від 2 квітня 2010 року в справі № 1-103/2010. У цьому випадку суд кваліфікував дії винного за ч. 2 ст. 362 КК України. Так, винний протягом серпня – жовтня 2009 року, маючи право доступу до інформації, що зберігається у його робочому персональному комп'ютері та на сервері комп'ютерної мережі КБ

ВАТ "Кредмаш", учинив несанкціоноване копіювання інформації – робочих файлів із розробками "Гроход Дайлида" розробки іншого співробітника підприємства, асфальтозмішувальних установок: "ДС-1863", "ДС-1857", "КДМ-201", які становлять комерційну таємницю ВАТ "Кредмаш" та повинні зберігатися в конструкторському бюро підприємства, та виніс цю інформацію за межі ВАТ "Кредмаш", що призвело до її витоку, який виявився в можливості ознайомлення із цією інформацією сторонніх осіб, котрі не мали права доступу до неї [46].

Таким чином, проведена робота щодо систематизації випадків застосування норм про кримінальну відповідальність за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку дозволила виділити в кожній групі судових рішень, пов'язаній із застосуванням конкретної статті розділу XVI, категорії, що об'єднуються певною специфікою ознак відповідних складів злочинів. Отримані результати представлено у відповідній таблиці.

Таблиця 2

Групи та категорії кримінальних справ, пов'язаних із застосуванням статей 361 – 363-1 КК України

№ з/п	Стаття розділу XVI КК, з застосуванням якої пов'язана група кримінальних справ	Категорії, виділені в межах групи	Абсолютна кількість випадків	Відсоток від кількості випадків в групі
1	361	крадіжка машинного часу	11	11,11
		незаконне підключення до телевізійних мереж	24	24,24
		незаконне підключення до телефонних мереж	7	7,07

Продовження таблиці

		IP-телефонія	13	13,13
		використання картокемуляторів	3	3,03
		втручання в роботу радіомереж	2	2,02
		витік	6	6,06
		втрата	4	4,04
		підробка	14	14,14
		блокування	2	2,02
		спотворення процесу обробки	2	2,02
		кілька наслідків	11	11,11
2	361-1	збут дисків	8	53,33
		збут технічних засобів	2	13,33
		розповсюдження з використанням комп'ютерних мереж	2	13,33
		використання вірусів для вчинення злочинів	1	6,67
		спеціалізовані програми для порушення авторських прав розробників програмного забезпечення	2	13,33
3	361-2	збут дисків	8	61,54
		надання доступу	1	7,69
		розповсюдження файлів даних	1	7,69
		повідомлення відомостей	2	15,38
		кардшаринг	1	7,69
4	362	переказ грошей	11	27,5
		фіктивне повернення платежів	7	17,5
		маніпуляції з АС енергопостачальників	5	12,5
		введення неправдивої інформації щодо знижки	4	10
		оформлення кредитів на підставних осіб	3	7,5

Продовження таблиці

		приховування слідів платежів	2	5
		зміна інформації	2	5
		знищення інформації	4	10
		копіювання інформації, що призвело до витоку	2	5

У свою чергу, запропонована класифікація дозволяє перейти до основного завдання дослідження практики застосування кримінального законодавства про злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку, а саме до аналізу чинників суспільної небезпечності діянь, із якими пов'язані відповідні судові рішення.

На нашу думку, не потребує додаткової аргументації така теза: суспільна небезпечність "комп'ютерних" злочинів, що вчиняються з метою подальшого вчинення інших злочинів (проти власності, конституційних прав, у сфері службової діяльності тощо), зумовлена небезпечністю останніх та заперечень не викликає. Таким чином, у межах досліджуваної групи видається можливим виділити таку категорію випадків, які характеризуються суспільною небезпечністю через те, що пов'язані із вчиненням іншого злочину. Цю категорію складають 64 випадки (38,32%), які за складами досліджуваних злочинів розподілилися таким чином: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361) – 27 випадків (27,27% серед судових рішень, пов'язаних із застосуванням цієї норми); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1) – 2 випадки (13,33%); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих

системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2) – 3 випадки (23,08%); несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362) – 32 випадки (80%).

Певна частина досліджених випадків характеризується тим, що внаслідок незаконних дій з комп'ютерною інформацією створювалися перешкоди в діяльності підприємств, установ чи організацій. За такі посягання засуджено п'ять осіб, або 2,99% від загальної кількості досліджених випадків застосування норм розділу XVI КК. Три особи засуджено за вчинення злочинів, передбачених ст. 361 КК [86, 13, 14], а дві – за ст. 362 КК [75].

Вироком Сарненського районного суду Рівненської області в справі № 1-221/2008 від 8 серпня 2008 року [86] було засуджено В., який, використовуючи домашній комп'ютер та підключення до мережі Інтернет, здійснив несанкціоноване втручання в роботу автоматизованої системи товариства з обмеженою відповідальністю "Торговий Дім «Північ-Центр»" міста Сарни Рівненської області, а саме комп'ютера магазину "Сам Маркет" цього ТОВ, на якому розміщувалася програма "1С-Бухгалтерія", і несанкціоноване знищення з нього файлу словника бази даних. У результаті видалення файлу програмою "1С-Бухгалтерія" було блоковано надходження інформації з касових апаратів магазину "Сам Маркет" до головного офісу ТОВ "Торговий Дім «Північ-Центр»" і спотворено процес обробки цієї інформації. Таким чином, у наведеному випадку суспільна небезпечність знищення інформації зумовлена тим, що внаслідок цього було порушено нормальну роботу підприємства торгівлі.

Інші два випадки пов'язані з блокуванням комп'ютерної інформації та характеризуються однаковими чинниками суспільної небезпечності [13, 14]. Одне із судових рішень ми вже

докладно розглядали. Ідеться про вирок Голованівського районного суду Кіровоградської області в справі № 1-156/08 від 16 вересня 2008 року [14] за обвинуваченням особи, яка користувалася послугами Інтернет від імені та за рахунок місцевої податкової адміністрації. У ході судового розгляду досліджено той факт, що через дії зловмисника працівники податкової адміністрації були позбавлені можливості працювати зі звітною інформацією платників податків, яка надходила на їх електронну адресу. Саме те, що внаслідок блокування було створено перешкоди в роботі державної установи, і зумовлює суспільну небезпечність комп'ютерного злочину в цих випадках та обґрунтовує доцільність притягнення винних осіб до кримінальної відповідальності.

Нарешті, вироком Павлоградського міськрайсуду Дніпропетровської області в справі № 1-0473-2008 від 22 квітня 2008 року [75] двох осіб (А. та Б.) засуджено за вчинення злочину, передбаченого ст. 362 КК. Злочин скоєно за таких обставин. А. призначили на посаду фахівця з організації управління відділу організації праці та заробітної плати шахти "Дніпровська" ОАО "Павлоградвугілля", у зв'язку з чим вона отримала доступ до інформації, що обробляється в корпоративній комп'ютерній мережі підприємства.

Б., який раніше працював на тому самому підприємстві, але був звільнений за власним бажанням, вирішив поновитися за попереднім місцем роботи. До звільнення його функціональні обов'язки полягали в забезпеченні цілісності баз даних та комп'ютерних програм ОАО "Павлоградвугілля", тому Б. був обізнаний з особливостями їх функціонування. З метою в посаді спеціаліста відділу інформаційних систем керування департаменту інформаційних технологій Б. вирішив вивести з ладу деякі програми комп'ютерної мережі шахти шляхом вилучення електронних довідників баз даних з жорсткого диска сервера шахти. Він усвідомлював, що це призведе до повної непрацездатності програмного забезпечення й унеможливить функціонування деяких відділів підприємства. Він розрахову-

вав, що це змусить керівництво шахти звернутися до нього, а отже сприятиме його поновленню на роботі.

Б. схилив А. до участі у вчиненні задуманого посягання. А., виконуючи вказівки, які Б. давав їй по телефону, скопіювала електронні довідники баз даних у приховану директорію, а в робочій директорії їх знищила. Унаслідок цього роботу програмного забезпечення комп'ютерів виробничих і управлінських відділів шахти та доступ до їх інформації було заблоковано.

В описаному випадку суспільна небезпечність вчиненого посягання зумовлена ускладненнями функціонування виробничого підприємства, що виникли через несанкціоновані дії з комп'ютерною інформацією.

В одному з досліджених випадків суспільна небезпечність посягання може бути обґрунтована збитками, заподіяними власникові інформації внаслідок її знищення. Так, вироком Южноукраїнського міського суду Миколаївської області в справі № 1-138/2007 від 22 червня 2007 року [99] особу було засуджено за злочин, передбачений ч. 1 ст. 362, до одного року виправних робіт. Злочин вчинено за таких обставин. Винну особу було прийнято на роботу на посаду інженера з комплектації обладнання. Крім того, згідно з розпорядженням керівництва до її обов'язків входило ведення в автоматизованій системі "Парус-підприємство" прибутково-видаткової документації. Коли винна особа дізналася, що її переводять на іншу ділянку роботи, вона з метою нашкодити колишньому керівництву знищила комп'ютерну інформацію щодо 178 видаткових накладних та 145 прибуткових ордерів, чим заподіяла матеріальні збитки в сумі 1284,4 грн. Отже, у цьому випадку суд, приймаючи рішення щодо суспільної небезпечності вчиненого діяння, дослідив характер і зміст заподіяних матеріальних збитків.

