ДЕРЖАВНА ФІСКАЛЬНА СЛУЖБА УКРАЇНИ
УНІВЕРСИТЕТ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

РИЧКА ДЕНИС ОЛЕГОВИЧ

УДК 343.3/.7:004.056.5](477)

ОСОБЛИВОСТІ КРИМІНАЛЬНО-ПРАВОВОЇ КВАЛІФІКАЦІЇ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук

Ірпінь – 2019

Дисертацією є рукопис

Робота виконана на кафедрі адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара

Науковий керівник:
доктор юридичних наук, доцент,
заслужений юрист України
Корнякова Тетяна Всеволодівна,
Дніпровський національний університет імені Олеся Гончара,
завідувач кафедри адміністративного
і кримінального права

Офіційні опоненти:
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
заслужений діяч науки і техніки України
Музика Анатолій Ананійович,
Державний науково-дослідний інститут МВС України,
провідний науковий співробітник
науково-дослідної лабораторії кримінологічних
досліджень та проблем запобігання злочинності

доктор юридичних наук, доцент
Мірошниченко Сергій Сергійович,
Університет державної фіскальної служби України,
професор кафедри кримінального права та кримінології

Захист відбудеться 30 травня 2019 року о 12^{00} годині на засіданні спеціалізованої вченої ради Д 27.855.03 в Університеті державної фіскальної служби України за адресою: 08205, м. Ірпінь, вул. Університетська, 31

З дисертацією можна ознайомитись у бібліотеці Університету державної фіскальної служби України за адресою: 08205, м. Ірпінь, вул. Університетська, 31

Автореферат розіслано «26» квітня 2019 року

Учений секретар
спеціалізованої вченої ради **І. В. Грицюк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Забезпечення інформаційної безпеки в Україні є однією з найважливіших функцій держави, адже добробут нації залежить від інформаційної складової. На сьогоднішній день стан криміногенної ситуації вимагає розробки та впровадження заходів для запобігання злочинним посяганням на об'єкти у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку.

Унаслідок соціально-економічних проблем Україна суттєво відстає у розвитку від країн-учасниць Конвенції про кіберзлочинність. Кібервійни, кібертероризм, кібершпигунство стали звичними, тому злочинність у інформаційній сфері є суттєвою загрозою національній безпеці України.

Зареєстрований масив злочинних посягань у аналізованій сфері свідчить про суттєве зростання рівня цих злочинів за останні роки і має такі показники: у 2013 році було обліковано 595 злочинів, у 2014 році – 443, у 2015 році – 598, у 2016 році – 865, у 2017 році – 2573, у 2018 році – 2301 злочин[1].

До питання кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку зверталося чимало провідних вітчизняних і зарубіжних учених. Серед них, зокрема: Д. С. Азаров, Ю. М. Батурин, П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, А. Г. Волевоз, О. В. Демешко, І. В. Європіна, М. В. Карчевський, С. А. Кузьміна, О. В. Мазоліна, К. В. Манжула, В. М. Машкова, С. С. Мірошниченко, А. А. Музика, М. В. Рудика, В. П. Шеломенцева, М. П. Бікмурзіна, Т. В. Корнякова, В. В. Кузнецова, Є. В. Лащук, Є. І. Литвинов, Ю. М. Онищенко, П. І. Орлова, С. О. Орлов, О. Е. Радутний, Н. А. Розенфельд, В. С. Романюк, О. В. Смаглюк, Л. В. Сорока, В. С. Цимбалюк, С. В. Шапочка, Н. С. Юзікова, І. О. Юрченко, К. В. Юртаєва та інші.

На рівні дисертаційних робіт окремі аспекти зазначеної проблематики вивчалися М. В. Карчевським «Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)» (2003 р.), «Кримінально-правова охорона інформаційної безпеки України» (2013 р.), О. Е. Радутним «Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю» (2002 р.), Н. А. Розенфельд «Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (2003 р.).

У 2005 році вийшов науково-практичний коментар за редакцією А.А. Музики та Д.С. Азарова «Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення», який присвячено кримінально-правовому аналізу складів злочинів, передбачених статтями розділу XVI «Злочини у сфері використання електронно-обчислювальних

[1] Єдиний звіт про кримінальні правопорушення по державі : офіційний сайт Генеральної прокуратури України URL : https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402 (дата звернення 04.12.2018)

машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини Кримінального кодексу України (далі – КК України) та суміжних з ними посягань.

Однією з найновіших наукових досліджень є дисертація на здобуття наукового ступеня кандидата юридичних наук С. В. Шапочки «Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж» (2018 р.), у якій запропоновано власну класифікацію шахрайства, що вчиняється з використанням комп'ютерних мереж, визначаються детермінанти та ступінь його латентності.

Водночас, при всій значущості цих та інших наукових напрацювань, на сьогодні існує чимало проблем у здійсненні кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, відсутній комплексний кримінально-правовий аналіз кваліфікації злочинів у даній сфері. Наведене свідчить про актуальність і своєчасність обраної теми наукового дослідження, необхідність вивчення кримінально-правової кваліфікації злочинних посягань та побудови моделі запобігання злочинам у цій сфері.

Зв'язок роботи із науковими програмами, планами, темами. Дисертація виконана відповідно до Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 11 липня 2018 року № 481-р; Стратегії кібербезпеки України від 15 березня 2016 року № 96/2016, затвердженої та введеної у дію Указом Президента України від 15 березня 2016 року № 96/2016, Стратегії розвитку наукових досліджень Національної академії правових наук України на 2016–2020 роки, затвердженої постановою Загальних зборів Національної академії правових наук України від 03.03.2016 року. Дослідження узгоджується зі Стратегією національної безпеки України від 26 травня 2015 року№ 287/2015, затвердженої та введеної у дію Указом Президента України від 26 травня 2015 року № 287/2015 та підготовлено відповідно до плану науково-дослідної роботи кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара.

