МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

КАРЧЕВСЬКИЙ МИКОЛА ВІТАЛІЙОВИЧ

УДК 343.3/.7

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

Автореферат дисертації на здобуття наукового ступеня доктора юридичних наук

Київ – 2013

Дисертацією є рукопис

Робота виконана в Національній академії внутрішніх справ,
Міністерство внутрішніх справ України

Науковий консультант доктор юридичних наук, професор
Розовський Борис Григорович,
Східноукраїнський національний університет імені Володимира Даля,
Інститут юриспруденції та міжнародного права,
професор кафедри правознавства

Офіційні опоненти:
доктор юридичних наук, професор,
академік Національної академії правових наук України
Костенко Олександр Миколайович,
Інститут держави і права імені В.М. Корецького НАН України,
завідуючий відділом проблем кримінального права, кримінології та судоустрою

доктор юридичних наук, професор
Музика Анатолій Ананійович,
Чернівецький національний університет імені Юрія Федьковича,
завідувач кафедри кримінального права і криміналістики

доктор юридичних наук, професор
Осадчий Володимир Іванович,
Національний технічний університет України
«Київський політехнічний інститут»,
професор кафедри теорії права та держави факультету соціології і права

Захист відбудеться «24» квітня 2013 р. о 14.00 год. на засіданні спеціалізованої вченої ради Д 26.007.03 у Національній академії внутрішніх справ за адресою: ДП-680, м. Київ, пл. Солом'янська, 1

З дисертацією можна ознайомитись у бібліотеці Національної академії внутрішніх за адресою: ДП-680, м. Київ, пл. Солом'янська, 1

Автореферат розісланий «20» березня 2013 р.

Учений секретар
спеціалізованої вченої ради А.Г. Чубенко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасне суспільство дедалі частіше називають інформаційним. Загальновизнано, 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. Розвиток інформаційних технологій забезпечив модернізацію суспільства та його управління, істотно розширив можливості реалізації конституційних права та свобод. Природно, що такі зміни в суспільстві вимагають певного нормативно-правового відображення і кримінально-правова охорона інформаційної безпеки є однією з найважливіших складових механізму правового регулювання інформаційних відносин. Проте, аналіз наявних у законодавстві про кримінальну відповідальність норм з питань інформаційної безпеки дозволяє дійти висновку, що більшість з них не охоплюється єдиним розумінням проблеми, не має спільної ідеології. Фрагментарність означених законодавчих рішень порушує питання про недостатню ефективність кримінально-правової охорони у відповідній сфері. При цьому, аналіз офіційної статистики МВС свідчить про наявність чіткої тенденції зростання кількісних показників злочинності в сфері використання інформаційних технологій: кількість зареєстрованих злочинів даної категорії у 2011 р. перевищує аналогічний показник 2001 р. у більше ніж 25 разів (!)[*].

Означена проблема не залишилася поза увагою науковців. Окремі питання кримінально-правової охорони інформаційної безпеки були предметами наукових досліджень. Проблеми кримінальної відповідальності за злочини в сфері використання інформаційних технологій досліджували: Д.С. Азаров, П.П. Андрушко, В.М. Бутузов, А.Г. Волєводз, В.Д. Гавловський, В.А. Голубєв, М.В. Гуцалюк, С.В. Дрьомов, В.В. Крилов, Т.В. Міхайліна, А.А. Музика, Ю.Ю. Орлов, С.О. Орлов, М.І. Панов, М.В. Плугатир, М.В. Рудик, Н.А. Савінова. Специфіку кримінально-правової охорони обмеженого доступу до інформації розглядали: П.С. Берзін, О.П. Горпинюк, В.Д. Гулкевич, Ю.І. Дем'яненко, О.В. Красненкова, С.Я. Лихова, О.Е. Радутний, С.О. Харламова. Суміжні проблеми правового регулювання відносин інформаційної безпеки досліджували: А.Б. Венгеров, О.А. Гаврилов, Р.А. Калюжний, Б.А. Кормич, О.М. Костенко, В.А. Ліпкан, В.М. Лопатін, А.І. Марущак, Н.С. Полєвой, Б.С. Українцев, В.С. Цимбалюк, М.Я. Швець. Соціальні наслідки інформатизації та особливості формування інформаційного суспільства вивчали: М. Альєтта, Д. Белл, Е. Гідденс, М.А. Дмитренко, Д.В. Дюжев, М. Кастельс, А.В. Колодюк, А. Ліпіц, К. Мей, В.М. Скалацький, А.О. Сіленко, Ф. Уебстер, Ю. Хабермас, Г. Шиллер та ін.

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

[*] Єдині звіти про злочинність за 2001–2011 роки (форма № 1) : Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж та мереж електрозв'язку // Департамент інформаційно-аналітичного забезпечення Міністерства внутрішніх справ України.

«інформаційна безпека», формулювання критеріїв суспільної небезпечності посягань на неї, меж застосування та змісту кримінально-правових засобів її захисту. 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 Кримінального кодексу України (КК)), напрями вдосконалення відповідних законів про кримінальну відповідальність. 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, небезпека маніпулювання свідомістю тощо.

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. Означене підкреслює актуальність та зумовлює вибір теми дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконано відповідно до Концепції Державної програми профілактики правопорушень на період до 2015 р. (розпорядження Кабінету Міністрів України від 29.09.2010 р. № 191 1-р), та Пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2010 – 2014 років (наказ МВС України від 29.07.2010 р. № 347, додаток 6.11, пункти 94, 95). Тему дисертації затверджено на засіданні Вченої ради Луганського державного університету внутрішніх (протокол від 30.10.2006 р. № 8), і схвалено Академією правових наук України (Перелік тем дисертаційних досліджень з проблем держави і права, 2006 р., № 578).

Мета і задачі дослідження. *Метою* роботи є розроблення концепції кримінально-правової охорони інформаційної безпеки, створення в її межах оптимальної моделі системи норм КК України, що передбачають відповідальність за злочини в цій сфері, і вироблення на цій основі пропозицій щодо вдосконалення чинного законодавства про кримінальну відповідальність.

Для досягнення цієї мети було поставлено такі основні *задачі*:

- сформулювати визначення інформаційної безпеки як об'єкта кримінально-правової охорони, встановити її структуру, співвідношення з суміжними категоріями;

- визначити специфіку методології наукового аналізу кримінально-правової охорони інформаційної безпеки;

- установити зміст соціальної зумовленості кримінальної відповідальності за злочини у сфері інформаційної безпеки[*];

- дослідити систему об'єктивних і суб'єктивних ознак юридичних складів злочинів у сфері використання інформаційних технологій, питання їх кваліфікації;

- вивчити систему засобів кримінально-правової охорони суспільних

[*] З формально-юридичної точки зору поняття «злочини у сфері інформаційної безпеки» може викликати певні заперечення оскільки його визначення на підставі чинної редакції КК України не є очевидним. Проте, використання саме цього терміну продиктовано метою та предметом дослідження.

відносин у сфері обмеженого доступу до інформації;

- проаналізувати кримінально-правову охорону суспільних відносин у сфері отримання доступу до інформації;

- встановити особливості кримінально-правової охорони інформаційної безпеки у сфері формування інформаційного ресурсу;

- провести аналіз чинного законодавства про кримінальну відповідальність за злочини у сфері інформаційної безпеки з позицій дотримання принципів криміналізації;

- розробити пропозиції щодо вдосконалення чинного законодавства про кримінальну відповідальність за злочини у сфері інформаційної безпеки;

- виявити можливі напрями подальшого наукового пошуку у сфері кримінально-правової охорони інформаційної безпеки.

Об'єкт дослідження – інформаційна безпека України.

Предмет дослідження – кримінально-правова охорона інформаційної безпеки України.

Методи дослідження обрані з урахуванням поставленої в роботі мети та задач дослідження, його об'єкта й предмета. Наукові методи *аналізу* та *синтезу*, а також принципи класифікації використано для дослідження змісту поняття «інформаційна безпека», а також при розгляді теорій інформаційного суспільства (підрозділи 1.1, 1.2). *Діалектичний* метод забезпечив комплексний розгляд позитивних і негативних тенденцій інформатизації суспільства (підрозділи 1.1, 1.2). Методи *алгоритмізації* та *формалізації* використано для організації та систематизації роботи щодо отримання контекстних законодавчих оцінок суспільної небезпечності діяння (підрозділ 2.2). За допомогою *системно-структурного аналізу* вдалося показати внутрішню побудову системи кримінально-правових норм, які передбачають відповідальність за злочини проти інформаційної безпеки, обсяг і зміст відповідних понять, місце кримінальної відповідальності за розглядані злочини в системі норм та інститутів Особливої частини кримінального права (підрозділи 3.1, 3.2, 4.3, 5.1, 5.2, 6.1). *Компаративістський* метод застосовувався для порівняння кримінального законодавства України, що передбачає відповідальність за злочини проти інформаційної безпеки, із відповідними нормами законодавства інших держав (підрозділи 4.2, 4.3). *Соціологічні* та *статистичні* методи використовувалися при вивченні практики застосування норм КК, які передбачають відповідальність за злочинні посягання на інформаційну безпеку, а також для дослідження позицій працівників ОВС щодо вдосконалення кримінально-правового забезпечення інформаційної безпеки (підрозділи 1.1, 1.2, 4.1, 4.2, 4.3). Метод *моделювання* використаний для оцінки ефективності кримінально-правової охорони суспільних відносин у сфері забезпечення доступу до інформації та формування інформаційного ресурсу (підрозділи 5.1, 6.1). Метод *контекстної законодавчої оцінки суспільної небезпечності діяння* дозволив проаналізувати систему норм про кримінальну відповідальність за посягання у сфері інформаційної безпеки з позицій відповідності їх санкцій чинникам суспільної небезпечності передбачених ними посягань (підрозділи 5.1, 5.2, 6.1). Дотримання вимог законодавчої техніки

та принципів конструювання кримінально-правових норм здійснювалося шляхом застосування *догматичного* методу (висновки).