Серед досліджених судових рішень також можна виділити ті, що стосуються порушення конституційних прав громадян [55, 36, 9]. Усі вони пов'язані з кваліфікацією за ст. 361 КК діянь, які полягали в незаконному ознайомленні зі змістом елек-

тронних поштових скриньок. Суспільна небезпечність цих посягань може бути обґрунтована тим, що в розглядних випадках порушення права власності на комп'ютерну інформацію спричиняє порушення конституційного права таємниці кореспонденції. На нашу думку, у таких випадках більш правильною буде кваліфікація за ст. 163 КК (відповідний прецедент ми вже неодноразово згадували [78]). Однак, не порушуючи питання щодо правильності кваліфікації, ще раз зазначимо, що ці випадки можуть бути визнані суспільно небезпечними, оскільки завдають шкоди конституційним правам громадян.

Віднесення решти досліджених посягань до таких, які можна визнавати суспільно небезпечними, є спірним. Їх кількість – 94 (56,29%). За складами досліджуваних злочинів ці випадки розподілилися таким чином: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361) – 66 випадків (66,67% серед судових рішень, пов'язаних із застосуванням цієї норми); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1) – 13 випадків (86,67%); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2) – 10 випадків (76,92%); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362) – 5 випадків (12,5 %).

Конкретизуємо наведені дані з урахуванням визначених раніше категорій. У групі випадків, пов'язаних із застосуванням ст. 361 КК, до суспільно небезпечних слід відносити категорії "втрата", "підробка" та "спотворення процесу обробки". Із 20 випадків цих категорій 19 пов'язані із вчиненням інших

злочинів, в одному – незаконні дії з інформацією призвели до перешкоджань у роботі підприємства. Категорії "витік", "кілька наслідків" та "крадіжки машинного часу" містять як випадки, що можуть обґрунтовано вважатися суспільно небезпечними, так і випадки, віднесення яких до суспільно небезпечних є спірним. Категорія "витік" об'єднує 6 випадків. Чотири з них можна віднести до суспільно небезпечних: в одному випадку комп'ютерний злочин пов'язаний із вчиненням іншого; три випадки характеризуються порушенням конституційних прав громадян (таємниця кореспонденції). Віднесення решти випадків цієї категорії [80, 26] до суспільно небезпечних посягань видається необґрунтованим. Так, вироком Прилуцького міськрайонного суду Чернігівської області в справі № 1-200/2010 від 29 липня 2010 року [80] Б. засуджено за вчинення злочину, передбаченого ч. 1 ст. 361 КК. Винний за допомогою спеціального програмного забезпечення отримав доступ до облікового запису користувача комп'ютерної мережі ТОВ "Телерадіокомпанія ТІМ", зареєструвавшись у системі під його логіном, одержав особистий пароль доступу до його електронної пошти, до лог-файлів виходів на сайт http://yellowcard.tim.ua та лог-файлів помилок цього сайту. Слід погодитися з висновком суду стосовно того, що відповідно до визначень термінів, наведених у ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", вчинене є витоком інформації. Однак жодних фактичних даних, які б свідчили про суспільну небезпечність цього витоку, суд не досліджував. Як можна побачити з вироку, факт ознайомлення з кореспонденцією потерпілої особи доведено не було, а отже, таємницю кореспонденції не порушено. Шкода, заподіяна провайдерові через ознайомлення зі службовими файлами, не досліджувалася.

Схожа ситуація спостерігається й у вироку Зарічного районного суду м. Суми в справі № 1-512/10 від 28 вересня 2010 року [26]. Цим судовим рішенням особу засуджено за незаконне втручання в роботу автоматизованої системи інформаційного порталу, що належить ТОВ "Інфолайн 1", та копію-

вання на жорсткий диск власного комп'ютера повної резервної копії цього сайту. Копія містила файли та базу даних цього інтернет-ресурсу, доступ до яких звичайним користувачам інтернет-сайту обмежений. Заподіяна цим копіюванням шкода не досліджувалася, що знову ж таки порушує питання про суспільну небезпечність описаного у вироку посягання.

Серед посягань, об'єднаних у категорію "крадіжки машинного часу", тільки два (загальна кількість – 11) можна віднести до суспільно небезпечних. Як ми вже зазначали, блокування комп'ютерної інформації, яким зазвичай характеризуються "крадіжки машинного часу", у цих випадках спричиняло перешкоди в роботі державної установи [13, 14]. Водночас інші випадки "крадіжок машинного часу", як свідчить практика національних судів [81, 76, 90, 40, 28, 92, 70, 54, 5], уже не можна вважати суспільно небезпечними. Наприклад, вироком Інгулецького районного суду м. Кривого Рога Дніпропетровської області в справі № 1-6/609 від 7 травня 2009 року [28] засуджено особу, яка використовувала реквізити доступу до Інтернету, що належали певному суб'єктові господарської діяльності. Її було визнано винною у вчиненні несанкціонованого втручання в роботу комп'ютерної мережі, яке призвело до блокування інформації, та призначено покарання у вигляді штрафу в розмірі 8000 гривень (до речі, відповідно до одного з попередньо згаданих вироків, пов'язаних з блокуванням інформації податкової адміністрації, винну особу було засуджено до штрафу в розмірі 1020 грн.). При цьому питання шкоди, заподіяної внаслідок цього блокування, не досліджувалося. Більше того винна особа зазначала, що користувалася чужими реквізитами доступу в неробочій час, тобто не створювала перешкод для роботи потерпілої особи. Цивільний позов в кримінальній справі не подавався, відповідно, і значної матеріальної шкоди заподіяно не було. Зрозуміло, що цей випадок характеризується як мінімум значно меншою суспільною небезпечністю, однак з точки зору чинної редакції ст. 361 КК наведені випадки небезпечні однаково, адже для кваліфікації за ч.1 ст. 361 КК не вимага-

ється встановлення шкоди, зумовленої блокуванням інформації.

У категорії "кілька наслідків" 7 з 11 випадків можуть бути визнані суспільно небезпечними, оскільки пов'язані із вчиненням інших злочинів. У решті судових рішень шкода, крім установлення фактів блокування, підробки чи знищення інформації, не досліджувалася, що виключає можливість обґрунтованого висновку щодо суспільної небезпечності відповідних посягань.

Суспільну небезпечність посягань, віднесених до категорій "незаконне підключення до телевізійних мереж" та "незаконне підключення до телефонних мереж", можна обґрунтувати таким чином. По суті, ці посягання являють собою отримання телекомунікаційних послуг особами, які не мають на це права. Видається, що притягнення до кримінальної відповідальності за такі діяння буде обґрунтованим у випадках, коли наявні ознаки складу злочину, передбаченого ст. 192 КК, або, як у відповідних випадках "крадіжок машинного часу", коли дії винної особи створюють такі перешкоди в користуванні телекомунікаційною мережею, які свідчать про суспільну небезпечність посягання. Інакше кажучи, незаконне отримання телекомунікаційної послуги обґрунтовано вважати суспільно небезпечним у тих випадках, коли воно: 1) заподіяло таку матеріальну шкоду, якої достатньо для притягнення до кримінальної відповідальності в загальному випадку отримання оплатної послуги без оплати (ст. 192 КК), при цьому аргументи на користь того, що отримання в такий спосіб саме телекомунікаційних послуг є більш суспільно небезпечним, видаються непереконливими; або 2) спричинило суспільно небезпечні перешкоди в отриманні телекомунікаційних послуг іншими абонентами певної мережі. З огляду на вищезазначене жодне з досліджених посягань категорій "незаконне підключення до телевізійних мереж" та "незаконне підключення до телефонних мереж" не може вважатися суспільно небезпечним. Так, за самовільне підключення до мережі кабельного телебачення, що

розглядається як несанкціоноване втручання в роботу мережі електрозв'язку, яке призвело до витоку або порушення порядку маршрутизації інформації, що передається цією мережею, вироками Краснолуцького міського суду Луганської області в справі № 1-208 від 4 квітня 2007 року [44], Замостянського районного суду м. Вінниці в справі № 1-249/08 від 27 березня 2008 року [25], Новокаховського міського суду Херсонської області в справі № 1-266/08 від 13 червня 2008 року та в справі № 1-344/08 від 19 серпня 2008 року [63; 62], Новомосковського міськрайсуду Дніпропетровської області в справі № 1-748/09 від 1 жовтня 2009 року [66] тощо винних осіб було засуджено переважно до одного року позбавлення волі. Однак, по-перше, ці судові рішення не містять вказівки на шкоду, достатню для притягнення до кримінальної відповідальності за ст. 192 КК. По-друге, специфічних наслідків для інших абонентів відповідних мереж електрозв'язку суди не досліджували або досліджували формально (вказівки на протоколи вимірювання рівня сигналу в мережі кабельного телебачення). Виникає справедливе питання: чи настільки небезпечними є такі несанкціоновані підключення до мережі кабельного телебачення, щоб визнавати їх злочинними та призначати настільки серйозне покарання?

Не можна віднести до суспільно небезпечних і посягання категорії "IP-телефонія". Тут головне проблемне питання полягає в тому, що саме конституює шкоду, заподіяну ними. У певних судових рішеннях цієї категорії зазначається, що такою шкодою є недоотриманий прибуток операторів зв'язку [17, 61, 38, 50]. Описана вище специфіка подібних дій вимагає критичного аналізу наведених висновків. Справа в тому, що при вчиненні діянь, які відносяться до цієї категорії, послуг зв'язку відповідні оператори не надають, телекомунікаційний сигнал не проходить відповідними мережами. Отже, заподіяна операторам шкода зумовлена наявністю на ринку зв'язку агентів, які, порушуючи встановлені правила, надають дешевші послуги. Можливо, прибуток, отриманий у такий спосіб, дає підстави

казати про застосування ст. 202 КК або подібна шкода може бути підставою для господарсько-правової відповідальності. Однак, її інкримінування в контексті відповідальності за злочин, передбачений ст. 361 КК, видається необґрунтованим. Візьмемо на себе сміливість припустити, що такі або подібні міркування стали причиною відсутності в більшості судових рішень цієї категорії вказівки на шкоду [89, 84, 33, 51, 59, 32, 16, 100]. Зазначене яскраво свідчить про те, що віднесення подібних діянь до суспільно небезпечних посягань у сфері інформаційних технологій є спірним, а притягнення осіб, що їх вчиняють, до кримінальної відповідальності – недоцільним. Аргументів на користь останнього висновку додає і той факт, що в п'яти судових рішеннях розгляданої категорії [89, 33, 59, 32, 16] шкода не досліджувалася, а витрати на експертизу становили від 776 грн. [89] до 14939 грн. [16].