Тема дисертації затверджена Вченою радою Дніпровського національного університету імені Олеся Гончара (протокол № 9 від 18 лютого 2016 року) та уточнена на засіданні Вченої ради Дніпровського національного університету імені Олеся Гончара (протокол № 5 від 23 листопада 2017 року).

Мета і задачі дослідження. *Мета* дисертаційної роботи полягає у визначенні особливостей, притаманних кримінально-правовій кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку і розробці пропозицій щодо вдосконалення норм чинного законодавства.

Для досягнення поставленої мети вирішувалися такі *задачі*:

– розглянути загальнотеоретичні аспекти кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– розкрити ознаки та елементи складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– висвітлити ґенезу та поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– проаналізувати види кіберзлочинності за міжнародним та національним законодавством;

– визначити об'єкт і предмет кіберзлочинів;

– здійснити аналіз та розкрити зміст об'єктивної сторони даної категорії злочинів;

– встановити суб'єктів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– з'ясувати особливості суб'єктивної сторони злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– здійснити спробу удосконалення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Об'єкт дослідження – суспільні відносини, що виникають при здійсненні інформаційних процесів з приводу виробництва, збору, обробки, накопичення, збереження, пошуку, передачі, розповсюдження і споживання комп'ютерної інформації, а так само в інших сферах, де використовуються комп'ютери, комп'ютерні системи і мережі.

Предмет дослідження – особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методи дослідження обрані з урахуванням поставленої мети та завдань дослідження, його об'єкта і предмета. У процесі дослідження використовувались загальнонаукові та спеціальні методи, методологічні принципи та підходи юридичної науки, які застосовувалися для вирішення поставлених завдань та забезпечення достовірності отриманих результатів, висновків та рекомендацій наукового пізнання.

В основу дисертації покладено *діалектичний метод*, як загальнонауковий метод пізнання соціально-правових явищ в їх протиріччях, розвитку та змінах, що надало можливість визначити особливості здійснення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (підрозділи 2.1, 2.2, 3.1, 3.2, 3.3, 3.4, 3.5). *Логіко-семантичний метод* використано для вдосконалення понятійного розуміння кримінально-правової кваліфікації злочинів та дослідження основних рис кримінально-правової кваліфікації кібернетичних злочинів (підрозділи 1.1, 1.2). *Історико-правовий метод* надав можливість дослідити генезис наукової думки щодо змісту використаних у дослідженні правових понять (підрозділи 2.1, 2.2). *Системно-структурний метод* дозволив визначити проблемні питання, які виникають під час здійснення кваліфікації (підрозділи 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 3.4, 3.5). *Статистичний метод* використовувався у процесі узагальнення, групування та аналізу емпіричного

матеріалу та оцінки кількісних і якісних показників сучасного стану злочинності в Україні (підрозділи 3.1, 3.2, 3.3, 3.4, 3.5). Застосування *порівняльного (компаративістського) методу* надало можливість дослідити досвід зарубіжних країн у боротьбі з кіберзлочинами (підрозділ 2.2). *Метод контент-аналізу* офіційних матеріалів, матеріалів друкованих ЗМІ та електронних Інтернет-ресурсів дозволив проаналізувати результативність роботи правоохоронних і судових органів у запобіганні злочинам у даній сфері (підрозділи 2.1, 2.2, 3.2, 3.3, 3.4, 3.5). *Синергетичний метод* дозволив вивчити складові кримінально-правової характеристики, що відображено у структурі наукового дослідження (підрозділи 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 3.3, 3.4, 3.5).

Емпіричну базу дослідження становлять статистичні дані Генеральної прокуратури України, Міністерства внутрішніх справ України, Державної служби статистики України за період 2013-2018 років; вибірковий аналіз матеріалів кримінальних проваджень (справ) за період 2013-2018 рр. за статтями 361-363-1 КК України, чим забезпечено обґрунтованість і достовірність сформованих у дисертації наукових положень, висновків, пропозицій і рекомендацій.

Наукова новизна отриманих результатів визначається тим, що дисертація є однією з перших у вітчизняній кримінально-правовій науці досліджень проблемних питань кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Результатом проведеного дослідження стала низка нових наукових положень і висновків, здобутих особисто дисертантом. Найважливіші з них зведено до наступних положень:

вперше:

– з метою уніфікації норм законодавства та уникнення колізій у визначенні діянь, що підпадають під ознаки злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку, та кіберзлочинів за законодавством країн-членів Конвенції про кіберзлочинність запропоновано замінити назву Розділу XVI КК України «Кіберзлочини» замість «Злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»;

– сформульовано авторське визначення категорії «злочинна необачність», яка включає у себе ознаки непрямого умислу і злочинної самовпевненості (легковажності), оскільки саме така форма вини притаманна ст. 361-1 КК України;

– запропоновано спростити процедуру визначення покарань за злочини даної категорії, а саме надати правовому режиму мережі Інтернет статус, подібний до статусу територій загального користування;

– запропоновано запровадити інститут відшкодування шкоди до кібернетичних злочинів з метою матеріальної компенсації порушених прав потерпілих;

удосконалено:

– статтю 361 КК України приміткою: «Під незаконним втручанням в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж розуміється проникнення до систем та мереж без дозволу на це власника такої інформації чи уповноваженої на це особи з можливістю розпорядження»;

– статтю 362 КК України доповненням: «... наявність в особи права доступу до інформації та реалізації такої можливості зі злочинним наміром»;

– частину 2 статті 362 КК України, а саме виключенням поняття «перехоплення», у зв'язку з відсутністю доступу суб'єкта до охоронюваної законом інформації. Пропонується введення нової статті до Розділу XVI, яка б передбачала відповідальність саме за перехоплення інформації, яка обробляється в ЕОМ, АС, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненого особами, які не мають на це права доступу, або ж доповнити статтю 361-2 Кримінального кодексу України;

– статтю 363 КК України наступним чином: «Порушення правил експлуатації автоматизованих ЕОМ, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж, якщо таке діяння заподіяло істотну шкоду, тобто – призвело до знищення, блокування або модифікації інформації, що на них міститься»;

дістали подальшого розвитку:

– наукові погляди щодо найбільш розповсюджених видів злочинів у кібернетичній сфері, враховуючи норми міжнародного законодавства;

– кваліфікуючі склади за вчинення комп'ютерних злочинів організованими групами та злочинними організаціями, підсилюючи кримінальну відповідальність за умови використання службового становища, не тільки до статті 362 КК України, а й до інших норм розділу.