Науково-теоретичне підґрунтя дисертації складають праці з кримінального права вітчизняних і зарубіжних науковців, присвячені як загальним проблемам кримінального права, так і питанням відповідальності за злочини у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж, мереж електрозв'язку та інші злочини у сфері інформаційної безпеки, а також праці з загальної теорії держави й права, історії держави й права України та зарубіжних країн, інформаційного, адміністративного, господарського та цивільного права.

Емпіричною базою дослідження є: статистичні дані МВС України, Верховного Суду України, Державної судової адміністрації України; дані, отримані при вивченні 270 кримінальних справ за ст.ст. 176, 361 – 363-1 КК, розслідуваних органами досудового слідства та розглянутих судами України у період 2005 – 2011 рр.; результати анкетування 320 працівників підрозділів МВС України, які здійснюють протидію кіберзлочинності.

Наукова новизна одержаних результатів. Дисертація є першим в Україні системним, монографічним дослідженням кримінально-правової охорони інформаційної безпеки України. На основі результатів дослідження сформульовано ряд нових концептуальних у теоретичному плані та важливих для юридичної практики положень і висновків, які виносяться на захист, а саме:

вперше:

- доведено, що інформаційна безпека як самостійний об'єкт кримінально-правової охорони являє собою систему суспільних відносини щодо забезпечення реалізації інформаційних потреб громадян, суспільства, держави;
- обґрунтовано, що структуру інформаційної безпеки складають три групи суспільних відносин: 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;
- визначено і систематизовано соціальні тенденції, що зумовлюють необхідність кримінально-правової охорони інформаційної безпеки;
- встановлено, що загальною рисою суспільних відносини інформаційної безпеки, які потребують кримінально-правової охорони, є те, що їх соціальне значення є похідним від значущості тих суспільних відносин, у межах яких виникає інформаційна потреба;
- аргументовано доцільність включення інформаційної безпеки до системи родових об'єктів злочинів, передбачених КК; на цій підставі пропонується заміна назви розділу XVI Особливої частини КК такою – «Злочини у сфері інформаційної безпеки» та об'єднання в ньому норм про відповідальність за злочини у сфері формування інформаційного ресурсу, забезпечення доступу до інформації та використання інформаційних технологій;
- для аналізу кримінально-правових засобів охорони інформаційної безпеки використано метод контекстної законодавчої оцінки суспільної небезпечності

діяння, який дозволив ефективно розв'язувати завдання представлення, установлення та порівняння законодавчої оцінки суспільної небезпечності злочинних посягань на інформаційну безпеку;

- встановлено, що при криміналізації посягань 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 ті, які такими не є; останнє різко негативно відбивається на ефективності кримінально-правової охорони інформаційної безпеки;

- обґрунтовано, що при криміналізації діянь, передбачених ст.ст. 361 – 363-1 КК, порушено принцип визначеності та єдності термінології, оскільки означені норми: характеризуються термінологічними розбіжностями з відповідними положеннями законодавства про адміністративну відповідальність; містять терміни, які неоднаково визначаються як на рівні законодавства, так і на рівні наукового тлумачення;

- доведено, що ефективність кримінально-правової протидії масовому розповсюдженню повідомлень електрозв'язку (ст. 363-1 КК) є недостатньою, через те, що кримінальна відповідальність за означені дії залежить від настання наслідків, які є нетиповими для подібних посягань. Переважна більшість випадків розповсюдження спаму не підпадає під ознаки злочину, передбаченого відповідною нормою;

- встановлено порушення принципу повноти складу злочину, яке полягає у формулюванні занадто громіздких законодавчих визначень, що ускладнюють з'ясування змісту ознак конкретних складів злочинів (ст. 361 КК передбачає відповідальність за два абсолютно самостійні склади злочинів), 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);

- аргументовано надлишковість зобов'язань, узятих на себе Україною при ратифікації Конвенції про кіберзлочинність, і сформульовано пропозиції щодо внесення нових застережень до Закону України «Про ратифікацію Конвенції про кіберзлочинність»;

- з позицій de lege ferenda запропоновано заходи щодо вдосконалення кримінально-правового захисту інформаційної безпеки у сфері використання інформаційних технологій;

- обґрунтовано, що кримінально-правова охорона інформаційної безпеки у сфері забезпечення обмеженого доступу до інформації характеризується фрагментарністю та не повною мірою відповідає соціальним потребам

кримінально-правової протидії;

- з використанням методу контекстної законодавчої оцінки суспільної небезпечності встановлено, що система кримінально-правових засобів забезпечення обмеженого доступу до інформації характеризується непослідовністю врахування чинників суспільної небезпечності при визначенні інтенсивності санкцій за окремі види незаконного надання та отримання доступу до інформації;

- сформульовано пропозиції щодо оптимізації системи норм про відповідальність за злочини у сфері обмеженого доступу до інформації, зокрема: запропоновано доповнити КК загальними нормами про відповідальність за незаконне надання та отримання доступу до інформації, а ст.ст. 132, 145, 163, 168, 182, 231, 232, 232-1 (у частині відповідальності за незаконне надання доступу до інсайдерської інформації) – виключити;

- обґрунтовано, що розширення переліку кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення суспільно шкідливої інформації є недоцільним через прогнозовану неефективність і декларативність таких норм, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації;

удосконалено:

- дефініцію права власності на комп'ютерну інформацію, як безпосереднього об'єкта злочинів в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж;

- визначення перспективних напрямів подальших наукових досліджень кримінально-правової охорони інформаційної безпеки, до яких пропонується відносити: а) підвищення ефективності кримінально-правової протидії посяганням на інтелектуальну власність шляхом удосконалення порядку обчислення матеріальної шкоди, а також диверсифікації правових засобів протидії означеним посяганням; б) розроблення та обґрунтування методу аналізу шкоди, заподіяної зловживанням або перевищенням влади чи службових повноважень у сфері інформатизації; в) можливості використання законів про кримінальну відповідальність за перевищення, зловживання владою чи службовими повноваженнями та недбалість для охорони прав громадян на доступ до інформації та протидії суспільно небезпечним видам незаконного збирання або зберігання персональних даних;

дістали подальшого розвитку положення про:

- зміст ознак складів злочинів, передбачених ст. ст. 361 – 363-1 КК;

- розмежування злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку, а також щодо їх відмежування від суміжних посягань;

- надлишковість кримінально-правової заборони, установленої ст. 361-2 КК та аргументація скасування цієї норми;

- недоцільність доповнення КК спеціальною нормою про відповідальність службової особи за ненадання доступу до інформації.

Практичне значення одержаних результатів. Теоретичні та прикладні висновки та рекомендації дисертаційного дослідження використані та мають перспективу використання у наступних галузях:

– *науково-дослідній діяльності* – теоретичною основою вирішення проблем кримінально-правової охорони інформаційної безпеки України (акт впровадження Апарату Ради національної безпеки і оборони України від 15.12.2011 р. № 303);

– *законотворчій діяльності* – при подальшому вдосконаленні законодавства про кримінальну відповідальність (листи Комітету з питань законодавчого забезпечення правоохоронної діяльності Верховної Ради України від 16.01.2009 р. № 04-19/15-56, від 11.11.2011 р. № 04-19/14-2338, від 06.11.2012 р. № 04-19/14-3270);

– *правозастосовній діяльності* – розроблені на основі результатів дослідження електронна довідкова система «Злочини у сфері використання інформаційних технологій» і база даних судових рішень «Кіберзлочинність. Судова практика» впроваджено в систему службової підготовки Управління боротьби з кіберзлочинністю МВС України (акт впровадження від 01.11.2012 р.);

– *навчальному процесі* – на основі дослідження розроблений та викладається курс для слухачів магістратури Луганського державного університету внутрішніх справ імені Е.О. Дідоренка «Злочини у сфері використання комп'ютерної техніки» (акти впровадження від 21.10.2010 р., 18.11.2010 р., 16.12.2010 р.)

Особистий внесок здобувача. Викладені в дисертації положення, що складають її наукову новизну, розроблено автором особисто. Наукові положення і результати кандидатської дисертації здобувача повторно не виносяться на захист докторської дисертації.

Апробація результатів дисертації. Результати дослідження оприлюднено на 13 науково-практичних заходах, у т.ч.: на спільному засіданні Вченої ради Інституту вивчення проблем злочинності НАПрН України та координаційного бюро з проблем кримінального права відділення кримінально-правових наук НАПрН України (м. Харків, 2012 р.); на міжнародному симпозіумі «Кримінальний кодекс України 2001 року: проблеми застосування і перспективи удосконалення» (м. Львів, 2012 р.); на міжнародних науково-практичних конференціях «Злочини у сфері використання комп'ютерної техніки: проблеми кваліфікації, розслідування та попередження» (м. Луганськ, 2004 р.); «Обеспечение законности и правопорядка в странах СНГ» (м. Вороніж, 2009 р.); «Теоретичні та прикладні проблеми кримінального права України» (м. Луганськ, 2011 р., 2012 р.); «10 років чинності Кримінального кодексу України: проблеми застосування, удосконалення та подальшої гармонізації із законодавством європейських країн» (м. Харків, 2011 р.); «Основні напрями розвитку кримінального права та шляхи вдосконалення законодавства України про кримінальну відповідальність» (м. Харків, 2012 р.); міжнародному круглому столі «Інформаційне забезпечення розслідування злочинів у сучасних умовах»

(м. Луганськ, 2010 р.); всеукраїнських науково-практичних конференціях «Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку» (м. Донецьк, 2009 р.); «Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи їх вирішення» (м. Донецьк, 2010 р., 2011 р.); міжвузівській науково-практичній конференції «Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення» (м. Донецьк, 2007 р.).