Через відсутність дослідження характеру та змісту заподіяної шкоди до спірних щодо суспільної небезпечності слід віднести й випадки категорії "втручання в роботу радіомереж" [93, 12]. Як ми вже зазначали, ці посягання полягали в здійсненні виходів у радіоефір в забороненому діапазоні. У судових рішеннях обґрунтовано зазначається: загальні принципи роботи радіопристроїв дозволяють стверджувати, що використання кількох пристроїв в одному діапазоні призводить до створення перешкод, може блокувати обмін даними. Однак питання про те, які саме дані блокувалися та наскільки це було суспільно небезпечним, не досліджувалося.

Нарешті, три випадки категорії "використання карток-емуляторів" також необґрунтовано зараховувати до суспільно небезпечних посягань. Сутність діянь, що об'єднані в цій категорії, полягає в безоплатному отриманні телекомунікаційних послуг. Як ми вже зазначали, подібні посягання мають отримувати кримінально-правову оцінку в межах ст. 192 КК. Проте в кожному з розглянутих випадків розміру заподіяної шкоди було недостатньо для притягнення до кримінальної відповідальності за цією нормою.

У групі випадків, пов'язаних із застосуванням ст. 361-1 КК, до суспільно небезпечних доцільно відносити лише два посягання (13,33%) [78, 49]. У цих випадках розповсюдження шкідливих засобів здійснюється з метою подальшого вчинення протиправних діянь: незаконного доступу до електронної пошти [78], використання програмного забезпечення з порушенням авторського права [49]. Саме це й виступає достатнім аргументом для того, щоб вважати ці діяння суспільно небезпечними. Водночас складно визнати суспільно небезпечними дії особи, яка надає вільний доступ до шкідливих програмних засобів, що записані на жорсткому диску власного комп'ютера, користувачам локальної мережі студентського гуртожитку. Однак вироком Кіровського районного суду міста Кіровограда в справі № 1-440/08 від 8 грудня 2008 року [35] таку особу визнано винною у вчиненні злочину, передбаченого ст. 361-1 КК України, та засуджено до штрафу в розмірі 1500 грн. Так само вельми спірною є суспільна небезпечність завантаження з загальнодоступних інтернет-ресурсів шкідливого програмного забезпечення, запис його на диск та збут цього диску [58, 6]. Таким чином, випадки цієї групи категорій "збут дисків" та "надання доступу з використанням мережі" не можуть бути віднесені до суспільно небезпечних, оскільки відповідні судові рішення не містять відомостей про те, чи створювали подібні діяння небезпеку заподіяння певної шкоди. Таку само аргументацію можна застосувати й до вироків категорії "розповсюдження технічних засобів". Разом із тим, усі ці судові рішення слід визнавати правомірними, адже чинний закон установлює відповідальність за розповсюдження шкідливих програм і технічних засобів, не пов'язуючи її з настанням певної шкоди або створенням небезпеки її настання.

У групі, що об'єднує випадки притягнення до кримінальної відповідальності за розповсюдження або збут комп'ютерної інформації з обмеженим доступом (ст. 361-2), до суспільно небезпечних ми віднесли три посягання, пов'язані із вчиненням інших злочинів [82, 41]. Решта випадків наочно демонструють

вади чинного законодавства. Як ми зазначали, систематичне тлумачення чинного КК приводить до висновку про надлишковість заборони. Розгляд статті 361-2 КК у контексті інших норм КК, що передбачають відповідальність за незаконні дії з інформацією з обмеженим доступом, свідчить, що зазвичай вона може застосовуватися в тих випадках, які не можна вважати суспільно небезпечними. Так, вироками, що належать до розгляданої групи та віднесені до найбільш вагомої категорії "збут дисків", за ст. 361-2 КК засуджено 8 осіб (61,54% від загальної кількості засуджених за цією нормою). І лише в одному випадку можна казати про те, що особу засуджено за суспільно небезпечне діяння [82]. Предметом збуту був електронний ключ, який дозволяє використовувати з порушенням авторського права інформаційно-довідковий програмний комплекс "Ліга-закон". У решті випадків [98, 94, 95, 67, 11] осіб було засуджено за розповсюдження баз даних з відомостями щодо абонентів "Укртелекому", власників автотранспорту, зовнішньоекономічних операцій, зареєстрованих Державною митною службою, тощо. При цьому жодне з цих судових рішень не містить відомостей про те, що предмет розповсюдження або збуту отриманий суб'єктом злочину злочинним шляхом. Отже, більшість судових рішень цієї групи пов'язані із засудженням осіб, які розповсюджували комп'ютерну інформацію з обмеженим доступом, але зобов'язань щодо збереження цих відомостей в таємниці не мали. Такий саме висновок маємо зробити й щодо випадку, віднесеного до категорії "надання доступу" [30].

На окрему увагу заслуговує випадок, що належить до категорії "розповсюдження файлів даних". Вироком Красногвардійського районного суду м. Дніпропетровська в справі № 1-173-2010 від 20 серпня 2010 року [96] за розповсюдження комп'ютерної інформації з обмеженим доступом засуджено заступника начальника служби економічної безпеки комерційного підприємства. Шляхом використання робочого комп'ютера та електронної пошти він передав відомості, що становлять комерційну таємницю підприємства (дані про дебіторську заборгова-

ність контрагентів), представникам інших господарюючих суб'єктів. При цьому в судовому рішенні не досліджуються питання змісту та розмірів шкоди, заподіяної підсудним. Отже, використання ст. 232 КК у розгляданому випадку виключається, оскільки кримінальна відповідальність за розголошення комерційної таємниці настає лише тоді, коли такими діями заподіяно істотну шкоду суб'єктові господарської діяльності. За логікою чинного кримінального законодавства підсудному, щоб уникнути кримінальної відповідальності, достатньо було роздрукувати дані, які становлять комерційну таємницю, та надіслати їх звичайною поштою. Наведений приклад ще раз свідчить про те, що відсутність чітких критеріїв суспільної небезпечності у відповідних нормах щодо кримінальної відповідальності за посягання у сфері інформаційних технологій зумовлює появу судових рішень, які є цілком правосудними, але достатньо спірними з позицій доцільності.

Подібну аргументацію маємо використати й при дослідженні вироку категорії "кардшаринг". Нагадаємо, що за ст. 361-2 у даному випадку кваліфіковано розповсюдження потоку даних для дешифрування закритого каналу супутникового телебачення. Цілком очевидно, що ознак суспільної небезпечності подібні діяння набувають у контексті аналізу шкоди, заподіяної господарюючому суб'єктові, який здійснює трансляцію зашифрованого каналу для авторизованих користувачів. У свою чергу, розглядане судове рішення не містить жодних відомостей із цього питання.

Група досліджуваних випадків застосування ст. 362 КК характеризується найбільшою кількістю судових рішень, що містять чіткі показники суспільної небезпечності вчинених діянь (87,5%). Проте п'ять із них ми віднесли до таких, які є спірними з точки зору суспільної небезпечності. Усі вони характеризуються спільною рисою – не містять відомостей щодо шкоди, заподіяної злочином. Так, вироком Печерського районного суду м. Києва в справі № 1-365/09 від 2 липня 2009 року [79] за вчинення злочину, передбаченого ч. 1 ст. 362 КК, засуджено

адміністратора з тестування послуг відділу тестування Департаменту розвитку інформаційних систем закритого акціонерного товариства "Український мобільний зв'язок" (ЗАТ "УМЗ"). Використовуючи доступ до корпоративної автоматизованої системи, він вносив зміни у відомості щодо підключення певних абонентів до мережі, а також щодо статусу та кредитних лімітів певних номерів контрактних абонентів. При цьому питання заподіяної шкоди не досліджувалося, хоча покарання було застосовано достатньо вагоме – штраф у розмірі 10200 грн.

Вироком Феодосійського міського суду АР Крим в справі № 1-307/09 від 24 червня 2009 року [91] засуджено економіста зі збуту електричної енергії абонентського відділу ВАТ "Крименерго". Маючи відповідно до посадової інструкції бухгалтера абонентської групи з розрахунків із фізичними особами право доступу до інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованій системі "Мегабілинг" і зберігається на носіях інформації ВАТ "Крименерго", та використовуючи закріплену за нею ПЕОМ, без оформлених належним чином рішень комісії ВАТ "Крименерго" винна особа неодноразово несанкціоновано в особових рахунках абонентів змінювала інформацію про суми штрафів, нарахованих їм за Актами про порушення правил користування електричною енергією, шляхом внесення і зміни в особових рахунках абонентів сум штрафів. Їй було відомо, що така інформація, згідно з Інструкцією, вноситься і змінюється тільки на підставі належно оформленого рішення комісії. Проте вона робила це, тому що на той період у їх організації було встановлено певний порядок роботи. Попередній розрахунок штрафу робився нею, а потім на засіданні комісії, відповідно до прийнятого рішення, сума штрафу могла змінитися, оскільки абоненти надавали комісії документи, на підставі яких робився перерахунок штрафу. Будь-яких корисливих мотивів при несанкціонованій зміні інформації вона не мала. Як і в попередньому випадку, жодних даних щодо заподіяної шкоди не наводиться.