Практичне значення отриманих результатів полягає в тому, що сформульовані та викладені у дисертації положення, узагальнення, висновки і рекомендації мають як загальнотеоретичне, так і практичне значення та використовуються у:

– *законотворчій діяльності* – для вдосконалення окремих положень чинного Кримінального кодексу України та проектів змін і доповнень до кримінального законодавства України;

– *практичній діяльності* – для підвищення ефективності роботи співробітників правоохоронних і судових органів щодо кримінально-правової кваліфікації злочинів у кібернетичній сфері України (акт впровадження прокуратури Дніпропетровської області від 18 вересня 2018 року);

– *науково-дослідній сфері* – для подальшого дослідження кримінально-правової кваліфікації кіберзлочинів та розробки рекомендацій щодо їх запобігання (акт впровадження Національної поліції України від 15 жовтня 2018 року);

– *освітньому процесі* – для підготовки підручників та навчальних матеріалів при викладанні курсу «Кримінологія», «Кримінальне право», написанні навчально-практичних і методичних посібників, спецкурсів та монографій (акт впровадження Дніпровського національного університету імені Олеся Гончара від 12 листопада 2018 року).

Апробація матеріалів дисертації. Основні положення та висновки дисертаційного дослідження обговорювалися на кафедрі адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара. Результати дослідження були оприлюднені на 4 міжнародних та

всеукраїнських науково-практичних конференціях і семінарах: «Сучасний стан і перспективи розвитку держави і права» (м. Дніпропетровськ, 4-5 грудня 2015 року); «Сучасний стан і перспективи розвитку держави і права» (м. Дніпро, 1-2 грудня 2017 року); «Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності» (м. Хмельницький, 2 березня 2018 року), «Вітчизняна наука на зламі епох: проблеми та перспективи розвитку» (м. Переяслав-Хмельницький, 16 березня 2018 року).

Публікації. Основні положення та висновки, що сформульовані в дисертаційному дослідженні, відображено у 9 наукових публікаціях, серед яких 4 наукові статті – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, 1 стаття – у зарубіжному періодичному виданні та 4 тези доповідей, опубліковані у збірниках матеріалів міжнародних науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 208 сторінок, із них основного тексту – 171 сторінка, список використаних джерел – 19 сторінок (194 найменування) та 11 додатків на 18 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність обраної теми дисертаційного дослідження, розкриваються стан її наукової розробленості та науково-теоретична основа, зв'язок роботи з науковими програмами, планами й темами; визначаються об'єкт, предмет, мета, задачі та методи дослідження; висвітлюється наукова новизна, практичне значення отриманих результатів та форми їхньої апробації, зазначено структуру й обсяг дисертації.

Розділ 1 «Теоретичні аспекти кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» складається з двох підрозділів.

У підрозділі 1.1 «Загальні засади кримінально-правової кваліфікації» висвітлено основоположні засади проведення кримінально-правової кваліфікації, визначено зміст та значення понять «кваліфікація злочинів» та «кримінально-правова кваліфікація».

З'ясовано роль кримінально-правової кваліфікації та підстави, що обумовлюють її проведення. Надано градацію та встановлено обсяг поняття кримінально-правової кваліфікації. Доведено, що кримінально-правова кваліфікація проводиться шляхом дихотомічного поділу родового поняття кримінально-правової кваліфікації. Обґрунтовано, що дослідження кримінального проступку у кібернетиці виступає необхідною складовою забезпечення законності, яка знайшла відображення у Проекті Закону «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень», підтриманого 22 листопада 2018 року.

Кваліфікація (злочинів/кримінальних проступків) у кібернетичній сфері пов'язана з необхідністю встановлення і доведення обставин: факту вчинення суспільно-небезпечного діяння суб'єктом злочину (дія/бездіяльність); відповідності ознак діяння ознакам складу злочину, передбаченого Розділом XVI КК України.

Охарактеризовано офіційну кваліфікацію кіберзлочинів. Кримінально-правова кваліфікація містить у собі кваліфікацію злочинів та інших діянь, які можуть не бути злочинними. Висвітлено процес встановлення уповноваженими на те органами тотожності між юридично-значущими ознаками злочину та ознаками злочинів, які передбачені Кримінальним кодексом України та встановленням між ними відповідності, певного зв'язку.

У підрозділі 1.2 «Склад злочину у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – невід'ємна частина кваліфікації» надано визначення поняття «злочин» та здійснено його відмежування від посягань, що за суспільною небезпечністю не є злочинними.

Проведено аналіз ознак злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Встановлено, що міра суспільної небезпеки злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж, мереж електрозв'язку визначається цінністю інформації, на яку вчиняється злочинне діяння (шляхом вчинення дій, чи внаслідок бездіяльності), та психічним ставленням суб'єкта до наслідків свого діяння, мотивом і метою, яку переслідував злочинець.

З'ясовано, що встановлення юридичної відповідності ознак злочинного діяння ознакам складу злочину є кваліфікацією злочину.