Публікації. Результати дисертаційного дослідження викладено в монографії, 22 статтях у наукових фахових виданнях, трьох підручниках, двох навчальних посібниках та 19 інших публікаціях.

Структура дисертації. Робота складається зі вступу, шести розділів, що включають 15 підрозділів, висновків, списку використаних джерел (514 найменувань) та 11 додатків. Повний обсяг дисертації становить 536 сторінок, з яких загальний обсяг тексту – 390 сторінки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність теми дисертації, визначаються мета, задачі, об'єкт, предмет і методи дослідження, формулюються положення, що відображають наукову новизну роботи й виносяться на захист, розкривається практичне значення одержаних результатів.

Розділ 1 «Концептуальні засади дослідження кримінально-правової охорони інформаційної безпеки України» складається з двох підрозділів і присвячений аналізу наукових праць з проблематики дослідження, виокремленню предмета дослідження, систематизації соціальних потреб у кримінально-правовій охороні інформаційної безпеки.

У *підрозділі 1.1. «Інформаційна безпека як об'єкт кримінально-правової охорони»* обґрунтовується визначення інформаційної безпеки як системи суспільних відносин, яка забезпечує можливість реалізації інформаційної потреби громадян, суспільства, держави. Інформаційну безпеку суб'єкту слід вважати забезпеченою тоді, коли він має можливість отримувати повну, достовірну та достатню для прийняття ефективних рішень інформацію. Такий стан досягається соціальною активністю в трьох взаємопов'язаних групах суспільних відносин, що являють собою структурні елементи інформаційної безпеки: суспільні відносини у сфері формування інформаційного ресурсу, у сфері забезпечення доступу до інформаційного ресурсу й у сфері використання інформаційних технологій. У межах першої групи забезпечується формування інформаційного ресурсу, котрий відповідає потребам суб'єктів, у межах другої – забезпечується можливість суб'єктів отримувати безперешкодний доступ до необхідних інформаційних ресурсів, а в межах третьої – виконується завдання забезпечення функціонування ефективних засобів інформаційної діяльності. Обґрунтовується, що підставами для розгляду інформаційної безпеки як самостійного об'єкта кримінально-правової охорони слід уважати: 1) актуалізацію проблематики

кримінальної відповідальності за злочини в сфері формування інформаційного ресурсу, забезпечення доступу до інформації та використання інформаційних технологій, викликану стрімким розвитком інформатизації та комп'ютеризації; 2) системні властивості визначеної сукупності суспільних відносин (структурні елементи інформаційної безпеки підпорядковані єдиній спільній соціальній меті – реалізації інформаційної потреби громадян, держави, суспільства; функціонування та ефективність кожного з елементів системи взаємозумовлені іншими); 3) зміст шкоди, що заподіюється під час посягань на інформаційну безпеку, який полягає у позбавленні, або обмеженні можливості реалізації інформаційної потреби.

У *підрозділі 1.2. «Соціальна зумовленість кримінально-правової охорони інформаційної безпеки України»* чинники, що свідчать про необхідність кримінально-правової охорони інформаційної безпеки, класифіковано за видами суспільних відносин інформаційної безпеки. На підставі результатів сучасних досліджень соціальних наслідків інформатизації, представлених у роботах Д. Белла, Е. Гідденса, М. Кастельса, Ф. Уебстера, Ю. Хабермаса, Г. Шиллера та ін., доводиться, що 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 гарантування встановлених обмежень доступу до певних видів інформації. Формування інформаційного ресурсу потребує кримінально-правових засобів охорони, оскільки існує, зумовлена головним чином комерціалізацією інформаційного простору, потенційна можливість істотних порушень соціальної стабільності шляхом зловживань у інформаційній сфері.

При цьому 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 значення останніх відносин визначає суспільну небезпечність відповідних посягань та інтенсивність засобів кримінально-правової охорони інформаційної безпеки. Даний висновок обґрунтовано як теоретично так і в ході емпіричного дослідження. За результатами проведеного анкетування працівників правоохоронних органів переважна більшість респондентів (84,38 %) підтримала означений підхід до визначення специфіки суспільної небезпечності посягань на інформаційну безпеку.

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 системної кримінально-правової

охорони відносин інформаційної безпеки.

Розділ 2 «Методологічні засади дослідження кримінально-правової охорони інформаційної безпеки України» складається з трьох підрозділів і присвячений обґрунтуванню вибору методів, їх адаптації до предмета і задач дослідження.

У *підрозділі 2.1. «Специфіка методології дослідження кримінально-правової охорони інформаційної безпеки»* визначаються особливості методології зумовлені об'єктом дослідження. Так, зазначається, що оскільки включення кримінально-правових засобів до механізму правового регулювання інформаційної безпеки відбувається в основному шляхом криміналізації суспільно небезпечних посягань на неї, як складову методології дослідження необхідно розглядати запропоновані у науці кримінального права положення щодо обґрунтованості криміналізації, інтерпретовані в контексті кримінально-правової охорони інформаційної безпеки. Означені питання більш докладно розглядаються у підрозділі 2.2.

Для визначення особливостей методології дослідження встановлено систему злочинів у сфері інформаційної безпеки. Кореспондуючи з структурою інформаційної безпеки, означена система включає три групи посягань:

1) злочини у сфері використання інформаційних технологій (ч.ч. 11, 12 ст. 158, ст.ст. 361 – 363-1, 376-1 КК);

2) злочини у сфері забезпечення доступу до інформації (ст.ст. 111, 114, 132, 145, ч. ч. 11, 12 ст. 158, ст. ст. 159, 163, 168, 182, ч. 2 ст. 209-1, 231, 232, 328, 330, 361-2, 361, 362, 376-1, 381, 387, 422 КК – злочини у сфері обмеженого доступу до інформації; ст. 136, ч. 1 ст. 209-1, ст. ст. 232-2, 238, ч. 3 ст. 243, ст. 285, ст. 298-1, 385 КК – злочини у сфері отримання доступу до інформації);

3) злочини у сфері формування інформаційного ресурсу (ч.ч. 2, 3 ст. 109, ст.ст. 110, 161, 171, 258-2, 295, 300, 301; ч. 2 ст. 442 КК).

Аналіз структури та змісту даної системи дозволяє зробити наступні висновки стосовно методології дослідження. По-перше, розосередженість засобів кримінально-правової охорони інформаційної безпеки по більшій частині інститутів Особливої частини дає підстави для формулювання гіпотези про те, що завдання охорони інформаційної безпеки в рамках існуючого КК реалізовано неповно та недостатньо. Це зумовлює специфіку використання методу системно-структурного яка полягає у тому, що наявна у чинному законодавстві система норм про відповідальність за злочини в сфері інформаційної безпеки має розглядатися з позицій її оптимізації, в ході дослідження має розв'язуватися питання доцільності, обґрунтованості та меж заміни наявної у чинному законодавстві розгалуженої системи спеціальних кримінально-правових заборон у сфері інформаційної безпеки такими нормами, які б забезпечували охорону більш широких сегментів відносин інформаційної безпеки.

По-друге, обґрунтовано що для розв'язання проблеми оптимізації системи кримінально-правових засобів забезпечення інформаційної безпеки доцільним є включення інформаційної безпеки до системи родових об'єктів. Реалізація наведеної пропозиції передбачає заміну назви розділу XVI Особливої частини КК України наступною – «Злочини у сфері інформаційної безпеки». При цьому

специфіка інформаційної безпеки, яка полягає у тому, що сукупність посягань на неї неможливо розглядати як такі, що відносяться виключно до єдиного родового об'єкту, зумовлює не тільки необхідність встановлення тих посягань, які доцільно розглядати в контексті запропонованого родового об'єкту, але також доцільність аналізу можливостей забезпечення кримінально-правової охорони відносин інформаційної безпеки за допомогою норм, що передбачають посягання на суміжні родові об'єкти.

У *підрозділі 2.2. «Методологія дослідження криміналізації суспільно небезпечних посягань на інформаційну безпеку»* з метою формулювання методологічних засад аналізу засобів кримінально-правової охорони інформаційної безпеки (норм законодавства про кримінальну відповідальність за злочини в сфері інформаційної безпеки) з позицій досягнень науки кримінального права в питанні криміналізації (декриміналізації) та їх критеріїв, положення щодо обґрунтованості криміналізації, запропоновані у дослідженнях В.К. Грищука, В.О. Навроцького, Н.О. Лопашенко, В.М. Кудрявцева, Г.А. Злобіна та ін., інтерпретуються в контексті дослідження проблем кримінально-правової охорони інформаційної безпеки. Так, підстави криміналізації посягань на інформаційну безпеку пропонується поділяти на дві групи. До першої групи слід відносити процеси, які мають істотне значення для позитивних трансформацій суспільства в бік розвитку та стабільності (зростання суспільної значимості інформаційних ресурсів та доступу них; розширення сфери застосування інформаційних технологій як засобів інтенсифікації людської діяльності). До другої – процеси, що характеризуються великим потенціалом суспільної небезпечності (розвиток форм та видів протиправного використання інформаційних технологій; надмірна капіталізація інформаційного простору; маніпуляції суспільною свідомістю).