Вище ми згадували вирок Лисичанського міського суду Луганської області в справі № 1-460/2009 від 10 липня 2009 року, яким було засуджено особу, котра з помсти за своє звільнення, але ще перебуваючи на посаді, що передбачає право доступу до автоматизованої системи підприємства, знищила в ній файли зі службовою документацією [53]. Аналіз цього судового рішення залишає без відповіді питання про те, наскільки важливою була інформація, знищена підсудною, та яку шкоду у зв'язку з цим було заподіяно. Принагідно зазначимо, що існує й інше судове рішення щодо кваліфікації подібних діянь. У згадуваному раніше вироку Южноукраїнського міського суду Миколаївської області в справі № 1-138/2007 від 22 червня 2007 року [99] така шкода досліджується. Саме це в останньому випадку і свідчить про дійсну суспільну небезпечність діяння, якому дається кримінально-правова оцінка.

Два наступні вироки пов'язані з кваліфікацією копіювання комп'ютерної інформації з обмеженим доступом [69, 46]. Вироком Орджонікідзевського районного суду м. Запоріжжя в справі № 1-59/2009 від 17 липня 2010 року [69] засуджено начальника відділу маркетингу ТОВ "Інфоком ЛТД". Діючи умисно, з метою несанкціонованого копіювання інформації, яка обробляється в комп'ютерній мережі підприємства та є його комерційною таємницею, використовуючи засоби операційної системи Microsoft Windows та маючи доступ до локальної комп'ютерної мережі, винний скопіював із сервера на жорсткий диск закріпленого за ним ноутбука файли, що містили відомості про організацію роботи підприємства. У подальшому ці дані використовувалися в роботі іншого підприємства, до якого перейшов працювати підсудний. Застосування норм про відповідальність за незаконне збирання або розголошення відомостей, що становлять комерційну таємницю (ст.ст. 231 і 232 КК) у цьому випадку виключається через відсутність шкоди, заподіяної ТОВ "Інфоком ЛТД", у вироку вона не досліджується. Знову ж таки доходимо висновку, що обґрунтування кри-

мінальної відповідальності тільки формою подання інформації є явно недостатнім.

Нарешті, до судових рішень, що пов'язані з посяганнями, суспільна небезпечність яких є спірною, ми віднесли вирок Крюківського районного суду м. Кременчука Полтавської області в справі № 1-103/2010 від 2 квітня 2010 року. Як ми зазначали, у цьому випадку кримінально-правову оцінку дано діям інженера, який скопіював комп'ютерні дані щодо певних технічних розробок та намагався винести їх за межі конструкторського бюро. У судовому рішенні витік розуміється як створення можливості ознайомлення з інформацією сторонніх осіб, які не мають права доступу до неї [46]. Якщо у випадках, які наводилися раніше, можна було допустити, що наслідки незаконних дій з комп'ютерною інформацією фактично мали місце, але в ході судового слідства не розглядалися, то в цьому випадку чітко вказується на відсутність наслідків.

Отже, здійснений нами аналіз практики застосування норм КК про відповідальність за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку дозволяє зробити такий висновок: практика національних судів містить рішення, у яких застосування кримінальної відповідальності до осіб, котрі вчиняли комп'ютерні злочини, було пов'язане з посяганнями, які дійсно є суспільно небезпечними (43,71%). Разом із тим, більше половини судових рішень досліджуваної категорії (56,29%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є достатньо спірним.

Достатньо вагомим аргументом, що підтверджує зроблений висновок, є практика застосування судами положень ст. 75 КК щодо звільнення від покарання за досліджувані злочини. Із 167 розглянутих судових рішень позбавлення волі застосовується у 99 (59,28%), обмеження волі – у 29 (17,37%), виправні роботи – у 4 (2,4%), громадські роботи – в 1 (0,6%), штраф – у 31 (18,56%). У двох випадках покарання не призначалося, в одному – було застосовано амністію. Тобто в 79,04% випадків суди призначали таке покарання, яке дозволяє звільнення від нього

з випробуванням. У цій групі практично у 9 випадках з 10 в подальшому приймалося рішення про звільнення від покарання з випробуванням (89,39%). Так, при призначенні покарання у вигляді позбавлення волі засуджені особи звільнялися від покарання з випробуванням у 90,91% випадків, при призначенні обмеження волі – у 89,66%. Загальний показник звільнення від покарання з випробуванням склав 70,66%. При цьому, за офіційними даними судової статистики, загальний рівень звільнення від покарання з випробуванням в Україні складав: у 2007 році – 55,3%, у 2008 – 52,2%, у 2009 – 48,2% [1, 2].

Досліджуючи питання покарання за злочини у сфері використання інформаційних технологій, не можна не звернути увагу й на очевидну непослідовність відповідних судових рішень. Серед досліджених випадків маємо такі приклади: три роки позбавлення волі за незаконне підключення до мережі кабельного телебачення [66] і один рік виправних робіт за знищення складської документації [99]; штраф у розмірі 1020 гривень за використання Інтернету від імені та за рахунок податкової адміністрації, яке призвело до блокування податкових звітів [14], та штраф у розмірі 8000 гривень за використання Інтернету від імені та за рахунок суб'єкта господарської діяльності без настання очевидної шкоди для останнього [28].

II. Аналіз практики використання кримінального законодавства про відповідальність за порушення авторського права на програмне забезпечення (ст.176 КК)

Дане дослідження практики було здійснене для підтвердження тези щодо недостатньої ефективності кримінально-правової протидії порушенням авторського права на програмне забезпечення. Використовуючи Єдиний державний реєстр судових рішень, за пошуковим запитом по категоріям "вирок", "кримінальне судочинство", "176", "комп'ютерна програма", "Adobe", "Microsoft" було отримано відомості щодо 103 судових рішень. Враховуючи, що програмне забезпечення компаній Adobe та Microsoft є найбільш поширеним, а також специфіку

нормативно-правової регуляції реєстру, отриману сукупність можна обґрунтовано вважати репрезентативної добіркою.

Дослідження показало, що 9,7% судових рішень (10 вироків) пов'язані із засудженням за діяння, які необґрунтовано відносити до суспільно небезпечних. Так, вироком Червонозаводського районного суду м. Харкова від 24 червня 2010 р в справі №1-232/10 [106] засуджено особу, яка передала (вирок не містить відомостей щодо продажу) іншій особі диск зі збіркою комп'ютерних програм. Шляхом вільного доступу винна особа отримала ці програми з мережі Інтернет та самостійно за допомогою власного комп'ютера записала на оптичний диск. Зазначені дії розглядаються як незаконне розповсюдження комп'ютерних програм, що завдало матеріальної шкоди у великому розмірі, оскільки ринкова вартість легальних версій програмних продуктів, які були предметом посягання, дорівнює 22338 грн. У вироку Харцизького міського суду Донецької області від 15 липня 2008 року в справі №1-296/2008 [117] кримінально-правова оцінка дається діям особи, що виявлялися в завантаженні з Інтернету та встановленні на особистий комп'ютер одного програмного продукту (Adobe Photoshop 7.0). Зауважимо, що у двох наведених прикладах кримінально-правова оцінка давалася не тільки зазначеним діям. Розглядані судові рішення містять відомості й про вчинення звинуваченими дійсно суспільно небезпечних діянь, таких як реалізація великої кількості дисків з контрафактним програмним забезпеченням. Однак самостійна кваліфікація дій, наведених як приклади, видається недоречною. Більш рельєфно ця проблема виявляється в судових рішеннях, пов'язаних виключно з діяннями, які доволі спірно відносити до суспільно небезпечних. Так, вироком Приморського районного суду м. Одеси від 12 травня 2010 року в справі № 1-395/10 [109] було засуджено особу, котра продала іншій свій комп'ютер із встановленим на ньому програмним забезпеченням, ринкова вартість якого становить 6166 грн. Вироком Центрально-Міського районного суду м. Макіївки Донецької області від 26 січня 2010 року в справі № 1-222/2010 [105] засуджено особу, яка придбала диск з нелі-

цензійним програмним забезпеченням на одному з ринків міста та встановила його на комп'ютер третьої особи. Зазначається, що встановлення на комп'ютер, який використовується для особистих цілей, стандартного пакета програм – операційної системи, програм для роботи з текстом та графікою – заподіяло шкоду в розмірі 11414 грн. Подібні обставини наводяться й у вироку Куп'янського міськрайонного суду від 3 лютого 2011 року в справі № 1-77/2011 [115]. Вироком Свердловського міського суду Луганської області від 24 березня 2011 року в справі № 1-299/11 [118] засуджено особу, яка, перебуваючи у себе вдома встановила на два системні блоки іншої особи комп'ютерну програму Adobe Photoshop CS3, ринкова вартість якої становить 6502 грн., чим заподіяла компанії Adobe Systems Inc. шкоду в розмірі 13004 грн. Вироком Суворовського районного суду м. Одеси від 10 червня 2010 року в справі № 1-670/2010 [113] засуджено А., який на прохання Б. завантажив на власний комп'ютер з мережі Інтернет програмне забезпечення для роботи з графічною інформацією "Adobe Photoshop creative suit 4", записав його на оптичні диски (3 шт.) та передав Б. за 80 грн. При цьому, як зазначається у вироку, заподіяв шкоду в розмірі 20736 грн. (ринкова вартість програмного продукту). Подібні обставини зустрічаються й у вироку Соснівського районного суду м. Черкаси від 8 грудня 2010 року в справі № 1-740/10 [114] та вироку Приморського районного суду м. Одеси від 23 листопада 2010 року в справі № 1-1918/2010 [104]. Уважаємо, що застосування в цих випадках засобів кримінально-правової протидії навряд чи можна розглядати як адекватне небезпечності посягання реагування держави на прояви порушення інтелектуальної власності. Аргументів на користь цієї тези додає й порівняння комплексних законодавчих оцінок суспільної небезпечності. Якщо для ч. 1 ст. 176 Іксосн = 40,62, то чи можна розглядати наведені приклади як близькі за рівнем суспільної небезпечності до таких посягань, як: ухилення від сплати податків, якщо воно призвело до фактичного ненадходження до бюджетів чи державних цільових фондів коштів у великих розмірах (ч. 2 ст. 212, Іксосн = 34,66)

або опір працівникові правоохоронного органу, державному виконавцеві під час виконання ним службових обов'язків, члену громадського формування з охорони громадського порядку та державного кордону або військовослужбовцеві під час виконання цими особами покладених на них обов'язків щодо охорони громадського порядку (ч. 2 ст. 341, Ікзосн = 38,85)?