Досліджено склад злочинів у кібернетичній сфері. У структурі складу злочину (на підставі структурного аналізу акту поведінки особи – її діяння) виокремлюють об'єкт (у низці випадків – також і предмет злочину), об'єктивну сторону (до якої відносять суспільно небезпечне діяння, суспільно небезпечні наслідки, причинний зв'язок між діянням і наслідками, місце, час, обстановку, спосіб, засоби вчинення злочину), суб'єктивну сторону (певна форма вини – умисел чи необережність, мотив та мета злочину), суб'єкта злочину (особа фізична, осудна, що досягла віку кримінальної відповідальності).

Розділ 2 «Особливості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» складається з двох підрозділів.

У підрозділі 2.1 «Ключові знання про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» наведено визначення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку; наведено їх регламентацію та досліджено історичне підґрунтя формування злочинності у даній сфері.

Досліджено чинники, що спонукають до вчинення «комп'ютерних» злочинів. Встановлено предмет, об'єкт та особливості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

У зв’язку з тим, що кіберзлочинність досягла транснаціонального рівня, досліджено особливості кіберзлочинів міжнародного характеру та злочинів, вчинених за допомогою комп’ютерної техніки. Транснаціональністю новітніх комп’ютерних технологій є види кіберправопорушень, які вчиняються у різних державах світу. Зазначено, що комп’ютерні злочини можна віднести як до міжнародних злочинів, так і до злочинів міжнародного характеру, що обумовлено об’єктами кібербезпеки: конституційні права та свободи людини і громадянина; сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави та об’єкти критичної інфраструктури.

У підрозділі 2.2 «Види злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» наведено класифікацію міжнародних видів кіберзлочинності та комп’ютерних злочинів за національним законодавством України.

Здійснено аналіз Конвенції про кіберзлочинність, що дозволило виокремити найбільш розповсюджені види кіберзлочинів, до яких віднесено: 1. Незаконний доступ до комп’ютерної системи. 2. Нелегальне перехоплення технічними засобами комп’ютерних даних. 3. Втручання у комп’ютерні дані. 4. Втручання у функціонування комп’ютерної системи. 5. Підробку та шахрайство, пов’язані з використанням комп’ютерів. 6. Правопорушення, пов’язані з дитячою порнографією. 7. Правопорушення, пов’язані з порушенням авторських та суміжних прав.

У зв’язку з появою нових видів комп’ютерних злочинів, сформовано такі доповнення злочинів до Кримінального кодексу України: у сфері фінансових злочинів: скімінг, кеш-трепінг, кардінг; у сфері електронної комерції та господарської діяльності – фішинг; у сфері інтелектуальної власності: піратство, кардшарінг; злочинами у сфері інформаційної безпеки; шахрайство з використанням ЕОМ; нелегальне інформаційне брокерство; кіберпіратство; кібершпигунство; кібервійна.

Наведено та розкрито зміст найбільш розповсюджених видів кібернетичних злочинів. Розтлумачено колізійні норми, що мають місце у міжнародній діяльності держав у сфері регулювання кіберзлочинності.

Розділ 3 «Практичні аспекти кримінально-правової характеристики злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» складається з п’яти підрозділів.

У підрозділі 3.1 «Об’єкт, предмет злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» досліджено позиції вітчизняної та зарубіжної наукової думки, на підґрунті чого сформовано підходи до визначення об’єкта та предмета злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Зазначено, що загальним об’єктом комп’ютерних злочинів є сукупність суспільних відносин, яким завдається шкода внаслідок впливу на інформацію, що

обертається у кібернетичних системах, тобто, внаслідок впливу на її предмет. Родовим об'єктом комп'ютерних злочинів виступають врегульовані законом суспільні відносини автоматизованої обробки інформації. До безпосереднього об'єкта злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку віднесено відносини, що виникають у зв'язку із здійсненням інформаційних процесів.

Встановлено, що до предмету комп'ютерних злочинів віднесено комп'ютерну інформацію та комп'ютерні системи (під якими мається на увазі будь-яка із систем: ЕОМ (комп'ютер), автоматизована система, комп'ютерна мережа чи мережа електрозв'язку).

У підрозділі 3.2 «*Об'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*» проаналізовано ознаки об'єктивної сторони кібернетичних злочинів.

Визначено, що відповідно до Конвенції про кіберзлочинність об'єктивна сторона комп'ютерних злочинів характеризується виокремленням чотирьох груп суспільно небезпечних діянь: проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; суспільно небезпечні діяння, пов'язані з використанням комп'ютерів; суспільно небезпечні діяння, пов'язані із змістом даних; суспільно небезпечні діяння, пов'язані з порушенням авторських і суміжних прав. Об'єктивною стороною кібернетичних злочинів можуть бути як активні дії (ст. 361 КК України), так і злочинна бездіяльність (ст. 363 КК України).

Наголошено, що результати злочинного впливу на комп'ютерну інформацію перебувають у тісному зв'язку з ознаками об'єктивної сторони та їх доцільно розглядати в залежності від наслідків злочинів (витік, втрата, підробка, блокування, порушення встановленого порядку її маршрутизації (ст. 361 КК України), зміна, знищення, блокування комп'ютерної інформації (ст. 362 КК України). При цьому наслідки, до яких можуть призвести кібернетичні злочини, залежать саме від змісту комп'ютерної інформації, яка зазнала шкоди.

Проведено аналіз об'єктивної сторони злочинів, передбачених Розділом XVI КК України, що дозволило сформувати шість моделей злочинного посягання, які розкривають зміст об'єктивної сторони у цій сфері.