Послідовне врахування вказаних соціальних тенденцій в процесі визнання певних суспільно небезпечних діянь злочинами забезпечується шляхом дотримання принципів криміналізації. Зокрема, зазначається, що дотримання принципу співрозмірності позитивних та негативних наслідків криміналізації у сфері інформаційної безпеки передбачає врахування наступних положень: незбалансований підхід до кримінально-правового забезпечення доступу до інформації може невиправдано обмежувати можливості реалізації інформаційної потреби через надмірну правову зарегульованість або, навпаки, надлишкові кримінально-правові гарантії такого доступу можуть призвести 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.

Підрозділ 2.3. «Метод контекстної законодавчої оцінки суспільної небезпечності діяння» присвячений викладенню розробленого автором методу, який використовується як методологічна основа порівняння кримінально-правових

санкцій та дозволяє ефективно розв'язувати завдання представлення, установлення та порівняння законодавчої оцінки суспільної небезпечності злочинних посягань на інформаційну безпеку. Необхідність розроблення та використання даного методу зумовлена розосередженістю системи кримінально-правових засобів інформаційної безпеки, а також недостатністю та обмеженістю наявного у науці кримінального права інструментарію порівняння суворості санкцій. Актуальність розроблення методу обумовлюється і тим, що багато дослідників, зокрема Д.С. Азаров, В.А. Мисливий, М.І. Мельник, Ю.А. Пономаренко, Н.О. Гуторова, В.І. Осадчий, зазначають, що законодавчим оцінкам суспільної небезпечності окремих діянь властива суб'єктивність і відсутність єдиного виваженого підходу.

Установлення об'єктивної законодавчої оцінки суспільної небезпечності передбачає дослідження певного закону в контексті вже існуючих заборон. На сьогодні найбільш поширеним індикатором суворості санкцій є її медіана. Однак цей показник характеризується низкою недоліків, які значно обмежують можливості його використання. Сутність запропонованого 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 небезпеки необхідно, ураховуючи положення науки кримінального права, провести порівняння суворості генеральної сукупності санкцій і систематизувати кримінально-правові заборони за цією ознакою. Місце, отримане певним посяганням у цій системі, і буде являти собою контекстну законодавчу оцінку суспільної небезпечності посягання.

Розділ 3 «Злочини у сфері використання інформаційних технологій» містить два підрозділи і присвячений аналізу складів злочинів, передбачених ст.ст. 361 – 363-1 КК, та їх відмежуванню від суміжних складів.

У *підрозділі 3.1. «Кримінально-правова характеристика складів злочинів, передбачених ст.ст. 361 – 363-1 КК України»* з урахуванням положень, висловлених у роботах М.І. Панова, А.А. Музики, А.П. Андрушка, Д.С. Азарова, Н.А. Савінової, С.В. Дрьомова, С.О. Орлова, Т.В. Міхайліної, М.В. Рудика та ін. формулюється зміст ознак складів злочинів, передбачених розділом XVI Особливої частини КК. Основні положення підрозділу полягають у такому. Установлено, що родовим об'єктом досліджуваних злочинів 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. Альтернативними безпосередніми об'єктами несанкціонованого втручання в роботу електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку (ст. 361 КК), а також незаконних дій з шкідливими програмними чи технічними засобами (ст. 361-1 КК) 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 являє собою: 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.

До предметів несанкціонованого втручання віднесено: комп'ютерну інформацію – 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; інформацію, що передається мережами електрозв'язку – відомості, подані у формі, яка дозволяє їх приймати або передавати засобами електрозв'язку.

Доведено, що об'єктивна сторону несанкціонованого втручання (ст. 361 КК) 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 до порушення встановленого порядку її маршрутизації; 2) несанкціоноване втручання в роботу мереж електрозв'язку, яке призвело до витоку, втрати, підробки, блокування інформації, що передається в мережі, спотворення процесу обробки такої інформації або до порушення встановленого порядку її маршрутизації.

Обґрунтовано, що об'єктивна сторона злочину, передбаченого ст. 361-1 КК, може виражатися в таких формах: 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 встановлення в ЕОМ, системи або комп'ютерні мережі; збут шкідливих програмних або технічних засобів – оплатне або безоплатне відчуження таких засобів.

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

обчислювальних машин (комп'ютерів), 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. 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. Суб'єктивна сторона цього злочину характеризується тим, що діяння може бути вчинене як умисно, так і з необережності, але до наслідків можливе тільки необережне ставлення.

Об'єкт злочину, передбаченого ст. 363-1 КК, визначено як суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки та мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію. Предмет – повідомлення електрозв'язку. 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 і наслідками.

У *підрозділі 3.2. «Відмежування злочинів у сфері використання інформаційних технологій від інших злочинних посягань, пов'язаних із використанням комп'ютерної техніки»* зазначається, 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. У свою чергу методологія процесу відмежування, як правило, полягає в застосуванні правил розв'язання конкуренції кримінально-правових норм, зокрема конкуренції цілого та частини, загальної та спеціальної норм. Так, особливістю кримінально-правової кваліфікації злочинів проти власності, вчинюваних із використанням комп'ютерної техніки, визнається необхідність розв'язання питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Відповідаючи 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 певну інформацію було незаконно знищено, блоковано, модифіковано. А в тих випадках, коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна.

---

[*] Терміни «комп'ютерні злочини», «злочини у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку», а також «злочини у сфері використання інформаційних технологій» використовуються як тотожні. Доцільність включення до наукового дискурсу останнього терміну обґрунтовується у підрозділі 4.3.

Розділ 4 «Удосконалення кримінально-правових засобів охорони інформаційної безпеки у сфері використання інформаційних технологій» містить чотири підрозділи.

У *підрозділі 4.1. «Юридичний аналіз норм розділу XVI Особливої частини КК України з позицій дотримання принципів визначеності та єдності термінології, а також повноти складу»* обґрунтовується, що норми вказаного розділу містять терміни, які неоднаково визначаються і на рівні законодавства, і на рівні наукового тлумачення, що звужує можливості його використання для охорони відповідних суспільних відносин. Так, КК використовує такі поняття, як «електронно-обчислювальна машина», «автоматизована система» та «комп'ютерна мережа», однак їх чіткі законодавчі визначення відсутні. 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.

Наступною термінологічною вадою означених норм є використання категорії «інформація». Таке законодавче рішення призводить до того, що віднесення комп'ютерних програм до предметів злочинів, передбачених ст.ст. 361 та 362 КК, стає проблематичним, оскільки входить в очевидну суперечність із визначенням інформації як певних відомостей про навколишній світ і процеси, що в ньому відбуваються. У зв'язку з цим пропонується використовувати термін «комп'ютерні дані», який визначається Конвенцією про кіберзлочинність та охоплює як інформацію, так і програми (дану пропозицію підтримали 98,13 % опитаних працівників правоохоронних органів).

Порушення принципу повноти складу полягає у формулюванні занадто громіздких законодавчих визначень, які ускладнюють установлення змісту ознак конкретних складів злочинів, а також у 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 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. Тому видається доцільним передбачити кримінальну відповідальність за несанкціоноване втручання в роботу мереж електрозв'язку в окремій статті КК (дану пропозицію підтримали 89,69 % опитаних працівників правоохоронних органів). 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 ускладнення практики застосування відповідної норми і, отже, не сприяє ефективності

кримінально-правової охорони. Недостатньо конкретним є формулювання ознак спеціального суб'єкта злочину, передбаченого ст. 362 КК. Воно 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. Обґрунтовується доцільність такого визначення: особа, яка має правомірний доступ до комп'ютерних даних у зв'язку з займаною посадою або спеціальними повноваженнями.

У *підрозділі 4.2. «Прогалини кримінально-правової охорони суспільних відносин у сфері використання інформаційних технологій та прояви її надлишковості»* зазначається, що певні прогалини в кримінально-правовій охороні суспільних відносин зумовлені вадами конструкції об'єктивної сторони складу злочину, передбаченого ст. 361 КК. Відповідно до чинного законодавства настання вказаних у цій статті 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. Очевидно, що відсутність несанкціонованого втручання (діяння) не означає, що настання наслідків втрачає суспільну небезпечність.

Окремою проблемою протидії суспільно небезпечним посяганням у сфері використання комп'ютерної техніки в контексті дотримання принципу відсутності прогалин є питання відповідальності за розповсюдження спаму (ст. 363-1 КК). Переважну більшість випадків розповсюдження спаму не можна кваліфікувати за цією нормою, оскільки воно, як правило, не призводить до наслідків, зазначених у ст. 363-1 КК. При цьому 81,56 % опитаних працівників правоохоронних органів погодилися з тим, що означена вада ст. 363-1 КК є головною причиною недостатньої ефективності протидії поширенню спаму в Україні.

Наводяться нові аргументи на користь того, що ст. 361-2 КК являє собою надлишкову кримінально-правову заборону та підлягає виключенню. Дослідження означеної норми в контексті інших кримінально-правових гарантій обмеженого доступу до інформації, наявних у КК, дозволяє зробити такий висновок: 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 такий аргумент є спірним та очевидно недостатнім. Форма інформації ні в якому разі не може обґрунтовувати підвищену суспільну небезпечність її розповсюдження або збуту.