Разом із тим, більшість досліджених вироків (90,2%) пов'язані з кваліфікацією діянь, які обґрунтовано можна вважати суспільно небезпечними. Однак специфіка цієї сукупності судових рішень полягає в тому, що віднесення відповідних посягань до суспільно небезпечних пов'язане з ознаками, які переважно не належать до складу злочину, але характеризують діяльність обвинувачених як таку, яка дійсно є істотним порушенням прав інтелектуальної власності та потребує реакції держави у вигляді застосування засобів кримінальної юстиції.

Так, усю сукупність судових рішень, пов'язаних із фактично суспільно небезпечними посяганнями на авторські права розробників програмного забезпечення, можна, на нашу думку, поділити на три категорії: "продаж" (32% від загальної кількості досліджених вироків), "використання" (38,8%), "встановлення" (18,4%).

До категорії "продаж" ми віднесли вироки, пов'язані з кваліфікацією діянь, що полягають у реалізації дисків з контрафактним програмним забезпеченням у підприємствах торгівлі [119], на ринках [101], у спеціально обладнаних торгових точках, комп'ютерних клубах, за оголошенням тощо. Подібний продаж програмного забезпечення, ураховуючи обставини, що свідчать про систематичність діяльності, слід розглядати як достатньо потужний засіб поширення "комп'ютерного піратства" в Україні, тому застосування кримінально-правових засобів у таких випадках є обґрунтованим. Справді, якщо порівнювати систематичне надання послуг з продажу дисків з неліцензійним програмним забезпеченням та разовий продаж або передачу таких дисків, то очевидною стає різниця суспільної небезпечності цих дій та недоцільність їх однакової кримінально-правової оцінки. Однак використовуваний порядок об-

числення шкоди від порушення авторського права призводить до того, що зазначені види порушень розглядаються як однакові за ступенем суспільної небезпечності та кваліфікуються за ч. 1 ст. 176. Вищезазначене підтверджується і судовою практикою: як просте порушення авторського права розглядаються і згадані раніше випадки разового продажу дисків з неліцензійним програмним забезпеченням [113, 114, 104] (у вироках відсутні відомості, які б дозволили зробити інший висновок), і випадки продажу дисків з неліцензійним забезпеченням, вчинених особами, котрі систематично займалися подібною діяльністю, наприклад здійснювали пошук покупців шляхом подачі рекламного оголошення в спеціалізованих виданнях [120, 112].

У межах категорії "використання" об'єднано судові рішення, пов'язані з кваліфікацією незаконного використання програмного забезпечення суб'єктами господарської діяльності. Ідеться про використання неліцензійного програмного забезпечення в комп'ютерних клубах [103], на підприємствах для здійснення документообігу [108], виконання робіт щодо опрацювання графічної інформації [111] тощо. Суспільна небезпечність цієї групи випадків зумовлена тим, що незаконне використання об'єктів авторського права здійснюється з метою отримання прибутку, а відповідно, поширення подібних видів діяльності формує попит на неліцензійне програмне забезпечення та врешті-решт сприяє розвиткові "комп'ютерного піратства". Цим обґрунтовується використання засобів кримінальної юстиції у випадках, віднесених до категорії "використання". Саме тому, як видається, спірним є зарахування до суспільно небезпечних посягань на інтелектуальну власність установлення контрафактного програмного забезпечення на комп'ютер, що використовується в особистих цілях (згаданий раніше вирок Харцизького міського суду Донецької області від 15 липня 2008 року в справі № 1-296/2008 [117]). Хоча зважаючи на ч. 1 ст. 176 КК та наявне розуміння змісту категорії "значна шкода", використання неліцензійного програмного забезпечення з метою отримання прибутку та використання його в особистих цілях слід розглядати як однакові.

Категорія "встановлення" об'єднує судові рішення, пов'язані з кваліфікацією діянь, що полягають у незаконному встановленні на комп'ютерну техніку контрафактного програмного забезпечення. Подібні дії зазвичай вчиняються працівниками підприємств з надання сервісних послуг [1] або підприємств, що здійснюють торгівлю комп'ютерною технікою [110]. Досить поширеними є також вироки, пов'язані з кваліфікацією діяльності фізичних осіб, які систематично на платній основі надають послуги щодо встановлення неліцензійного програмного забезпечення [107]. Цю категорію можна розглядати як окремий вид "продажу", а тому подібним є й обґрунтування доцільності використання в таких випадках засобів кримінальної юстиції, оскільки зазначена діяльність являє собою систематичне поширення неліцензійного програмного забезпечення. Розглядана категорія справ так само чітко демонструє неможливість розмежування суспільно небезпечних видів порушення авторського права і тих, які такими не є, шляхом використання ознаки "заподіяння значної шкоди". Так, якщо порівнювати, наприклад, продаж власного комп'ютера із встановленим програмним забезпеченням (згаданий раніше вирок Приморського районного суду м. Одеси в справі від 12 травня 2010 року № 1-395/10 [109]) та продаж комп'ютеру з встановленим програмним забезпеченням у підприємстві торгівлі [102], стає очевидним, що другий випадок слід розглядати як суспільно небезпечний, а перший – ні. Водночас якщо предметом першого і другого виступає однакове програмне забезпечення, то з позицій ч. 1 ст. 176 КК такі діяння є однаковими.

Матеріали узагальнення практики
та кримінальні справи, використані в огляді:

1. Аналіз стану здійснення судочинства судами загальної юрисдикції в 2008 р. [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу: http://www.scourt.gov.ua/clients/vs.nsf/0/9DDE825F47D1FAF

3C225766A0041BF8D?OpenDocument&CollapseView&RestrictToCategory=9DDE825F47D1FAF3C225766A0041BF8D&Count=500&)

2. Аналіз стану здійснення судочинства судами загальної юрисдикції в 2009 р. [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу: http://www.scourt.gov.ua/clients/vs.nsf/0/09F805995C5F5CA6C2257752002A196D?OpenDocument&CollapseView&RestrictToCategory=09F805995C5F5CA6C2257752002A196D&Count=500&)

3. Кримінальна справа № 1-159/08 // Архів Краснолуцького міського суду Луганської області

4. Кримінальна справа № 1-16/8 // Архів Алчевського міського суду в Луганській області.

5. Кримінальна справа № 1-325/10 // Архів Алчевського міського суду в Луганській області.

6. Кримінальна справа № 1-377/10 // Архів Балаклейського районного суду Харківської області.

7. Кримінальна справа № 1- 316/2010 // Архів Богунського районного суду м. Житомира.

8. Кримінальна справа № 1-468/2009 // Архів Богунського районного суду м. Житомира.

9. Кримінальна справа справа № 1-487/07 // Архів Богунського районного суду м. Житомира.

10. Кримінальна справа № 1-163/10 // Архів Боровського районного суду Харківської області.

11. Кримінальна справа № 1-482/2010 // Архів Броварського міськрайонного суду Київської області.

12. Кримінальна справа № 1-46/2010 // Архів Великолепетиського районного суду Херсонської області.

13. Кримінальна справа № 1-154/2008 // Архів Голованівського районного суду Кіровоградської області.

14. Кримінальна справа № 1-156/08 // Архів Голованівського районного суду Кіровоградської області.

15. Кримінальна справа № 1-9/10 // Архів Голосіївського районного суду м. Києва.

16. Кримінальна справа № 1-326/2008 // Архів Дергачевського районного суду Харківської області.

17. Кримінальна справа № 1-433/2009 // Архів Деснянського районного суду м. Чернігова.

18. Кримінальна справа № 1-900/07 // Архів Дзержинського районного суду м. Харкова.

19. Кримінальна справа № 1-184 2007 // Архів Дружковського міського суду Донецької області.

20. Кримінальна справа № 1-88/10 // Архів Єланецького районного суду Миколаївської області.

21. Кримінальна справа № 1-348/10 // Архів Єнакіївського міського суду Донецької області.

22. Кримінальна справа № 1-169/2008 // Архів Жмеринського міськрайонного суду Вінницької області.

23. Кримінальна справа № 1-212/2009 // Архів Жовтневого районного суду м. Дніпропетровська.

24. Кримінальна справа № 1- 594/2010 // Архів Заводського районного суду м. Запоріжжя.

25. Кримінальна справа № 1-249/08 // Архів Замостянського районного суду м. Вінниці.

26. Кримінальна справа № 1-512/10 // Архів Зарічного районного суду м. Суми.

27. Кримінальна справа № 1-435/2010 // Архів Ізюмського міськрайонного суду Харківської області.

28. Кримінальна справа № 1-6/609 // Архів Інгулецького районного суду м. Кривого Рога Дніпропетровської області.

29. Кримінальна справа № 1-377/2007 // Архів Каховського міськрайонного суду Херсонської області.

30. Кримінальна справа № 1-316/10 // Архів Каховського міськрайонного суду Херсонської області.

31. Кримінальна справа № 1-94/2008 // Архів Київського районного суду м. Сімферополя Автономної Республіки Крим

32. Кримінальна справа № 1- 714/09 // Архів Київського районного суду м. Харкова.