Підрозділ 3.3 «*Суб'єкт злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*» присвячено особистості кіберзлочинця. Проведено градацію та типізацію суб'єктів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Доведено, що найбільш розповсюдженими злочинцями у вищеназваній сфері протягом 2017-2018 років стали особи віком від 30 до 50 років (53 %), трохи менше віком від 25 до 30 років (26 %), від 18 до 25 років (14 %), віком від 50 до 65 років (5 %) та від 65 років і вище (2 %). Проводячи класифікацію суб'єктів вчинення комп'ютерних злочинів за сферами їх діяльності встановлено, що 55 % злочинів вчинялися працездатними, які не працювали та не навчалися (найвищий показник); працівники господарських товариств складають 2 %.

Наведено характеристику суб'єктів злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: це загальний суб'єкт (особи, які не мають права доступу до комп'ютерної інформації). Про спеціальний суб'єкт йшлося у випадках, коли особа має право доступу до інформації (ст. 362 КК України); особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363 КК України). Зазначено, що особливим суб'єктом кібернетичних злочинів є хакер. Це особа, яка зламує комп'ютерні системи та мережі з метою фінансової наживи чи з інших мотивів, або ж заради завоювання авторитету в хакерських колах; володіючи вміннями та досвідом, спрямовують свою діяльність на шкоду іншим особам, вчиняючи злочини в комп'ютерних системах.

Враховуючи широкий розвиток технологій та вчинення кібернетичних злочинів особами, які не досягли віку, з якого передбачена кримінальна відповідальність за дану категорію злочинів, пропонується встановити вік настання кримінальної відповідальності з 14-річного віку.

У підрозділі 3.4 «Суб'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» досліджено психічне ставлення суб'єкта до вчиненого діяння і його наслідків, що має вираження у формі умислу або необережності.

Зазначено, що психічним ставленням особи до виконання дій, що входять до складу об'єктивної сторони злочинів в сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку, є умисна форма вини. Тільки злочинні діяння, відповідальність за які передбачена ч. 2 ст. 361-1 і ст. 363 КК України, поєднують в собі умисел і необережність. Досліджено, що у більшості випадках такі злочини визнаються вчиненими навмисно. Виокремлено найбільш розповсюджені мотиви вчинення комп'ютерних злочинів: 1) корисливі мотиви; 2) політичні мотиви; 3) дослідницька цікавість; 4) хуліганські мотиви і бешкетництво; 5) помста.

Обґрунтовано, що застосування статті 361-1 КК України можливе лише за умови встановлення, що винна особа знала про шкідливість програм. У процесі оцінки суб'єктивної сторони складу злочинів, передбачених ст. 361 та ст. 362 КК України, приділено окрему увагу усвідомленню особою, щодо якої є підозра несанкціонованості її дій, оскільки ознаки відсутності в неї такого усвідомлення або відсутність ознак того, що вона мала таке усвідомлення (відсутність підпису про інструктаж, відсутність будь-яких інструкцій з боку власника системи чи інформації тощо), обумовлює і відсутність відповідної форми вини цієї особи – умислу.

Підрозділ 3.5 «Окремі спеціальні питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» присвячено з'ясуванню кваліфікуючих ознак та особливостей проведення кваліфікації у випадках вчинення комп'ютерних злочинів як у кібернетичній сфері, так і у сукупності з іншими сферами злочинних посягань.

З’ясовано, що кваліфікуючими ознаками (ч. 2 ст. 361, ч. 2 ст. 361-1, ч. 2 ст. 361-2, ч. 2 ст. 362 КК України) їх вчинення є: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ними істотної шкоди.

Проведено науковий аналіз кримінально-правової відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, вчинених у складі організованих груп та злочинних організацій. Розглянуто ознаки, притаманні злочинним організаціям та досліджено розподіл ролей та обов’язкової наявності специфічного учасника злочинної групи – хакера.

Досліджено злочини, передбачені розділом XVI КК України та їх співвідношення з іншими складами злочинів. На підставі такого аналізу сформовано правила щодо проведення правильної кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку та діянь, що пов’язані з ними.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та вирішено наукове завдання, що полягає у визначенні особливостей, які притаманні кримінально-правовій кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, і розробці на його основі пропозицій щодо вдосконалення норм чинного законодавства. У результаті проведеного дослідження сформовано низку висновків, пропозицій та рекомендацій, спрямованих на досягнення мети та завдань дослідження.

1. Висвітлено загальнотеоретичні аспекти кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Встановлено, що кримінально-правова кваліфікація зазначених злочинів виступає інструментом реалізації законності у кримінальному провадженні.

Підтримано позицію, що така кваліфікація є якісним відображенням дослідження обставин, за яких вчинено суспільно-небезпечне, протиправне, винне, каране діяння.

Доведено, що термін «кримінально-правова кваліфікація» є ширшим за поняття «кваліфікація злочинів», останнє виступає його складовою частиною, тому до процесу дослідження входять злочини та діяння, визнані малозначними, або ж вчинені за обставин, що виключають злочинність діяння.

2. Розкрито ознаки та елементи складу злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Встановлено, що діяння повинно відповідати ознакам (злочину/кримінального проступку): 1) бути передбаченим у законі про кримінальну відповідальність; 2) суспільно небезпечним; 3) винним; 4) караним. Визначено, що міра суспільної небезпеки злочинів у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж, мереж електрозв’язку визначається цінністю

інформації на яку вчиняється злочинне діяння (шляхом вчинення дій, чи внаслідок бездіяльності), та психічним ставленням суб'єкта до наслідків свого діяння, мотивом і метою, яку переслідував злочинець.

Розкрито особливості, притаманні кібернетичним злочинам, шляхом розкриття основоположних елементів складу злочину. Складом злочину визначається юридичне визначення кіберзлочину, у якому об'єднано його найбільш істотніші, типові та універсальні ознаки. Зазначено, що елементами кіберзлочину є: об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона з урахуванням існуючих у Розділі XVI КК України кваліфікуючих ознак.

