МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ОЛЕСЯ ГОНЧАРА
УНІВЕРСИТЕТ ДЕРЖАВНОЇ ФІСКАЛЬНОЇ СЛУЖБИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

РИЧКА ДЕНИС ОЛЕГОВИЧ

УДК 343.3/.7:004.056.5](477)

ДИСЕРТАЦІЯ
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»

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____Д.О. Ричка

Науковий керівник: **Корнякова Тетяна Всеволодівна**,
доктор юридичних наук, професор,
заслуженный юрист України.

Ірпінь – 2019

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. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. – Дніпровський національний університет імені Олеся Гончара, Дніпро; 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 проведення кримінально-правової кваліфікації. Окреслено ознаки, притаманні даній категорії злочинної діяльності. Визначено елементи 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'єкта 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 уточненя до чинного законодавства України.

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.

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. – *Qualification scientific work on the rights of manuscripts.*

The dissertation for obtaining the degree of Candidate of Law Sciences, Specialty 12.00.08 - Criminal Law and Criminology; Criminal and Executive Law. – Oles Honchar Dnipro National University, Dnipro; 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.

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. С. 133-138.

3. Ричка Д.О. Модель комп'ютерних злочинців. *«Науковий вісник Ужгородського національного університету.* Серія : «Право». Ужгород, 2018. 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. 101–105.

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»*. 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»*. 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»*. 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»*. Переяслав-Хмельницький, 2018. Вип.41. С. 87-88.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Забезпечення інформаційної безпеки вУкраїні 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 використаннях електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку.

Внаслідок 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 у сфері економіки.

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.

---

[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)

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 машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» особливої частини Кримінального кодексу 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 створено 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, грантами. 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, Стратегієї 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 завдання 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 *завдання*:

– 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

Кримінального кодексу України (далі 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 Кримінального кодексу 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 Кримінального кодексу 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 Кримінального кодексу 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 Кримінального кодексу України доповненням: «... наявність в особи права доступу до інформації та реалізації такої можливості зі злочинним наміром»;

– частину 2 статті 362 Кримінального кодексу 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 Кримінального кодексу 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, 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 у науково-дослідну роботу 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 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.

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

1.1 Загальні засади кримінально-правової кваліфікації

Кримінально-правова кваліфікація злочинів є одним з ключових етапів застосування норм кримінального права. Вірна кваліфікація забезпечує реалізацію конституційного принципу законності у кримінальному судочинстві (ст. 129 Конституції) [70, ст. 129], гарантує охорону й здійснення прав і свобод людини і громадянина, виступає необхідною умовою призначення справедливого покарання (чи звільнення від кримінальної відповідальності або від покарання).

Зареєстрований масив злочинних посягань у аналізованій сфері має наступні 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 «Додаток **А**» [52].

З метою комплексного дооослідження засад кримінально-правової кваліфікації злочинів пропонуємо розглянути кваліфікацію злочинів.

Визначення "кваліфікація злочинів" є вужчим за обсягом, навідміну від кримінально-правової кваліфікації, у зв'язку з чим воно охоплюється родовим поняттям — «кримінально-правова кваліфікація» і є лише його частиною. У той час, як під кримінально-правовою кваліфікацією розуміється не лише кваліфікація злочинів, а й кваліфікація інших діянь, які можуть і не бути злочинами (малозначних діянь; діянь, вчинених за обставин, що виключають злочинність діяння, тощо) .

Термін «кваліфікація злочинів» походить від латинських слів – «quails» (якість, який за якістю) та «facio» (роблю) [2, с. 15] та використовується як у кримінальному (статті 9, 29, 33, 35, 66, 67 Кримінального кодексу України (далі — КК), так і у кримінальному процесуальному законодавстві (п. 5 ч. 5 ст. 214, п. 5 ч. 1

ст. 277, п. 5 ч. 2 ст. 291 та ін. Кримінального процесуального кодексу України (далі — КПК).

У теорії і практиці кримінального права поняття «кваліфікація злочинів» визначають по-різному: як встановлення тотожності ознак вчиненого суспільно небезпечного діяння і ознак кримінально-правової норми, що передбачає відповідальність за це діяння [103, с. 46]; як кримінально-правову оцінку вчиненого суспільно небезпечного діяння [98, с. 6-44]; як встановлення і юридичне закріплення точної відповідності ознак вчиненого діяння і ознак складу злочину, передбаченого кримінально-правовою нормою [83; 86; 84; 38].