33. Кримінальна справа № 1-43/09 // Архів Кіровського районний суд міста Кіровограда.

34. Кримінальна справа № 1-57/08 // Архів Кіровського районний суд міста Кіровограда.

35. Кримінальна справа № 1-440/08 // Архів Кіровського районний суд міста Кіровограда.

36. Кримінальна справа № 1-182/2010 // Архів Ковпаківського районного суду м. Суми.

37. Кримінальна справа № 1-410/2010 // Архів Коломийського міськрайонного суду Івано-Франківської області.

38. Кримінальна справа № 1-182/2010 // Архів Корабельного районного суду м. Миколаєва.

39. Кримінальна справа № 1-221/2010 // Архів Корабельного районного суду м. Миколаєва.

40. Кримінальна справа № 1-162/2009 // Архів Корольовського районного суду м. Житомира.

41. Кримінальна справа №1-326/09 // Архів Корольовського районного суду м. Житомира.

42. Кримінальна справа № 1-44/2010 // Архів Коростенського міськрайонного суду Житомирської області

43. Кримінальна справа № 1-56/2007 // Архів Косівського районного суду Івано-Франківської області.

44. Кримінальна справа № 1-208/7 // Архів Краснолуцького міського суду Луганської області.

45. Кримінальна справа № 1-87/2010 // Архів Кривоозерського районного суду Миколаївської області.

46. Кримінальна справа № 1-103/2010 // Архів Крюківського районного суду м. Кременчука Полтавської області.

47. Кримінальна справа № 1-691/2007 // Архів Ленінського районного суду м. Вінниці.

48. Кримінальна справа № 1-133/10 // Архів Ленінського районного суду м. Кіровограда.

49. Кримінальна справа № 1-789/10 // Архів Ленінського районного суду м. Луганська.

50. Кримінальна справа № 1-321/2007 // Архів Ленінського районного суду м. Миколаєва.

51. Кримінальна справа № 1-37/09 // Архів Ленінського районного суду м. Севастополя.

52. Кримінальна справа № 1-279/2010 // Архів Лисичанського міського суду Луганської області.

53. Кримінальна справа № 1-460/2009 // Архів Лисичанського міського суду Луганської області.

54. Кримінальна справа № 1-1037/2005 // Архів Лисичанського міського суду Луганської області.

55. Кримінальна справа № 1-40/10 // Архів Лутугінського районного суду Луганської області.

56. Кримінальна справа № 1-345/2008 // Архів Луцького міськрайонного суду Волинської області.

57. Кримінальна справа № 1-435/2010 // Архів Луцького міськрайонного суду Волинської області.

58. Кримінальна справа № 1-1012/07 // Архів Малиновського районного суду м. Одеси.

59. Кримінальна справа № 1-0169/2007 // Архів Місцевого Комінтернівського районного суду м. Харкова.

60. Кримінальна справа № 1-23/10 // Архів Млинівського районного суду Рівненської області.

61. Кримінальна справа № 1-210/2010 // Архів Новозаводського районного суду міста Чернігова.

62. Кримінальна справа № 1-344/08 // Архів Новокаховського міського суду Херсонської області.

63. Кримінальна справа 1-266/08 // Архів Новокаховського міського суду Херсонської області.

64. Кримінальна справа № 1-941/09 // Архів Новомосковського міськрайонного суду Дніпропетровської області.

65. Кримінальна справа № 1-885/09 // Архів Новомосковського міськрайонного суду Дніпропетровської області.

66. Кримінальна справа № 1-748/09 // Архів Новомосковського міськрайонного суду Дніпропетровської області.

67. Кримінальна справа № 1-359 // Архів Оболонського районного суду м. Києва.

68. Кримінальна справі № 1-9/10 // Архів Октябрського районного суду м. Полтави.

69. Кримінальна справа № 1-59/2009 // Архів Орджонікідзевський районний суд м. Запоріжжя.

70. Кримінальна справа № 1-395/09 // Архів Орджонікідзевський районний суд м. Маріуполя Донецької області.

71. Кримінальна справа № 1-815/2009 // Архів Орджонікідзевського районного суду м. Запоріжжя..

72. Кримінальна справа № 1-87/2007 // Архів Оржицького районного суду Полтавської області.

73. Кримінальна справа №1-0604/2008 // Архів Павлоградського міськрайонного суду Дніпропетровської області.

74. Кримінальна справа № 1-58/09 // Архів Павлоградського міськрайонного суду Дніпропетровської області.

75. Кримінальна справа № 1-0473/2008 // Архів Павлоградського міськрайонного суду Дніпропетровської області.

76. Кримінальна справа № 1-17/2010 // Архів Перевальського районного суду Луганської області.

77. Кримінальна справа №1-51/10 // Архів Першотравенського міського суду Дніпропетровської області.

78. Кримінальна справа № 1-235/2008 // Архів Першотравневого районного суду м. Чернівці.

79. Кримінальна справа № 1-365/09 // Архів Печерського районного суду м. Києва.

80. Кримінальна справа № 1-200/2010 // Архів Прилуцького міськрайонного суду Чернігівської області.

81. Кримінальна справа № 1-1472/10 // Архів Приморського районного суду м. Одеси.

82. Кримінальна справа № 1-517/2010 // Архів Приморського районного суду м. Одеси.

83. Кримінальна справа № 1-289/2007 // Архів Рубежанського міського суду Луганської області.

84. Кримінальна справа № 1-25/07 // Архів Саксаганського району м. Кривого Рога Дніпропетровської області.

85. Кримінальна справа № 1 - 520/08 // Архів Саксаганського районного суду м. Кривого Рога Дніпропетровської області.

86. Кримінальна справа № 1-221/2008 // Архів Сарненського районного суду Рівненської області.

87. Кримінальна справа № 1-240/2010 // Архів Смілянського міськрайонного суду Черкаської області.

88. Кримінальна справа № 1-246/05 // Архів Станічно-Луганского районного суду Луганської області.

89. Кримінальна справа № 1-321/10 // Архів Суворовського районного суду м. Херсона.

90. Кримінальна справа № 1-545/07 // Архів Суворовського районного суду м. Херсона.

91. Кримінальна справа № 1-307/09 // Архів Феодосійського міського суду АР Крим.

92. Кримінальна справа № 1-202/09 // Архів Центрального районного суду м. Сімферополя АР Крим.

93. Кримінальна справа № 188/2010 // Архів Цюрупинського районного суду Херсонської області.

94. Кримінальна справа № 1-0384/2008 // Архів Червоногвардійського районного суду м. Дніпропетровська.

95. Кримінальна справа № 1-019/2010 // Архів Червоногвардійського районного суду м. Дніпропетровськ.

96. Кримінальна справа № 1-173/2010 // Архів Червоногвардійського районного суду м. Дніпропетровська.

97. Кримінальна справа № 1-144/2009 // Архів Червоногвардійського районного суду м. Дніпропетровська.

98. Кримінальна справа № 1-1331/08 // Архів Шевченківського районного суду м. Києва.

99. Кримінальна справа № 1-138/2007 // Архів Южноукраїнського міського суду Миколаєвської області.

100. Ухвала колегії суддів судової палати у кримінальних справах апеляційного суду Хмельницької області від 26 грудня 2006 р. [Електронний ресурс] // Єдиний державний реєстр судових рішень. – Режим доступу: http://www.reyestr.court.gov.ua/

101. Кримінальна справа № 1- 79/2010 // Архів Переяслав-Хмельницького міськрайонного суду Київської області.

102. Кримінальна справа № 1-101/10 // Архів Іванівського районного суду Херсонської області.

103. Кримінальна справа № 1-101/2009 // Архів Миколаївського районного суду Львівської області.

104. Кримінальна справа № 1-1918/2010 // Архів Приморського районного суду м. Одеси.

105. Кримінальна справа № 1-222/2010 // Архів Центрально-Міського районного суду м. Макіївки Донецької області.

106. Кримінальна справа № 1-232/10 // Архів Червонозаводського районного суду м. Харкова.

107. Кримінальна справа № 1-378/2008 // Архів Крюківського районного суду м. Кременчука Полтавської області.

108. Кримінальна справа № 1-39/2008 // Архів Жидачівського районного суду Львівської області.

109. Кримінальна справа № 1-395/10 // Архів Приморського районного суду м. Одеси.

110. Кримінальна справа № 1-468/11 // Архів Святошинського районного суду м. Києва.

111. Кримінальна справа № 1-502/10 // Архів Джанкойського міськрайонного суду Автономної республіки Крим.

112. Кримінальна справа № 1-555/11 // Архів Новомосковського міськрайонного суду Дніпропетровської області.

113. Кримінальна справа № 1-670/2010 // Архів Суворовського районного суду м. Одеси.

114. Кримінальна справа № 1-740/10 // Архів Соснівського районного суду м. Черкаси.

115. Кримінальна справа № 1-77/2011 // Архів Куп'янського міськрайонного суду.

116. Кримінальна справа №1-196/10 // Архів Авдіївського міського суду Донецької області.

117. Кримінальна справа №1-296/2008 // Архів Харцизького міського суду Донецької області.