У *підрозділі 4.3. «Суспільна небезпечність посягань у сфері використання інформаційних технологій як чинник їх криміналізації»* обґрунтовується, що під час криміналізації посягань, передбачених розділом XVI Особливої частини КК, були допущені порушення принципу суспільної небезпечності. До них слід відносити недоліки диференціації відповідальності залежно від заподіяної шкоди.

Однаковими в плані кваліфікації будуть, наприклад, несанкціоновані втручання, що спричинили матеріальні збитки в розмірах 120 та 520 неоподатковуваних мінімумів доходів громадян, або несанкціоноване втручання, що спричинило порушення роботи світлофорів у певному мікрорайоні, та несанкціоноване втручання, що спричинило порушення роботи системи радіаційної безпеки АЕС. Недоліком, який не дозволяє повною мірою враховувати суспільну небезпечність певних посягань, є і відсутність у нормах розділу спеціальної вказівки на можливість так званої змішаної повторності. 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. Суспільна небезпечність даних злочинів 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. Однак для настання кримінальної відповідальності за більшість злочинів, передбачених у розділі XVI Особливої частини КК, установлення таких характеристик суспільно небезпечних наслідків не є обов'язковим. Судячи з прийнятого законодавцем рішення, витік, втрата, підробка, блокування інформації, порушення встановленого порядку її маршрутизації або спотворення процесу її обробки (ст.ст. 361, 362 КК) визнаються суспільно небезпечними самі по собі.

Неповна відповідність чинного законодавства означеній специфіці суспільної небезпечності комп'ютерних злочинів зумовлює появу негативних тенденцій у практиці застосування норм про кримінальну відповідальність. Більше половини судових рішень досліджуваної категорії (56,29 %) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є достатньо спірним. Наприклад, близько чверті випадків застосування ст. 361 КК (24,24 %) являють собою кримінально-правову оцінку несанкціонованого підключення до мереж кабельного телебачення. Відсутність чітких критеріїв суспільної небезпечності у нормах про кримінальну відповідальність за посягання у сфері інформаційних технологій зумовлює появу судових рішень, які є цілком правосудними, але достатньо спірними з позицій доцільності та дотримання принципу ultima ratio. Інтерпретація отриманих фактичних даних в контексті результатів наукових досліджень з питань ефективності кримінально-правової охорони, що містяться в роботах А.Е. Жалінського, В.К. Грищука, А.А. Музики, О.М. Костенка, дозволяє наступним чином сформулювати сутність допущеного порушення принципу суспільної небезпечності криміналізації: 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 ті, які такими не є. Таке становище

різко негативно відбивається на ефективності кримінально-правової охорони інформаційної безпеки у сфері використання інформаційних технологій. Додаткових аргументів для таких висновків додає і те, що у 70,66 % досліджених судових рішень покарання призначалося з випробуванням.

З урахуванням обґрунтованої раніше необхідності термінологічних уточнень та пропозицій 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 щодо надання та отримання телекомунікаційних послуг.

При цьому необхідним для нормативного відображення специфіки суспільної небезпечності досліджуваних злочинів є передбачення у відповідних складах системи додаткових обов'язкових об'єктів, які б відображали дійсну суспільну небезпечність посягань у сфері використання інформаційних технологій. Видається, що 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 й мають складати систему додаткових обов'язкових об'єктів досліджуваних злочинів.

Послідовною, такою що відповідає означеній специфіці безпосереднього об'єкта, а отже, і 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 у вигляді різних форм 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 уважати злочином.

Для формулювання законодавчих критеріїв суспільної небезпечності посягань у сфері використання інформаційних технологій доречним видається також використання специфічних суб'єктивних ознак. 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, пропонується: 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.

У контексті встановленої специфіки суспільної небезпечності посягань у сфері використання інформаційних технологій також обґрунтовано доцільність: 1) криміналізації незаконних дій із шкідливими програмними чи технічними засобами не як самостійного посягання, а як кваліфікуючої ознаки посягань на відносини власності на комп'ютерні дані; 2) скасування спеціальних заборон у сфері використання інформаційних технологій (ч.ч. 11, 12 ст. 158 та ст. 376-1 КК).

У *підрозділі 4.4. «Кримінально-правові засоби протидії злочинам у сфері використання інформаційних технологій у контексті дотримання принципу міжнародно-правової необхідності та допустимості криміналізації»* розглядається питання відповідності чинного законодавства про кримінальну відповідальність за злочини у сфері використання інформаційних технологій ратифікованій Україною Конвенції про кіберзлочинність. Констатується, що в цілому національне законодавство відповідає ратифікованим міжнародним нормативно-правовим актам, а виняток становить лише некриміналізований чинним законодавством незаконний доступ. Разом із цим рішення, прийняте законодавцем щодо ратифікації Конвенції, зобов'язує на рівні національного законодавства визнавати злочинами діяння, які не характеризуються суспільною небезпечністю, що повертає до проблематики, розглянутої вище. Тому 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 відповідних змін.

Розділ 5 «Кримінально-правова охорона суспільних відносин у сфері забезпечення доступу до інформації» містить два підрозділи. Властива правовому регулюванню відносин у сфері забезпечення доступу до інформації дуалістичність зумовлює існування двох груп кримінально-правових засобів інформаційної безпеки в її відповідному сегменті. Шляхом правового регулювання даної сфери досягається баланс між протилежними суспільними інтересами: потребою в обмеженні доступу до інформації та потребою в отриманні доступу до інформації. Відповідно існують дві групи правових засобів: правові засоби інформаційної безпеки у сфері обмеженого доступу до інформації та правові засоби інформаційної безпеки у сфері отримання доступу до інформації.

У *підрозділі 5.1. «Система засобів кримінально-правової охорони суспільних відносин у сфері обмеженого доступу до інформації: аналіз та шляхи вдосконалення»* зазначається, що кожне посягання на відносини у сфері обмеження доступу до інформації можна віднести до одного з таких видів: 1) отримання незаконного доступу до інформації; 2) надання незаконного доступу до інформації. Під отриманням незаконного доступу пропонується 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, являє собою результат дій зловмисника, що полягає у створенні можливості ознайомлення з певною інформацією з обмеженим доступом для особи, яка не має права на це.

Система кримінально-правових засобів забезпечення обмеженого доступу до інформації, передбачена чинним КК, характеризується: 1) непослідовністю впливу 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 із 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); 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 (ч.ч. 11, 12, ст. 158, ст.ст. 361, 362, 376-1); 3) недоліки законодавчої оцінки 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. У свою чергу, дослідження 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 говорити про фрагментарність і несистемність законодавства в цій сфері. Наявні в КК норми не можуть розглядатись як нормативна база ефективної протидії зростанню тіньової цифрової економіки. Розділяє даний висновок і переважна більшість опитаних працівників правоохоронних органів (85,94 %).

Обґрунтовується, що велика кількість спеціальних заборон у цій сфері являє собою об'єктивну передумову якісного оновлення відповідної системи кримінально-правових засобів. Доцільною видається відмова від розгалуженої системи норм, які передбачають відповідальність за фактично однакові діяння, але стосовно інформації з обмеженим доступом різних видів. При цьому, безсумнівно, є сенс у збереженні низки спеціальних заборон, але тільки тих,

які характеризуються істотно більшою суспільною небезпечністю.

Наведено аргументи щодо доцільності збереження кримінально-правових заборон, передбачених ст.ст. 111, 114, ст. 159, ч. 2 ст. 209-1, ст. ст. 328, 330, 381, 387, 422 КК. Водночас доповнення КК загальними 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 ст.ст. 132, 145, 163, 168, 182, 231, 232 КК, а також ст. 232-1 КК у частині захисту від незаконного надання доступу до інсайдерської інформації. Тому названі норми, у разі прийняття відповідного законодавчого рішення, можуть бути виключені.

У *підрозділі 5.2. «Кримінально-правова охорона суспільних відносин у сфері отримання доступу до інформації»* зазначається, що у загальному розумінні зміст відносин у сфері отримання доступу полягає в наявності в одних суб'єктів права на отримання певної інформації та відповідного обов'язку в інших надавати її. Порушення таких відносин полягає у ненаданні інформації або наданні неправдивої чи неповної інформації особою, яка має зобов'язання щодо надання доступу до цих відомостей. Дослідження системи кримінально-правових засобів у сфері забезпечення отримання доступу до інформації методом контекстної законодавчої оцінки суспільної небезпечності дозволяє стверджувати, що вона відповідає чинникам фактичної небезпечності відповідних посягань, є послідовною та обґрунтованою. Однак, з огляду на те, що забезпечення отримання доступу до інформації є достатньо соціально значущим, актуальності набуває питання доповнення КК загальною нормою про відповідальність за обмеження доступу до інформації. Дослідження зарубіжного досвіду в цій сфері й аналіз можливостей застосування чинного законодавства про кримінальну відповідальність дозволяють зробити такі висновки: 1) ефективність кримінально-правового захисту відносин у сфері надання доступу до інформації залежить передусім від якості правового регулювання інформаційних відносин; 2) передбачена чинним законодавством система відповідних кримінально-правових засобів є обґрунтованою та достатньою, дозволяє забезпечити ефективний захист відносин у сфері надання доступу до інформації, доповнення КК новими нормами в цій сфері є недоцільним; 3) перспективним напрямом кримінально-правових досліджень видається аналіз можливостей використання чинних законів про кримінальну відповідальність за зловживання, перевищення повноважень і недбалість як засобів правової охорони прав громадян на доступ до інформації.

Розділ 6 «Кримінально-правова охорона суспільних відносин у сфері формування інформаційного ресурсу» містить два підрозділи.