Кваліфікація злочинів має декілька різновидів, у широкому значенні кваліфікація злочинів — це:

1) "результат кримінально-правової оцінки діяння органами дізнання, досудового розслідування, прокуратури і суду внаслідок чого констатовано, що скоєне є саме злочином, визначена норма(и) кримінального закону, яка(і) передбачає(ють) відповідальність за вчинене, встановлена відповідність між юридично значущими ознаками посягання і ознаками злочину, передбаченими законом, та процесуально закріплений висновок про наявність такої відповідності" (проф. В. Навроцький) [98, с. 54; 175, с. 32];

2) "кримінально-правова оцінка вчиненого діяння, вибір і застосування до нього тієї кримінально-правової норми, яка у повній мірі описуватиме його ознаки" (проф. М. Коржанський) [72, с. 16].

За вченим П.В. Хряпінським кваліфікація злочинів є видом кримінально-правової кваліфікації, під час проведення якої відбувається встановлення відповідності фактичних ознак посягання всім ознакам злочину, передбаченого статтею Кримінального кодексу України (далі – КК України), що містить забороняючу кримінально-правову норму. З метою розкриття сутності, змісту та структури кримінально-правової діяльності необхідно розглянути і встановити її підстави, логіко-гносеологічні засади (аспекти) та етапи її здійснення, здійснити розмежування складів злочинів, як необхідної умови правильної кваліфікації злочинів [175, с. 32].

За загальним правилом кваліфікація злочинів складається з таких дій:

Проводячи кримінально-правову кваліфікацію злочинів, виходячи з обставин за яких їх було вчинено підбирають норми за якими передбачається відповідальність за скоєне. Наводиться попередній висновок про наявність злочинного діяння, а не адміністративного проступку, цивільного делікту, дисциплінарного проступку чи іншого правопорушення. Висувається припущення про застосування певних кримінально-правових норм та констатують, що скоєне не підпадає під ознаки інших кримінально-правових норм. Це початковий етап кримінально-правової кваліфікації;

Після цього відбувається встановлення відповідності між фактичними ознаками вчиненого посягання та ознаками складу злочину, передбаченими кримінальним законодавством. Важливо аби доказова база була зібрана законним процесуальним шляхом, адже тільки у такому разі вона матиме статус законно отриманих доказів. Після цього з кримінально-правової норми, яку обрано для юридичної оцінки вчиненого, виділяють ознаки, що характеризують вчинене посягання, і за наявності кількох альтернативних ознак обирають ознаки, характерні для посягання, що підлягає кваліфікації. У цьому процесі використовують конструкцію складу злочину, чому присвячено наступну главу наукової роботи [105].

Наступним кроком є закріплення результатів кваліфікації, воно відбувається в процесуальних документах та включає у себе щонайменше три дії:

1) виклад фактичних обставин справи;

2) складання формули кваліфікації;

3) виклад формулювання обвинувачення.

Виклад фактичних обставин по справі полягає у формулюванні фактичного складу діяння. Для цього з встановлених у справі фактичних даних обирають ті, які мають найбільше значення, вони враховуються при її вирішенні й виступають фактичною підставою застосування правової норми [105].

Кваліфікація злочинів пов’язана з необхідністю обов’язкового встановлення і доказування кримінально-процесуальними і криміналістичними засобами двох важливих обставин:

1) факту вчинення особою (суб’єктом злочину) суспільно небезпечного діяння, тобто конкретного акту її поведінки (вчинку) у формі дії чи бездіяльності;

2) відповідності ознак діяння ознакам передбачуваного складу злочину.

Вищеперелічені обставини є підставами кваліфікації, тобто за їх наявності доцільно проводити кваліфікацію злочинних діянь, адже «підстава» означає «те головне, на чому базується, основується що-небудь» [24, с. 782]. Це дозволяє дійти до думки, що підстави кримінально-правової кваліфікації — це ті об’єктивні обставини, які лежать в основі визнання вчиненого суспільно небезпечного діяння певним злочином з одночасною констатацією відповідної норми кримінального закону (його статті чи частини статті), яка визначає таке діяння забороненим і яку було порушено внаслідок вчинення цим діяння [7, с. 8-9].

Виходячи з визначення і змісту поняття «кваліфікація злочинів», підстави кваліфікації в юридичній літературі поділяють на два види: «фактичну підставу» і «юридичну (нормативно-правову) підставу».

Фактичною підставою кримінально-правової кваліфікації злочинів-наявність факту вчинення особою суспільно-небезпечного діяння, яке виступає об'єктом кваліфікації з точки зору визнання (невизнання) його злочином. До того ж, фактичні підстави знаходиться у тісному співвідношенні з обставинами, що підлягають доказуванню у кримінальному провадженні (предмет доказування). Ними, згідно з ч. 1 ст. 91 КПК, зокрема, є:

1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою для закриття кримінального провадження;

5) обставини, які є підставами для звільнення від кримінальної відповідальності або покарання;

6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру [79, ст. 91].