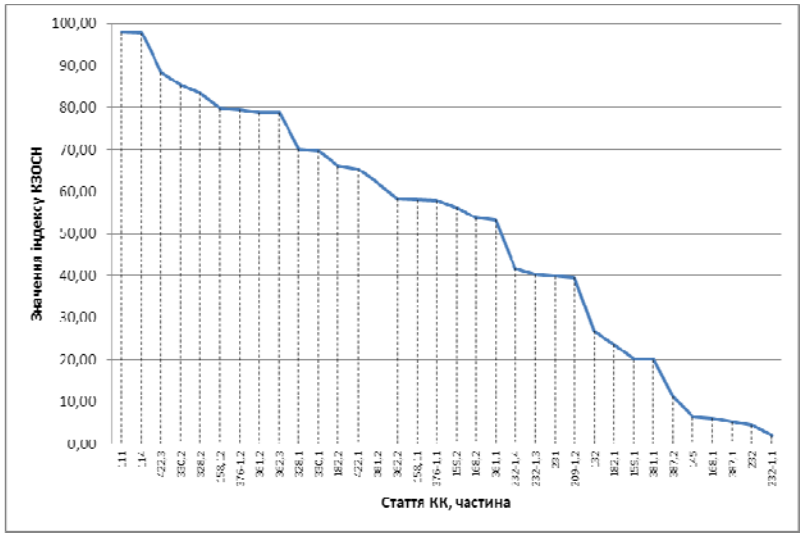
118. Кримінальна справа №1-299/11 // Архів Свердловського міського суду Луганської області.

119. Кримінальна справа №1-543/10 // Архів Калінінського районного суду м. Донецька.

120. Кримінальна справа №1-809/2010 // Архів Тернопільського міськрайонного суду Тернопільської області.

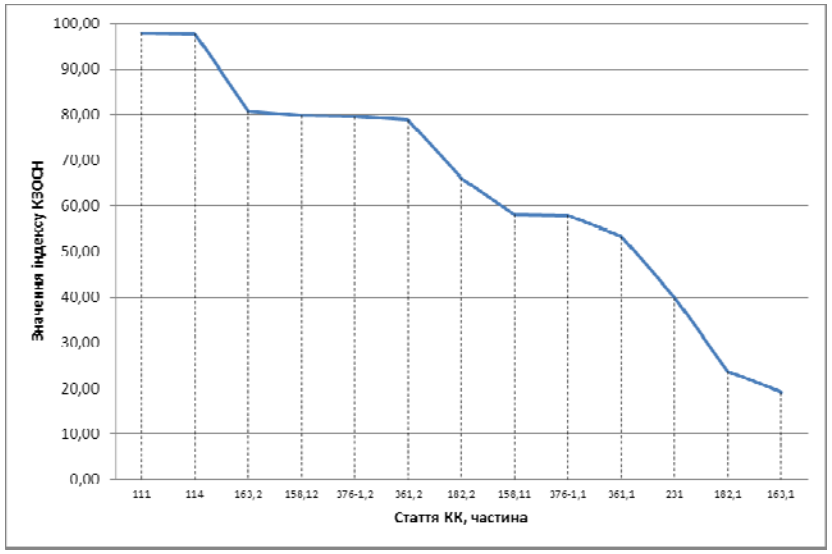
Додаток 6

Графічне представлення результатів аналізу методом контекстної законодавчої оцінки суспільної небезпечності діяння законів про кримінальну відповідальність за незаконне надання доступу до інформації



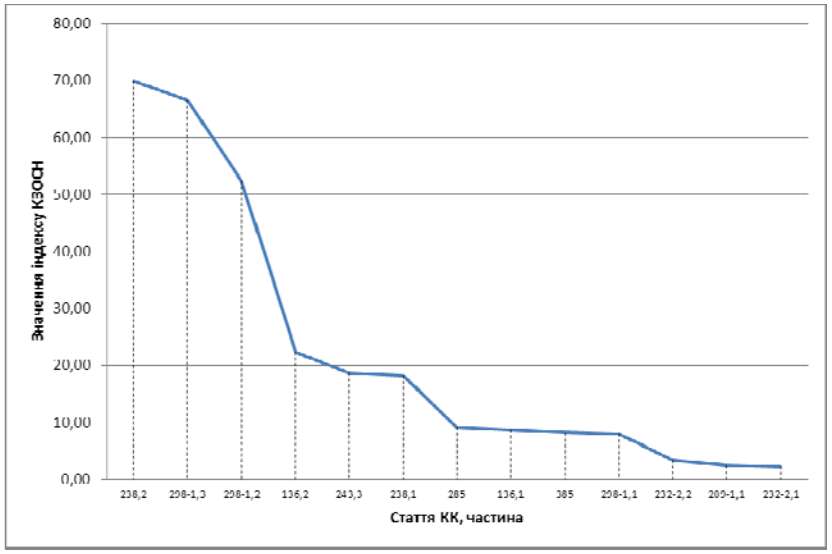
Додаток 7

Графічне представлення результатів аналізу методом контекстної законодавчої оцінки суспільної небезпечності діяння законів про кримінальну відповідальність за незаконне отримання доступу до інформації



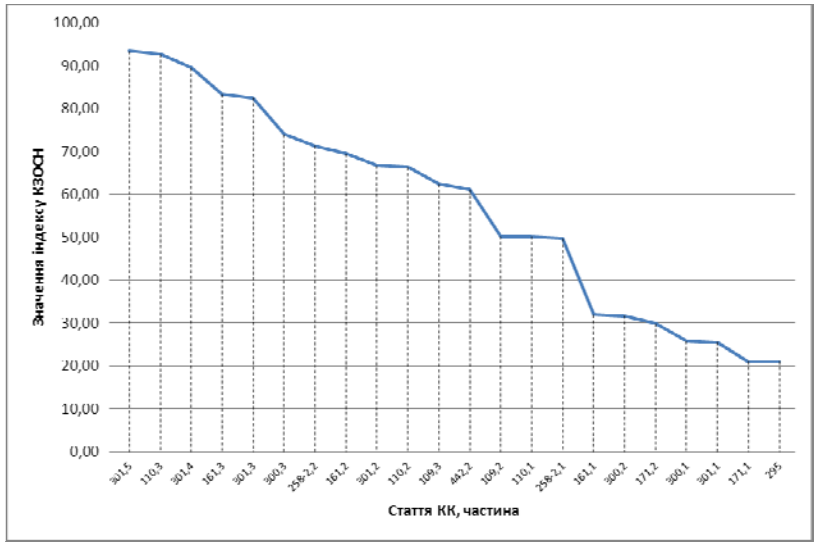
Додаток 8

Графічне представлення результатів аналізу методом контекстної законодавчої оцінки суспільної небезпечності діяння законів про кримінальну відповідальність за обмеження доступу до інформації



Додаток 9

Графічне представлення результатів аналізу методом контекстної законодавчої оцінки суспільної небезпечності діяння законів про кримінальну відповідальність за посягання у сфері формування інформаційного ресурсу



Додаток 10

Проект Закону України "Про внесення змін та доповнень до Кримінального кодексу України та Кодексу України про адміністративні правопорушення з питань відповідальності за посягання у сфері інформаційної безпеки"

I. У Кримінальному кодексі України (Відомості Верховної Ради України (ВВР), 29.06.2001, № 25, ст. 131 з наступними змінами):

1. Назву розділу XVI Кримінального кодексу викласти в такій редакції "Злочини у сфері інформаційної безпеки".

2. Виключити з Кримінального кодексу статті 132, 145, 163, 168, 182, 231, 232, 376-1.

3. Статті 361 – 363-1 викласти в такій редакції:

"**Стаття 361. Незаконні дії з комп'ютерними даними**

1. Незаконне знищення, блокування, порушення цілісності, порядку маршрутування чи спотворення процесу обробки комп'ютерних даних, якщо воно спричинило умисне істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, –

карається штрафом від шестисот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Ті самі діяння, вчинені щодо комп'ютерних даних, які спеціально охороняються програмними, технічними чи організаційними заходами, або з використанням шкідливих програмних чи технічних засобів, або повторно, або за попер-

ньою змовою групою осіб, або особою, яка має правомірний доступ до комп'ютерних даних у зв'язку з займаною посадою або спеціальними повноваженнями, або якщо вони спричинили значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, –

караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

Примітка. 1. У статтях 361 – 361-3, 363-1 повторним визнається злочин, вчинений особою, що раніше вчинила будь-який із злочинів, передбачених цими статтями цього Кодексу.

2. У статтях 361 – 361-3 істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, значна шкода, а також тяжкі наслідки можуть мати як матеріальний, так і нематеріальний характер.

3. У статтях 361 – 361-3 істотним порушенням реалізації прав, свобод або законних інтересів окремих фізичних осіб, якщо воно полягає в заподіянні матеріальних збитків, уважається: а) шкода фізичній особі, заподіяна через обмеження або виключення можливості реалізації нею своїх прав, свобод чи законних інтересів, яка у два або більше рази перевищує неоподатковуваний мінімум доходів громадян; б) сукупна шкода двом або більше фізичним особам, заподіяна протягом одного місяця, через обмеження або виключення можливості реалізації ними своїх прав, свобод чи законних інтересів, яка у п'ять

або більше разів перевищує неоподатковуваний мінімум доходів громадян.

4. У статтях 361 – 361-3 істотним порушенням реалізації державних чи громадських інтересів, якщо воно полягає в заподіянні матеріальних збитків, уважається шкода, заподіяна через обмеження або виключення можливості реалізації державних чи громадських інтересів, яка у двадцять або більше разів перевищує неоподатковуваний мінімум доходів громадян.

5. У статтях 361 – 361-3 істотним порушення діяльності юридичної особи, якщо воно полягає в заподіянні матеріальних збитків, уважається шкода, яка складається з витрат, які зазнає юридична особа у зв'язку з порушенням її діяльності, а також витрат, які вона мусить зробити для відновлення своєї діяльності, яка в п'ятнадцять або більше разів перевищує неоподатковуваний мінімум доходів громадян.