У *підрозділі 6.1. «Кримінально-правова охорона у сфері формування інформаційного ресурсу в контексті соціальних тенденцій»* зазначається, що проведений аналіз системи норм про кримінальну відповідальність за злочини у сфері формування інформаційного ресурсу методом контекстної оцінки суспільної небезпечності діяння дозволяє встановити, що в цілому ця система є обґрунтованою, однак спостерігається певне необґрунтоване завищення суворості санкцій за окремі дії з порнографічними предметами. Разом із цим, 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, можливості маніпулювання свідомістю. У зв'язку з цим розглядається питання про доцільність доповнення КК нормами про відповідальність за поширення суспільно шкідливої інформації, використання сучасних інформаційних технологій для розповсюдження асоціальної інформації. Обґрунтовується висновок про те, що розширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення суспільно шкідливої інформації є недоцільним через прогнозовану неефективність і декларативність таких норм, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації.

У *підрозділі 6.2. «Можливі напрями подальшого наукового пошуку з питань кримінально-правового забезпечення формування інформаційного ресурсу»* зазначається, що оскільки інформаційна безпека є багатоаспектним поняттям, певні проблеми кримінально-правової охорони інформаційної безпеки можуть, а в умовах становлення інформаційного суспільства й повинні стати предметом суміжних досліджень.

По-перше, обґрунтовується та підтверджується в ході дослідження судової практики, що ефективність кримінально-правової протидії порушенням авторського права на програмне забезпечення є недостатньою оскільки у сфері кримінальної юстиції крім дійсно суспільно небезпечних посягань, опиняються діяння, які не можна визнавати суспільно небезпечними. Лише 14,38 % опитаних працівників правоохоронних органів оцінюють рівень ефективності протидії означеним посяганням як достатній, тоді як 47,50 % вважають його задовільним, а 38,12 % – незадовільним. Тому до можливих напрямів подальшого наукового розроблення проблем кримінально-правової охорони інформаційної безпеки слід віднести: вдосконалення порядку обчислення матеріальної шкоди від порушення авторського права на програмне забезпечення, проведення додаткових кримінологічних досліджень, з метою диверсифікації засобів протидії означеним посяганням.

Наступною проблемою є кримінально-правове забезпечення процесів інформатизації в Україні. Вкрай незадовільна динаміка цього надважливого суспільного процесу, перебуває у явній невідповідності зі значними адресними витратами державного бюджету. Виникає потреба в науковому аналізі можливостей використання засобів кримінальної юстиції для забезпечення ефективного використання державних ресурсів у сфері інформатизації.

Останньою проблемою, на яку необхідно звернути увагу, є кримінально-правова протидія зловживанням у сфері збирання персональних даних. Певну увагу цій проблемі було приділено в розділі 5 дисертації, 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 персональних даних може через розширення можливостей органів державної влади створювати загрозу демократичному розвитку країни або забезпечувати умови для специфічних зловживань у комерційній сфері. Відсутність або недостатня ефективність законодавчих обмежень збирання персональної інформації небезпечна створенням тотальних інформаційних систем персональних даних і, відповідно, тотальним контролем над поведінкою індивідів. При цьому нещодавні зміни до ст. 182 КК, особливо в контексті принципу суспільної небезпечності криміналізації, не можуть бути сприйняті беззаперечно. Видається, що суспільно небезпечними такі дії можуть розглядатися в тих випадках, коли виступають видами зловживання або перевищення повноважень (ст.ст. 364, 364-1, 365, 365-1 КК) чи недбалості (ст. 367 КК). Отже, наступним напрямом наукового пошуку у сфері кримінально-правового забезпечення інформаційної безпеки має стати дослідження можливостей використання для протидії суспільно небезпечним видам незаконного зберігання персональних даних законів про кримінальну відповідальність за перевищення повноважень, зловживання ними або недбалість.

ВИСНОВКИ

У **висновках** дисертації викладено концептуальні положення щодо кримінально-правової охорони інформаційної безпеки, розроблено оптимальну модель системи норм КК України, що передбачають відповідальність за злочини в означеній сфері, на цій основі вироблено пропозиції щодо вдосконалення чинного законодавства про кримінальну відповідальність.

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 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. Суспільна небезпечність посягань на інформаційну безпеку визначається значенням тих суспільних відносин, в межах яких виникає інформаційна потреба.

Оскільки інформаційна безпека являє собою систему суспільних відносин, частина яких потребує кримінально-правового захисту, та характеризується специфічним, властивим саме цій групі відносин, змістом чинників суспільної небезпечності посягань на них, доцільним є включення інформаційної безпеки до системи родових об’єктів злочинів, передбачених КК України.

Основні положення щодо вдосконалення кримінально-правової охорони інформаційної безпеки у сфері використання інформаційних технологій полягають у наступному:

- доцільною є побудова відповідних кримінально-правових заборон на основі юридичних конструкцій властивих злочинам з похідними наслідками;
- система безпосередніх об’єктів даних злочинів повинна включати:

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;

- в якості додаткових обов'язкових об'єктів слід передбачити суспільні відносини у сфері: реалізації прав, свобод або законних інтересів окремих фізичних осіб; реалізації державних чи громадських інтересів; нормальної діяльності юридичних осіб (установ, підприємств, організацій);

- структура об'єктивної сторони цих злочинів повинна включати як основні наслідки – різні форми порушення запропонованих безпосередніх об'єктів, так і похідні наслідки; 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.

- для забезпечення подальшої диференціації кримінальної відповідальності за злочини у сфері використання інформаційних технологій пропонується в окремих статтях передбачити відповідальність за посягання, пов'язані з умисним або необережним ставленням до похідних наслідків.

Кримінально-правова охорона відносин інформаційної безпеки в сфері забезпечення доступу до інформації складається з охорони суспільних відносин у сфері обмеженого доступу до інформації та у сфері реалізації прав на доступ до інформації. Охорона останньої групи суспільних відносин на достатньому рівні забезпечена нормами чинного КК. У свою чергу, для оптимізації кримінально-правової охорони відносин у сфері обмеженого доступу до інформації, побудови системи норм, яка б відповідала встановленій специфіці суспільної небезпечності посягань на інформаційну безпеку, пропонується доповнення КК загальними нормами про відповідальність за незаконне надання доступу до інформації та його незаконне отримання, та виключення ст.ст. 132, 145, 163, 168, 182, 231, 232 КК, а також ст. 232-1 КК у частині заборони незаконного надання доступу до інсайдерської інформації. При цьому доцільним є збереження кримінально-правових заборон, передбачених ст.ст. 111, 114, 159, ч. 2 ст. 209-1, ст. ст. 328, 330, 381, 387, 422 КК.

Дослідження соціальних тенденцій та закономірностей формування інформаційного ресурсу дозволило встановити, що хоча кількісні та якісні показники формування національного інформаційного ресурсу свідчать про значний потенціал можливих суспільно небезпечних наслідків, розширення кримінально-правових засобів забезпечення інформаційної безпеки у сфері формування інформаційного ресурсу, доповнення КК новими нормами про відповідальність за поширення суспільно шкідливої інформації є недоцільним.

У порядку реалізації послідовно підтримуваної ідеї щодо змісту інформаційної безпеки як самостійного об'єкта кримінально-правової охорони та специфіки суспільної небезпечності посягань на неї пропонується:

1) назву розділу XVI Особливої частини КК викласти у наступній редакції «Злочини у сфері інформаційної безпеки»;

2) виключити з КК ст.ст. 132, 145, ч. 11 ст. 158, ст.ст. 163, 168, 182, 231, 232, 376-1;

3) абзац перший ч. 12 ст. 158 КК викласти у наступній редакції:

«Дії, передбачені частинами дев'ятою або десятою цієї статті, що вплинули на результати голосування виборців на виборчій дільниці або у 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»;

4) ст.ст. 361 – 363-1 КК викласти у наступній редакції:

«Стаття 361. Незаконні дії з комп'ютерними даними

1. Незаконне знищення, блокування, порушення цілісності, порядку маршрутизації 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…

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 попередньою 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…

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, – караються...

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 у заподіяння матеріальних збитків, вважається: а) шкода фізичній особі, заподіяна через обмеження або виключення можливості реалізації нею своїх прав, свобод чи законних інтересів, яка в два або більше разів перевищує неоподатковуваний мінімум доходів громадян; в) 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 у заподіяння матеріальних збитків, вважається, шкода заподіяна через обмеження або виключення можливості реалізації державних чи громадських інтересів, яка в двадцять або більше разів перевищує неоподатковуваний мінімум доходів громадян.

5. У статтях 361 – 361-3 істотним порушення діяльності юридичної особи, якщо воно полягає у заподіянні матеріальних збитків, вважається шкода, яка складається з витрат, які 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.

6. Значною шкодою у статтях 361 – 363, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

7. Тяжкими наслідками у статтях 361 – 363, якщо вони полягають у заподіянні матеріальних збитків, вважаються такі наслідки, які у п'ятсот і більше разів перевищують неоподатковуваний мінімум доходів громадян.

Стаття 361-1. Незаконні дії в 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…

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…

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, – караються…

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...

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 спричинило значну шкоду, – караються…

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, – караються…

Примітка: У статтях 361-2 та 362-2 надання доступу до таємної, службової або конфіденційної інформації не може бути визнано незаконним, якщо суд встановить, що воно було суспільно необхідним.