3. Висвітлено історичні основи виникнення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Дослідження міжнародних джерел боротьби з кібернетичною злочинністю та відсутність тотожного понятійно-категоріального апарату у національному законодавстві України ускладнює застосування методів боротьби зі злочинами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Саме тому запропоновано змінити назву Розділу XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Кіберзлочини».

4. Розглянуто види кіберзлочинності за міжнародним та національним законодавством України. Ґрунтуючись на позитивному міжнародному досвіді боротьби з кіберзлочинністю та враховуючи появу нових видів злочинів, запропоновано доповнити Кримінальний кодекс України такими видами злочинів: 1. У сфері фінансових злочинів: скімінгом, кеш-трепінгом, кардінгом; 2. У сфері електронної комерції та господарської діяльності – фішингом; 3 У сфері інтелектуальної власності – піратством, кардшарінгом; 4. Злочинами у сфері інформаційної безпеки; 5. Шахрайством з використанням ЕОМ; 6. Нелегальним інформаційним брокерством; 7. Кіберпіратством; 8. Кібершпигунством; 9. Кібервійною.

5. Встановлено, що загальним об'єктом комп'ютерних злочинів виступає сукупність суспільних відносин, яким завдається шкода, внаслідок впливу на інформацію, що обертається у кібернетичних системах, тобто, внаслідок впливу на її предмет. Родовим (видовим) об'єктом комп'ютерних злочинів виступає інформація, яка звертається або зберігається в ЕОМ, системах ЕОМ, їх мережах або на машинних носіях. Безпосереднім об'єктом злочинів, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виступають відносини, що виникають у зв'язку із здійсненням інформаційних процесів.

Встановлено, що до предмету комп'ютерних злочинів віднесено комп'ютерну інформацію та комп'ютерні системи (під якими мається на увазі будь-яка із систем: ЕОМ (комп'ютер), автоматизована система, комп'ютерна мережа чи мережа електрозв'язку).

6. Здійснено аналіз та розкрито зміст об'єктивної сторони злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Проведено аналіз об'єктивної сторони злочинів, передбачених Розділом XVI КК України, що дозволило сформувати шість моделей злочинного посягання, які розкривають зміст об'єктивної сторони у цій сфері: 1) у випадках, коли наслідки спричинені діями особи, яка не мала права доступу до комп'ютерної інформації – такі дії мають ознаки несанкціонованого втручання в систему, зокрема, здійснені з порушенням порядку доступу до інформації або з подоланням засобів захисту інформації. За наявності необхідних ознак складу злочину такі дії доцільно кваліфікувати за ст. 361 КК України. Доступ до комп'ютерної інформації без подолання засобів захисту; дії, що призвели до наслідків, визначених у ст. 361 КК України, якщо їм не передувало несанкціоноване втручання в роботу засобів опрацювання інформації; ознайомлення з інформацією, яка обробляється в ЕОМ (комп'ютерах), АС, комп'ютерних мережах чи мережах електрозв'язку, без факту несанкціонованого втручання (ст. 361 КК України); 2) створення, розповсюдження і збут програмних засобів, не призначених для несанкціонованого втручання і шкідливі властивості яких можуть проявлятися без втручання в роботу ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку, у такому випадку йдеться про комп'ютерні віруси (ст. 361-1 КК України); 3) збут або розповсюдження інформації з обмеженим доступом, яку було створено з порушенням чинного законодавства; збут або розповсюдження інформації з обмеженим доступом, яку було отримано із захищеної комп'ютерної мережі шляхом подолання системи захисту, а на момент розповсюдження така інформація вже не захищалася спеціальними технічними засобами, наприклад, незаконне розповсюдження електронних баз персональних даних (ст. 361-2 КК України); 4) перехоплення інформації під час її передачі мережами електрозв'язку; незаконне введення інформації до ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку (ст. 362 КК України). Якщо наслідки спричинені діями особи, яка мала право доступу до комп'ютерної інформації, але не мала права вчиняти з нею певних дій – змінювати, знищувати, блокувати, перехоплювати або копіювати, то такі дії слід кваліфікувати за ст. 362 КК України. Враховуючи зміст частини 2 статті 362 Кримінального кодексу України, пропонується виключити поняття «перехоплення», у зв'язку з відсутністю доступу суб'єкта до охоронюваної законом інформації; 5) якщо наслідки спричинені діями (бездіяльністю) особи, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку і такі діяння вчинено з порушенням правил експлуатації або порядку чи правил захисту інформації, яка в них оброблюється, таке діяння повинно отримати кримінально-правову оцінку за ст. 363 КК України; 6) якщо наслідки спричинені будь-якою особою шляхом масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів, такі дії кваліфікуються за ст. 363-1 КК України.

7. Встановлено, що суб'єкт злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є загальним (особи, які не мають права доступу до комп'ютерної інформації). Про спеціальний суб'єкт йшлося у випадках, коли особа має право доступу до інформації (ст. 362 КК України); особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

(ст. 363 КК України). Звернено увагу на те, що особливим суб'єктом кібернетичних злочинів виступає хакер.

За віковою категорією суб'єктів комп'ютерних злочинів згруповано таким чином: 1. Загальний суб'єкт – фізична осудна особа, яка досягла шістнадцятирічного віку (ст. 361, 361-1, 361-2, 363-1 КК України); 2. Особа, яка має право доступу до інформації, що обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах, або зберігається на носіях такої інформації (ст. 362 КК України); 3. Особа, що відповідає за експлуатацію ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку (ст. 363 КК України).