6. Значною шкодою в статтях 361 – 363, якщо вона полягає в заподіянні матеріальних збитків, уважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

7. Тяжкими наслідками в статтях 361 – 363, якщо вони полягають у заподіянні матеріальних збитків, уважаються такі наслідки, які в п'ятсот і більше разів перевищують неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Незаконні дії у сфері телекомунікаційних послуг

1. Незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання, якщо воно спричинило умисне істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, –

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк

до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Ті самі діяння, вчинені з використанням шкідливих технічних засобів або повторно, або за попередньою змовою групою осіб, або якщо вони спричинили значну шкоду, –

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, –

караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

Стаття 361-2. Незаконне надання доступу до інформації

1. Незаконне надання доступу до таємної, службової або конфіденційної інформації, якщо воно спричинило умисне істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, –

карається штрафом до однієї тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі до п'яти років, або позбавленням волі до трьох років.

2. Те саме діяння, вчинене з корисливою метою або повторно, або групою осіб за попередньою змовою, або особою, яка має правомірний доступ до інформації у зв'язку з займаною посадою чи спеціальними повноваженнями, або вчинене з використанням засобів масової інформації чи інших інфор-

маційних технологій, що забезпечують доступ до інформації значної кількості осіб, або якщо воно заподіяло значну шкоду, –

карається позбавленням волі від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією майна або без такої.

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, –

караються позбавленням волі від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого та з конфіскацією майна або без такої.

Примітка: У статтях 361-2 та 362-2 надання доступу до таємної, службової або конфіденційної інформації не може бути визнано незаконним, якщо суд установить, що ця інформація, на час надання доступу до неї, була суспільно необхідною.

Стаття 362. Заподіяння необережної шкоди через незаконні дії з комп'ютерними даними

1. Умисне незаконне знищення, блокування, порушення цілісності, порядку маршрутування чи спотворення процесу обробки комп'ютерних даних, якщо воно з необережності заподіяло значну шкоду, –

карається штрафом до п'ятисот неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до ста двадцяти годин або виправними роботами на строк до одного року з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Ті самі діяння, якщо вони з необережності спричинили тяжкі наслідки, –

караються штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до двохсот сорока годин, виправними роботами на строк до двох років або обмеженням волі до трьох років з конфіскацією про-

грамних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

Стаття 363. Порушення вимог інформаційної безпеки

1. Незастосування або неналежне використання засобів захисту комп'ютерних даних особою, що відповідає за дотримання вимог інформаційної безпеки, якщо воно з необережності заподіяло істотну шкоду, –

карається штрафом до двохсот п'ятдесяти неоподаткованих мінімумів доходів громадян, або громадськими роботами на строк від ста двадцяти до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на той самий строк, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

2. Діяння, передбачене в частині першій, якщо воно з необережності спричинило тяжкі наслідки, –

карається штрафом від шестисот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Стаття 363-1. Незаконне отримання доступу до інформації

1. Отримання незаконного доступу до таємної, службової або конфіденційної інформації, вчинене шляхом подолання технічних, програмних або організаційних засобів захисту інформації, –

карається штрафом до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами до ста вісімдесяти годин або арештом до трьох місяців.

2. Ті самі дії, вчинені шляхом використання технічних або програмних засобів, призначених для незаконного отримання доступу до інформації або з метою надання незаконного доступу до інформації, або повторно, або групою осіб за попередньою змовою, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на строк до трьох років з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи".

4. Доповнити Кодекс статтями 361-3, 362-1, 362-2, 362-3, виклавши їх у такій редакції:

"**Стаття 361-3. Порушення правил здійснення масових розсилок електронних повідомлень**

1. Порушення правил здійснення масової розсилки електронних повідомлень, якщо воно спричинило умисне істотне порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, –

карається штрафом від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Те саме діяння, вчинене повторно, або за попередньою змовою групою осіб, або якщо воно заподіяло значну шкоду, –

карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи, з конфіскацією майна або без такої та зі штрафом від двох тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян.

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, –

караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи, з конфіскацією майна або без такої та зі штрафом від двох тисяч до п'яти тисяч неоподатковуваних мінімумів доходів громадян.

Стаття 362-1. Заподіяння необережної шкоди через незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання

1. Умисне незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання, якщо воно з необережності заподіяло значну шкоду, –

карається штрафом до п'ятисот неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до ста двадцяти годин або виправними роботами на строк до одного року з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Ті самі діяння, якщо вони з необережності спричинили тяжкі наслідки, –

караються штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до двохсот сорока годин, виправними роботами на строк до двох років або обмеженням волі до трьох років з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

Стаття 362-2. Заподіяння необережної шкоди через незаконне надання доступу до інформації

1. Незаконне надання доступу до таємної, службової або конфіденційної інформації, вчинене особою, яка має правомірний доступ до інформації у зв'язку з займаною посадою

або спеціальними повноваженнями, якщо воно з необережності заподіяло значну шкоду, –

карається штрафом до п'ятисот неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до ста двадцяти годин або виправними роботами на строк до одного року.

2. Те саме діяння, якщо воно необережності спричинило тяжкі наслідки, –

карається штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до двохсот сорока годин, виправними роботами на строк до двох років або обмеженням волі до трьох років.

Стаття 362-3. Заподіяння необережної шкоди через порушення правил здійснення масових розсилок електронних повідомлень

1. Порушення правил здійснення масової розсилки електронних повідомлень, якщо воно з необережності заподіяло значну шкоду, –

карається штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до ста двадцяти годин або виправними роботами на строк до одного року з конфіскацією програмних і технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи.

2. Те саме діяння, якщо воно з необережності спричинило тяжкі наслідки, –

карається штрафом до тисячі неоподатковуваних мінімумів доходів громадян, громадськими роботами на строк до двохсот сорока годин, виправними роботами на строк до двох років або обмеженням волі до трьох років з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено злочин, які є власністю винної особи".

5. Абзац перший частини першої ст. 232-1 викласти в такій редакції:

"1. Умисне незаконне надання з використанням інсайдерської інформації рекомендацій стосовно придбання або відчуження цінних паперів чи похідних (деривативів), якщо це призвело до отримання особою, яка вчинила зазначені дії, чи третіми особами необґрунтованого прибутку в значному розмірі, або уникнення учасником фондового ринку чи третіми особами значних збитків, або якщо це заподіяло значну шкоду охоронюваним законом правам, свободам та інтересам окремих громадян або державним чи громадським інтересам, або інтересам юридичних осіб, – ".

II. У Кодексі України про адміністративні правопорушення (Відомості Верховної Ради УРСР, 1984, додаток № 51, ст. 1122):

1. Назву статті 148-1 викласти в такій редакції: "Порушення у сфері телекомунікаційних послуг".

2. Абзац перший частини першої статті 148-1 викласти в такій редакції:

"Незаконне створення перешкод для надання телекомунікаційних послуг або їх незаконне отримання, якщо воно спричинило порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, – тягне за собою …".

3. Назву статті 212-6 викласти в такій редакції: "Порушення у сфері здійснення права власності на комп'ютерні дані".

4. Абзац перший частини першої статті 212-6 КУпАП викласти в такій редакції:

"Незаконне знищення, блокування, порушення цілісності, порядку маршрутування чи спотворення процесу обробки комп'ютерних даних, якщо воно спричинило порушення реалізації прав, свобод або законних інтересів окремих фізичних осіб, або державних чи громадських інтересів, або діяльності юридичної особи, – тягне за собою…".

III. Щороку до 15 листопада проводити засідання профільного комітету Верховної Ради України щодо ефективності кримінально-правової протидії злочинам у сфері інформаційної безпеки. До проведення засідання залучати представників відповідних спеціалізованих підрозділів правоохоронних і судових органів.

ЗМІСТ

Вступ 5

Глава 1. Концептуальні засади дослідження кримінально-правових засобів охорони інформаційної безпеки України 8

1.1. Інформаційна безпека як об'єкт кримінально-правової охорони 8

1.2. Соціальні потреби в кримінально-правовій охороні інформаційної безпеки України 39

Висновки до першої глави 69

Глава 2. Методологічні засади дослідження кримінально-правових засобів охорони інформаційної безпеки України 72

2.1. Методологія дослідження кримінально-правових засобів охорони інформаційної безпеки 72

2.2. Метод контекстної законодавчої оцінки суспільної небезпечності діяння 86

Висновки до другої глави 98

Глава 3. Злочини у сфері використання інформаційних технологій 101

3.1. Аналіз складів злочинів, передбачених ст.ст. 361 – 363[1] КК України 105

3.2. Розмежування злочинів у сфері використання інформаційних технологій та їх відмежування від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки 160

Висновки до третьої глави 183

Глава 4. Удосконалення кримінально-правових засобів охорони інформаційної безпеки у сфері використання інформаційних технологій 188

4.1. Аналіз норм розділу XVI КК України з позицій дотримання принципів визначеності та єдності термінології, а також повноти складу 189

4.2. Прогалини кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій та прояви її надлишковості 200

4.3. Суспільна небезпечність посягань у сфері використання інформаційних технологій як чинник їх криміналізації 216

4.4. Кримінально-правові засоби протидії злочинам у сфері використання інформаційних технологій у контексті дотримання принципу міжнародно-правової необхідності та допустимості криміналізації 259

Висновки до четвертої глави 268

Глава 5. Кримінально-правова охорона суспільних відносин забезпечення доступу до інформаційного ресурсу 272

5.1. Аналіз законодавства про кримінальну відповідальність за незаконні дії з інформацією з обмеженим доступом 274

5.2. Кримінально-правове забезпечення реалізації прав громадян на доступ до інформації 332

Висновки до п'ятої глави 344

Глава 6. Кримінально-правова охорона суспільних відносин у сфері формування інформаційного ресурсу 346

6.1. Кримінально-правове забезпечення формування інформаційного ресурсу

в контексті соціальних тенденцій 348
6.2. Можливі напрями подальшого наукового пошуку з питань кримінально-правового забезпечення формування інформаційного ресурсу 367
Висновки до шостої глави 382

Післямова 384

Список використаних джерел 395

Додатки 442