Стаття 362. Заподіяння необережної шкоди через незаконні дії з комп'ютерними даними

1. Умисне незаконне знищення, блокування, порушення цілісності, порядку маршрутизації чи спотворення процесу обробки комп'ютерних даних, якщо воно з необережності спричинило значну шкоду, – карається…

2. Ті самі діяння, якщо вони з необережності спричинили тяжкі наслідки, – карається…

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 спричинило істотну шкоду – карається…

2. Діяння, передбачене у частині першій, якщо воно з необережності спричинило тяжкі наслідки, – карається...

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…

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…»

5) Доповнити кодекс статтями 361-3, 362-1, 362-2, 362-3 виклавши їх у наступній 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…

2. Те саме діяння вчинене повторно, або за попередньою змовою групою осіб, або якщо воно спричинило значну шкоду, – карається…

3. Діяння, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки, – караються…

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 спричинило значну шкоду, – карається…

2. Ті самі діяння, якщо вони з необережності спричинили тяжкі наслідки, – карається…

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 спричинило значну шкоду, – карається…

2. Те саме діяння, якщо воно необережності спричинило тяжкі наслідки – карається…

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 спричинило значну шкоду, – карається…

2. Те саме діяння, якщо воно з необережності спричинило тяжкі наслідки, – карається...»

6) абзац перший ч. 1 ст. 232-1 КК викласти у наступній 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…».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографія

1. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

(Рецензії: Бурдін В. М. Новий погляд на проблему кримінально-правової охорони інформаційної безпеки // Науковий вісник Львівського державного університету внутрішніх справ. – 2012. – № 2. – С. 382–385; Берзін П. С. Актуальне дослідження кримінально-правової охорони інформаційної безпеки України // Підприємництво, господарство і право. – 2012. – № 10. – С. 144–145).

Статті у наукових фахових виданнях

1. Карчевский Н. В. Средства массовой информации как фактор стабильности общественных отношений / Н. В. Карчевский // Вісник ЛІВС МВС України. – 2000. – № 3. – С. 91–111.

2. Карчевський М. В. Суб'єктивна сторона незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж / М. В. Карчевський // Вісник Львівського інституту внутрішніх справ: Збірник / Гол. ред. В. Л. Ортинський. – Львів : Львівський інститут внутрішніх справ при НАВС України. – 2002. – Вип. 3. – С. 118–124.

3. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу мереж електрозв'язку (нова редакція ст. 361 КК України) / М. В. Карчевський // Вісник Луганської академії внутрішніх справ імені 10-річчя незалежності України. – 2004. – № 2. – С. 220–234.

4. Карчевский Н. В. Информатика и законодательство об уголовной ответственности: система научных проблем / Н. В. Карчевский // Вісник ЛАВС МВС імені 10-річчя незалежності України. – Спец. випуск. –2005. – С. 41–44.

5. 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.

6. Карчевський М. В. Визначення поняття «інформаційна безпека» у контексті юридичної науки / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ. – 2008. – № 1. – С. 88–96.

7. Карчевський М. В. Нормативне регулювання обмеження права інформаційної приватності в контексті вимог європейських законодавчих стандартів / М. В. Карчевський // Вісник ЛДУВС імені Е. О. Дідоренка. – 2009. – № 1. – С. 51–74.

8. Карчевський М. В. Кримінально-правові засоби протидії злочинам в сфері використання комп'ютерної техніки та мереж електрозв'язку характеризуються як надлишковістю заборони так і прогалинами / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2010. – № 4. – С. 97–107.

9. Карчевський М. В. Соціальні передумови правових заходів інформаційної безпеки / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2011. – № 1. – С. 35–55.

10. Карчевський М. В. До питання єдності та визначеності термінології при криміналізації злочинів у сфері використання комп'ютерної техніки та мереж електрозв'язку (розділ XVI КК України) / М. В. Карчевський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – № 23. – С. 316–322.

11. Карчевський М. В. Спам може бути корисним: досвід правового регулювання розсилки множинних електронних повідомлень у США / М. В. Карчевський // Підприємництво, господарство і право. – № 6. – 2011. – С. 131–135.

12. Карчевський М. В. Чи відповідає КК України потребам протидії злочинам у сфері використання комп'ютерної техніки? / М. В. Карчевський // Право України. – 2011. – № 7.– С. 203–209.

13. Карчевський М. В. Метод контекстної законодавчої оцінки суспільної небезпечності діяння / М. В. Карчевський // Вісник Луганського державного

університету внутрішніх справ імені Е. О. Дідоренка. – 2011. – № 3. – С. 51–64.

14. Карчевський М. В. Вдосконалення закону про кримінальну відповідальність за розповсюдження шкідливих технічних та програмних засобів / М. В. Карчевський // Актуальні проблеми права: теорія і практики : збірник наукових праць № 22. – Луганськ : Східноукраїнський національний університет імені Володимира Даля, 2011. – С. 311–316.

15. Карчевський М. В. Деякі причини недостатньої ефективності кримінально-правової протидії «комп'ютерному піратству» в Україні / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2011. – № 4. – С. 56–68.

16. Карчевський М. В. Особливості кваліфікації злочинів проти власності, що вчиняються з використанням комп'ютерної техніки / М. В. Карчевський // Підприємництво, господарство і право. – № 1. – 2012. – С. 139–142.

17. Карчевський М. В. Можливості забезпечення доступу до інформації кримінально-правовими засобами / М. В. Карчевський // Проблеми правознавства та правоохоронної діяльності. – 2012. – № 1 (48). – С. 85–90.

18. Карчевський М. В. Питання оптимізації зобов'язань, зумовлених ратифікацією Конвенції про кіберзлочинність / М. В. Карчевський // Бюлетень Міністерства юстиції України. – 2012. – № 3. – С.70–74.

19. Карчевський М. В. Положення чинного КК України в контексті тенденцій формування національного інформаційного простору / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2012. – № 2. – С. 107–117.

20. Карчевський М. В. Недоліки та можливі шляхи вдосконалення системи кримінально-правових засобів забезпечення обмеженого доступу до інформації / М. В. Карчевський // Науковий вісник Львівського державного університету внутрішніх справ. – 2012. – № 1. – С. 304–312.

21. Карчевський М. В. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони / М. В. Карчевський // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 27. – С. 267–272.

22. Карчевский Н. В. Особенности криминализации общественно опасных посягательств в сфере информационной безопасности / Н. В. Карчевский // Вопросы правоведения. – 2012. – № 4. – С. 154–165.

Статті, виступи, тези доповідей,
які додатково відображають наукові результати дисертації

1. Карчевский Н. В. Проблемы совершенствования уголовно-правовой защиты авторского права на программное обеспечение и перспективы их разрешения / Н. В. Карчевский // Вісник ЛІВС МВС України. – 1998. – № 2. – С. 93–99.

2. Карчевський М. В. Злочини в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку, що вчиняються організованими

злочинними групами та злочинними організаціями: проблеми кваліфікації та попередження / М. В. Карчевський // Компьютерная преступность и кибертерроризм : исследования по Программе малых грантов. – Запорожье : Центр исследования компьютерной преступности. – 2004. – Выпуск первый. – С. 48–84.

3. Карчевський М. В. Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж (ст. 361 КК України): аналіз складу злочину / М. В. Карчевський // Збірник наукових праць Харківського Центру по вивченню організованої злочинності спільно з Американським Університетом у Вашингтоні. – Х. : Східно-регіональний центр гуманітарно-освітніх ініціатив. – 2004. – Випуск восьмий. – С. 143–189.

4. Карчевський М. В. Проблеми кваліфікації незаконного втручання в роботу мереж електрозв'язку (нова редакція ст. 361 КК України) / М. В. Карчевський // Компьютерная преступность и кибертерроризм : сборник научных статей / Под ред. Голубева В. А., Ахтырской Н. Н. – Запорожье : Центр исследования компьютерной преступности, 2004. – Вып. 2. – С. 136–141.

5. Карчевський М. В. Незастосування заходів щодо захисту інформації як фактор вчинення злочинів у сфері комп'ютерної інформації / М. В. Карчевський // Віктимологічні аспекти злочинності: Кримінологічні дослідження : Випуск 1 / Луган. держ. ун-т внутр. справ ; Луган. гуманіт. Центр ; [Відп. ред. В. І. Поклад]. – Луганськ : РВВ ЛДУВС, 2006. – С. 63–69.

6. Карчевський М. В. Проблеми відмежування комп'ютерних злочинів від злочинів проти власності, пов'язаних з використанням комп'ютерної техніки / М. В. Карчевський // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их разрешения : материалы международной научно-практической конференции. – Донецк : ДЮИ ЛГУВД, 2007. – С. 335–340.

7. Карчевский Н. В. Квалификация деяний, предусмотренных Конвенцией о киберпреступности, в соответствии с украинским уголовным законодательством / Н. В. Карчевский // Вісник ЛДУВС імені Е. О. Дідоренка. – Спеціальний випуск у двох частинах № 6. – 2008. – Ч. 1. – С. 148–162.

8. Карчевський М. В. Комп'ютерна інформація, як предмет злочинів в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку / М. В. Карчевський // Боротьба зі злочинами у сфері комп'ютерної інформації: проблеми та шляхи їх вирішення : Матеріали міжвузівської науково-практичної конференції. – Донецьк : ДЮІ ЛДУВС, 2008. – С. 61–64.

9. 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.

10. Карчевський М. В. Деякі питання практики застосування кримінального законодавства про злочини в сфері використання комп'ютерної техніки / М. В. Карчевський // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали

всеукраїнської науково-практичної конференції (м. Донецьк, 4 грудня 2009 р.). – Донецький юрид. ін-т ЛДУВС ім. Е. О. Дідоренка. – Донецьк : ДЮІ ЛДУВС, 2009. – С. 63–71.