8. Досліджено особливості суб'єктивної сторони злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, на підставі чого сформовані такі групи: 1. Злочини, що мають прямий умисел (ч. 1 ст. 361, ст. 362 та 363-1 КК України); 2. Злочини, які мають подвійну форму вини (умисел та необережність) (ч. ст. 361, 361-1, 361-2, 363 КК України). Кваліфікуючими ознаками злочинів, передбачених Розділом XVI Кримінального кодексу України (ч.2 ст. 361, ч.2 ст. 361-1 КК, ч. 2 ст. 361-2 КК, ч. 2 ст. 362 КК України) є їх вчинення: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ними істотної шкоди.

Відмічено, що застосування статті 361-1 КК України можливе лише за умови встановлення, що винний знав про шкідливість програм. Враховуючи, що у «формальних» складах, де є характеристика інтелектуального моменту умислу, умисел може бути тільки прямим, – запропоновано доповнити існуючі форми вини – злочинною необачністю, яка б включала у себе ознаки непрямого умислу та злочинної самовпевненості (легковажності).

Інтелектуальний момент прямого умислу при поводженні із шкідливими програмами може бути визначено як такий стан свідомості винного, коли він знав, чи допускав з високим ступенем ймовірності, що дані програми призначені для несанкціонованого знищення, блокування, модифікації або копіювання комп'ютерної інформації, порушення роботи ЕОМ, системи ЕОМ або їх мереж.

9. На основі проведених досліджень здійснено спробу удосконалити кримінально-правову кваліфікацію злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Виявлено найбільш проблемні питання у проведенні кримінально-правової кваліфікації кібернетичних злочинів та розроблено наступні заходи, спрямовані на їх вирішення:

– використання особистих даних зі злочинними намірами, наприклад, злам баз даних, внаслідок чого здійснено копіювання особистої інформації клієнтів банку, що може призвести до більш тяжких наслідків. Запропоновано введення статті 361-3 КК України «Неправомірне копіювання інформації з обмежених доступом, яка зберігається на електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації».

– розвиток інформаційних технологій зумовив появу нових злочинних діянь, які на сьогодні відсутні у Кримінальному кодексі України. Проте враховуючи відсутність протиправних діянь у законодавстві притягнення до відповідальності

особи неможливо. Запропоновано доповнити норми Розділу XVI КК України найбільш розповсюдженими видами міжнародних злочинів.

– вчинення кібернетичних злочинів за допомогою комп'ютерів (ЕОМ) у мережі «Інтернет». Проблему становить невизначеність застосування законодавчого регулювання, подекуди місцем вчинення злочину і місцем настання суспільно-небезпечних наслідків є різні країни. Обґрунтовано надання правовому режиму мережі Інтернет статус, подібний до статусу територій загального користування.

– при здійсненні кримінально-правової кваліфікації необхідно подолати конкуренцію правових норм злочинів, передбачених Розділом XVI та іншими розділами КК України. У випадках, коли складом певного злочину охоплюється вчинене одночасно з цим злочином діяння, передбачене статтею Розділу XVI КК України, і санкцією статті Особливої частини КК України встановлене за цей злочин більш суворе основне покарання, ніж за діяння, передбачене статтею Розділу XVI Особливої частини КК України, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує. Не буде сукупності злочинів у тих випадках, коли вчинені діяння передбачені різними пунктами однієї статті, якщо ці пункти не мають власних санкцій. Якщо суспільна небезпечність відносин, що охороняються додатковим об'єктом, є більшою, ніж основного об'єкта, то діяння утворюватиме ідеальну сукупність. Якщо вчинене є посяганням на різні безпосередні об'єкти кримінально-правової охорони, то діяння необхідно кваліфікувати за правилами сукупності злочинів.

– невирішеним залишається доля потерпілих від кіберзлочинів. Застосування покарання націлене на попередження вчинення злочинів, з введенням інституту кримінальних правопорушень внесено корективи у Розділ XVI КК України – збільшено обсяги грошових стягнень. Проте штраф у більшості випадках не застосовується, або ж застосовується, кошти від якого надходять до державного бюджету. Компенсація жертві можлива за умови подання нею цивільного позову, проте це поодинокі випадки. Здебільшого потерпілий у найкращому випадку отримує лише моральні здобутки. Саме тому запропоновано запровадити інститут відшкодування шкоди до кібернетичних злочинів з метою матеріальної компенсації порушених прав потерпілих. У разі відсутності необхідної суми запропоновано застосовувати громадські роботи, кошти від яких перераховуватимуться на рахунок потерпілих.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ричка Д. О. Комп'ютерні віруси - шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету*. Серія: «Юридичні науки». Херсон, 2018. Вип. 1. Том 2. С. 89-93.

2. Ричка Д. О. Транснаціональна злочинність новітніх комп'ютерних технологій. *Науково-виробничий журнал «Держава та регіони. Серія : Право»,* Класичний приватний університет. Запоріжжя, 2018. № 1 (59). С. 133–138.

3. Ричка Д. О. Модель комп'ютерних злочинців. *«Науковий вісник Ужгородського національного університету. Серія : «Право»*. Ужгород, 2018. № 49. Том 2. С. 122–125.

4. Ричка Д. О. Прояви організованої злочинності у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку. *Науковий збірник «Актуальні проблеми вітчизняної юриспруденції»*. № 5. Дніпро, 2018. С. 126–130.

5. Rychka D. O. Types of crime in information and telecommunication systems. Cybersquatting (cybercrime). *Международный научно-практический журнал «Право и закон»*. 2018. № 3. С. 117–121.

6. Ричка Д. О. Історичні аспекти кіберзлочинності. Матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених *«Сучасний стан і перспективи розвитку держави і права»* (м. Дніпропетровськ, 04-05 грудня 2015 року). Дніпропетровськ, 2015. С. 293-295.

7. Ричка Д. О. Передумови виникнення злочинів у сфері використання електронно-обчислювальних машин. Матеріали IX Міжнародної наукової конференції студентів, аспірантів та молодих вчених *«Сучасний стан і перспективи розвитку держави і права»* (м. Дніпро, 01-02 грудня 2017 року). Дніпро, 2017. С. 267-268.

8. Ричка Д. О. Тенденції розвитку криптовалюти на території України. Матеріали II Всеукраїнської науково-практичної конференції *«Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності»* (м. Хмельницький, 02 березня 2018 року). Хмельницький : Вид-во НАДПСУ, 2018. С. 520-522.

9. Ричка Д. О. Комп'ютерна фобія. Матеріали Всеукраїнської наукової інтернет-конференції *«Вітчизняна наука на зламі епох: проблеми та перспективи розвитку»* (м. Переяслав-Хмельницький, 16 березня 2018 року). Переяслав-Хмельницький, 2018. Вип.41. С. 87-88.

АНОТАЦІЯ

Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. – *Рукопис.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. – Університет державної фіскальної служби України, Ірпінь, 2019.

Дисертацію присвячено розкриттю особливостей кримінально-правової кваліфікації у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено засади здійснення кримінально-правової кваліфікації. Окреслено ознаки, притаманні даній категорії злочинної діяльності. Визначено ознаки кібернетичних злочинів. Висвітлено ґенезу та поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Досліджено різновиди як міжнародних, так і національних кібернетичних злочинів. Проведено комплексний аналіз елементів складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено об'єкт і предмет

кібернетичних злочинів, здійснено аналіз та розкрито зміст об'єктивної сторони; встановлено суб'єктів та досліджено особливості суб'єктивної сторони злочинів даної категорії. Розглянуто кваліфікуючі ознаки та здійснено їх відмежування від суміжних складів, на підставі чого сформовано нововведення та доповнення до чинного законодавства України з питань здійснення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Ключові слова: кіберзлочини, кіберпростір, транснаціональна кіберзлочинність, інформаційний простір, хакер, шкідливі технічні засоби, модель комп'ютерних злочинців, організована комп'ютерна злочинність, віртуальні банди, комп'терне підпілля.

АННОТАЦИЯ

Рычка Д.О. Особенности уголовно-правовой квалификации преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, и сетей электросвязи. –Рукопись.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. – Университет государственной фискальной службы Украины, Ирпень, 2019.

Диссертацию посвящено раскрытию особенностей уголовно-правовой квалификации в сфере использования электронно-вычислительных машин (компьютеров), систем, и компьютерных сетей и сетей электросвязи. Определены принципы проведения уголовно-правовой квалификации. Описаны признаки, присущие данной категории преступной деятельности.

Освещены общетеоретические аспекты уголовно-правовой квалификации преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. Установлено, что уголовно-правовая квалификация указанных преступлений выступает инструментом реализации законности в уголовном производстве.

Доказано, что термин «уголовно-правовая квалификация» является шире понятия «квалификация преступлений», последнее выступает его составной частью, поэтому к процессу исследования входят преступления и деяния, признаваемые незначительными, или совершенные при обстоятельствах, исключающих преступность деяния.

Определены элементы кибернетических преступлений. Описано исторические предпосылки и понятие преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. Исследованы как международные, так и национальные кибернетические преступления.

Проведен комплексный анализ элементов состава преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. Определены объект и предмет кибернетических преступлений, осуществлен анализ и раскрыто содержание объективной стороны; установлен субъект и исследованы особенности субъективной стороны преступлений данной категории.

Рассмотрены квалифицирующие признаки и осуществлено их разграничение от смежных составов, на основании чего сформированы нововведения и уточнения в действующему законодательству Украины по вопросам проведения уголовно-правовой квалификации преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи.

Ключевые слова: киберпреступления, киберпространство, транснациональная киберпреступность, информационное пространство, хакер, вредные технические способы, модель компьютерных преступников, організованная компьютерная преступность, вертуальные банды, компьютерное подполье.

SUMMARY

Rychka D.O. Peculiarities of the criminal-law qualification of crimes in the sphere of the use of electronic computers (computers), systems and computer networks and telecommunication networks. – *The manuscript.*

The dissertation for obtaining the degree of Candidate of Law Sciences, Specialty 12.00.08 – Criminal Law and Criminology; Criminal and Executive Law. – University of the State Fiscal Service of Ukraine, Irpin, 2019.

The dissertation is devoted to the disclosure of peculiarities of criminal-law qualification in the sphere of the use of electronic computing machines (computers), systems, and computer networks and telecommunication networks. The principles of conducting criminal-law qualification are determined. Characteristics inherent in this category of criminal activity are described. Elements of cyber crimes are defined. The historical preconditions and the concept of crimes in the sphere of the use of electronic computing machines (computers), systems and computer networks and telecommunication networks are described. Both international and national cybercrime crimes were investigated. A complex analysis of the elements of the crimes in the sphere of the use of electronic computers (computers), systems and computer networks and telecommunication networks has been carried out. The object and object of cybernetic crimes were determined, the analysis and the content of the objective side were revealed; the subject is established and the features of the subjective part of the crimes of this category are investigated. Qualifying attributes are considered and their distinction from adjacent compositions is carried out, on the basis of which new innovations and clarifications in the current legislation of Ukraine on the issues of criminal-law qualification of crimes in the sphere of the use of electronic computing machines (computers), systems and computer networks and telecommunication networks are formed.

Key words: cybercrime, cyberspace, transnational cybercrime, information space, hacker, harmful technical means, computer criminals model, organized crime, virtual gangs, computer underground.

Підписано до друку 26.04.2019. Формат 60×84/16.
Папір офсетний. Друк офсетний.
Друк. арк. 0,9. Тираж 100 прим.
Замов. № 328.

Видруковано в Університеті державної фіскальної служби України.
08205, Київської обл., м. Ірпінь, вул. Університетська, 31