11. Карчевский Н. В. Направления совершенствования украинского законодательства о компьютерных преступлениях в контексте Конвенции о киберпреступности / Н. В. Карчевский // Международная научно-практическая конференция «Обеспечение законности и правопорядка в странах СНГ» : сборник материалов. – Ч. 1. Юридические науки. – Воронеж : Воронежский институт МВД России, 2009. – С. 17–21.

12. Карчевський М. В. Межі та критерії ефективного правового регулювання масових розсилок електронних повідомлень / М. В. Карчевський // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукраїнської науково-практичної конференції, (м. Донецьк, 12 листопада 2010 р.) / ДЮІ ЛДУВС ім. Е. О. Дідоренка. – Донецьк, 2010. – С. 34–39.

13. Карчевський М. В. Напрямки вдосконалення системи кримінально-правових засобів забезпечення обмеженого доступу до інформації / М. В. Карчевський // 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. 373–377.

14. Карчевський М. В. Поняття та сутність інформаційної безпеки як об'єкта кримінально-правової охорони / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. Інформаційне забезпечення розслідування злочинів у сучасних умовах. – Спец. випуск № 3. – 2011. – С. 156–162.

15. Карчевський М. В. Легітимація заборони розповсюдження та збуту шкідливих програмних та технічних засобів / М. В. Карчевський // 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. 212–217.

16. Карчевський М. В. Основні напрями вдосконалення кримінально-правового забезпечення інформаційної безпеки / М. В. Карчевський // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукраїнської науково-практичної конференції, м. Донецьк, 9 грудня 2011 р. / Донецький юрид. ін-т МВС України. – Донецьк : ДЮІ МВС України, 2012. – С. 53–57.

17. Карчевський М. В. До питання доцільності використання кримінально-правових засобів у сфері формування інформаційного ресурсу / М. В. Карчевський // Теоретичні та прикладні проблеми сучасного кримінального права : матеріали

ІІ міжнар. наук-практ. конф., м. Луганськ, 19-20 квітня 2012 р. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – С.210–216.

18. Карчевський М. В. До питання ефективності кримінально-правової охорони авторського права / М. В. Карчевський // Кримінальний кодекс України 2001 р.: проблеми застосування і перспективи удосконалення: тези доповідей та повідомлень учасників Міжнародного симпозіуму, 21-22 вересня 2012 р. – Львів : Львівський державний університет внутрішніх справ, 2012. – С. 333–337.

19. Карчевський М. В. Метод контекстної законодавчої оцінки суспільної небезпечності діяння / М. В. Карчевський // Основні напрями розвитку кримінального права та шляхи вдосконалення законодавства України про кримінальну відповідальність : матеріали міжнар. наук.-практ. конф., 11-12 жовтня 2012 р. / редкол. : В. Я. Тацій (голов. ред.), В. І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2012. – С. 156–159.

Підручники, навчальні посібники

1. Карчевский Н. В. Уголовное право. Общая часть : учеб. пособ. (схемы и таблицы) / Н. В. Карчевский ; Луганская академия внутренних дел им. 10-летия независимости Украины. – Луганск : РИО ЛАВД, 2005. – 278 с.

2. Карчевський М. В. Злочини в сфері використання комп'ютерної техніки : навч. посібн. / М. В. Карчевський. – К. : Атіка, 2010. – 168 с.

3. Карчевський М. В. Розділ 17. Злочини в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку // Кримінальне право України. (Особлива частина) : підруч. [А. М. Бабенко, Ю. А. Вапсва, В. К. Грищук та ін.] ; за заг. ред. О. М. Бандурки ; МВС України, Харків. нац. ун-т внутр. справ. – Х. : Вид-во ХНУВС, 2011. – С. 451–463.

4. Карчевський М. В. Глава 14. Повторність, сукупність і рецидив злочинів // Кримінальне право. Загальна частина : підруч. / За ред. А. С. Беніцького, В. С. Гуславського, О. О. Дудорова, Б. Г. Розовського. – К. : Істина, 2011. – С. 611–630.

5. Карчевський М. В. Глава 18. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), система та комп'ютерних мереж і мереж електрозв'язку // Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 2 – Луганськ : видавництво «Елтон-2», 2012. – С. 373–391.

АНОТАЦІЯ

Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України. – Рукопис.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. – Національна академія внутрішніх справ, Київ, 2013.

Дисертація присвячена дослідженню проблем тлумачення, застосування та вдосконалення кримінального законодавства, що передбачає відповідальність за злочини у сфері інформаційної безпеки. Врахування результатів проведеного дослідження при подальшому вдосконаленні законодавства дозволить сформулювати ефективну систему кримінально-правової охорони інформаційної безпеки. Отримані законодавчі положення враховуватимуть специфіку суспільної небезпечності посягань на неї та чітко обмежуватимуть відповідну сферу кримінально-правового впливу, чим, у свою чергу, створять умови для підвищення ефективності протидії злочинам у сфері інформаційної безпеки.

Ключові слова: інформатизація, інформаційне суспільство, інформаційна безпека, злочин, криміналізація, законодавча оцінка суспільної небезпечності, кіберзлочинність, доступ до інформації, формування інформаційного ресурсу.

АННОТАЦИЯ

Карчевский Н. В. Уголовно-правовая охрана информационной безопасности Украины. – Рукопись.

Диссертация на соискание ученой степени доктора юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. – Национальная академия внутренних дел, Киев, 2013.

В диссертации исследуются проблемы толкования, применения и совершенствования законодательства об уголовной ответственности за преступления в сфере информационной безопасности.

Информационную безопасность предлагается рассматривать как систему общественных отношений, обеспечивающую возможность реализации информационной потребности граждан, общества, государства. Субъект находится в состоянии информационной безопасности тогда, когда эффективность его деятельности обеспечена полной, достоверной и достаточной для принятия решений информацией. Такое состояние достигается социальной активностью в трех взаимосвязанных группах общественных отношений, представляющих собой структурные элементы информационной безопасности: общественные отношения в сфере использования информационных технологий, в сфере обеспечения доступа к информационному ресурсу и в сфере формирования информационного ресурса. При этом, общественная опасность посягательств на информационную безопасность не является самостоятельной, зависит от социальной значимости тех отношений, в пределах которых возникает информационная потребность.

Относительно уголовно-правовой охраны отношений информационной безопасности в сфере использования информационных технологий установлено, что наиболее существенным недостатком действующего законодательства является нарушение принципа общественной опасности криминализации: из-за отсутствия в законодательных определениях четких критериев общественной опасности в сфере уголовной юстиции оказываются как действительно общественно опасные деяния, так и те, которые таковыми не являются. Такое

положение резко негативно сказывается на эффективности уголовно-правовой охраны информационной безопасности. Также установлено нарушение таких принципов криминализации, как определенность и единство терминологии, отсутствие пробелов, полнота составов. Для формулирования нормативных определений компьютерных преступлений, которые бы учитывали специфику их общественной опасности, предлагается решение, основывающееся на применении законодательных конструкций преступлений с производными последствиями.

Анализ предусмотренной действующим законодательством системы уголовно-правовых средств обеспечения ограниченного доступа к информации, позволил установить, что она характеризуется непоследовательностью влияния факторов общественности на интенсивность санкций за отдельные виды незаконного предоставления или получения доступа к информации.

Обосновывается, что большое количество специальных запретов в этой сфере представляет собой объективную предпосылку качественного обновления соответствующей системы уголовно-правовых средств. При совершении незаконного предоставления доступа к информации необходимость применения средств уголовной юстиции, а также их интенсивность должны зависеть не от вида информации с ограниченным доступом, а от того, какие последствия наступили. Потому предлагается отказ от разветвленной системы норм, которые предусматривают ответственность за фактически одинаковые деяния, но относительно информации с ограниченным доступом разных видов. При этом, несомненно, есть смысл в сохранении ряда специальных запретов, характеризующихся существенно большей общественной опасностью.

Указывается, что, несмотря на значительный потенциал общественно опасных последствий коммерциализации формирования национального информационного ресурса, расширение уголовно-правовых средств обеспечения информационной безопасности в данной сфере, дополнение УК новыми нормами об ответственности за распространение общественно вредной информации является нецелесообразным. В условиях глобализации информационного поля подобные законодательные решения будут неэффективными и декларативными, кроме того, они бы не соответствовали принципам уголовно-политической адекватности, а также соразмерности положительных и негативных последствий криминализации.

С учётом установленных тенденций и закономерностей уголовно-правового обеспечения информационной безопасности сформулированы предложения по совершенствованию действующего законодательства об уголовной ответственности.

Ключевые слова: информатизация, информационное общество, информационная безопасность, преступление, криминализация, законодательная оценка общественной опасности, киберпреступность, доступ к информации, формирование информационного ресурса.

SUMMARY

Karchevskyy M V. Criminal protection of information security of Ukraine. – Manuscript.

Thesis for a doctor's degree with specialization 12.00.08 – Criminal Law and Criminology; Criminal Executive Law. – National Academy of Internal Affairs, Kyiv, 2013.

Thesis deals with the interpretation, application and improvement of the criminal law, which stipulates responsibility for crimes in the field of information security. Taking into account the results of the study in further improving legislation will formulate effective criminal protection of information security. The obtained legislative provisions take into account the specifics of the social danger of attacks on it and clearly limit the scope of the relevant criminal and legal action, that, in its turnwill create the conditions for enhancement of efficiency of counteraction to crimes in the field of information security.

Keywords: informatization, information society, information security, crime, criminal prosecution, legal assessment of public danger, cybercrime, access to information, the formation of an information resource.