Наприклад, перебуваючи у магазині по вул. Грушевського, 46 в м. Рівне Микола Петрович, здійснюючи злочинний умисел, направлений на неправомірний доступ до захищеної інформації ВАТ, діючи без дозволу товариства, здійснив несанкціоноване втручання в роботу автоматизованих систем зазначеного товариства, а саме за допомогою супутникового ресивера, виконав його налаштування для підключення до віддаленого серверу, встановивши IP-адресу «», користувача «», пароль «», протокол обміну даними «», систему «» та «», що призвело до витоку вище вказаної інформації та порушення встановленого порядку її маршрутизації та дозволило здійснювати перегляд закодованих каналів телебачення, використовуючи мережу Інтернет.

Зазначені дії, на нашу думку, підпадають під ознаки злочину, передбаченого ч.1 ст.361 КК України (етап складання формули кваліфікації).

Виклад формулювання обвинувачення матиме наступне вираження — визнати Миколу Петровича винуватим та призначити покарання : за ч.1 ст.361 КК України - у виді двох років позбавлення волі з конфіскацією технічних засобів, а саме двох супутникових ресиверів.

Під кримінально-правовою кваліфікацією розуміють:

- оцінку скоєного, з точки зору держави, тобто не лише юридичну, а й суспільно-політичну оцінку посягання, як злочину;
- логічну діяльність із встановлення відповідності (тотожності) між фактичними і юридичними ознаками посягання, дихотомічного поділу родового поняття кримінально-правової кваліфікації. Такий поділ завжди:

1) співрозмірний (сума обсягів видових понять рівна обсягу поділеного родового поняття);

2) члени поділу виключають один одного (не мають спільних елементів, не перетинаються);

3) поділ є безперервним;

4) поділ здійснюється лише за однією підставою [98, с. 8].

Кримінально-правова кваліфікація охоплює кваліфікація злочинів та кваліфікацію не-злочинів [98, с. 9-10; 175, с. 32]. За вченням В.О. Навроцького кримінально-правова кваліфікація має внутрішню будову, яка складається з певних елементів, структуру якої утворюють її об’єкт, суб’єкт та зміст. Відповідно до вчення об’єктом кримінально-правової кваліфікації є оцінка вчиненого діяння з позиції кримінального закону. Об’єктом кваліфікації виступають діяння, за попередньою кваліфікацією, внаслідок об'єктивних обставин підпадають під ознаки злочину. Адже кримінально-правовій оцінці піддаються не тільки злочинні посягання, а й інші діяння, які чимось схожі із злочинами.

На думку вченого В.О. Навроцького до кола уваги органів, які здійснюють кваліфікацію, діяння, які «схожі із злочинами», входять, тому що вони можуть бути формально передбаченими кримінальним законом; виступати об’єктивно суспільно-небезпечними у зв’язку із заподіянням істотної шкоди правоохоронюваним

інтересам; характеризуватися умислом на заподіяння великої шкоди; вчинятися з мотивом чи метою, які характерні для злочинів [98, с. 8].

Якщо об'єктом кваліфікації можливо назвати діяння, що підлягає кримінально-правовій оцінці, то об'єктом кримінально-правової кваліфікації слід вважати вчинене особою діяння, ознаки якого (об'єктивні та суб'єктивні) мають подібність, схожість (формально співпадають) з ознаками діяння, склад якого визначено законодавцем у статті (частині статті чи її пункті) Особливої частини КК України — злочином.

Кримінально-правова кваліфікація повинна даватись з позиції:

1) визнання діяння таким, що фактично містить передбачений відповідною статтею (частиною статті чи її пунктом) склад злочину;

2) визнання діяння таким, що лише формально містить склад злочину — його ознаки співпадають з ознаками складу злочину, передбаченого відповідною статтею (її частиною чи пунктом) Особливої частини КК, - але яке з підстав, передбачених законом, не є злочином внаслідок відсутності однієї із ознак злочину, зазначених у ч. 1 ст. 11 КК: або воно не є суспільно небезпечним через малозначність (ч. 2 ст. 11 КК), або ж не є суспільно небезпечним та/ або протиправним, оскільки містить склад правомірного діяння, яке визнається однією із обставин, що виключають злочинність діяння. Позиція професора П.П. Андрушко, щодо кваліфікації діяння, як злочину співпадає з наведеною позицією В.О. Навроцького, що про кримінально-правову кваліфікацію (оцінку) діяння як злочину можна вести мову, «коли процес кваліфікації вже завершено» [6, с. 150]. Завершується ж процес кваліфікації винесенням процесуального акту суду (обвинувального вироку чи постанови (ухвали) про звільнення від кримінальної відповідальності з підстав, передбачених нормами Загальної чи Особливої частини КК).

Розподіл кримінально-правової кваліфікації на види може здійснюється за досить різними критеріями:

1) за суб'єктами, які її здійснюють, виділяють офіційну і неофіційну або доктринальну кваліфікацію;

2) за інститутами Загальної частини, які використовуються при кваліфікації, виділяють:

а) кваліфікацію закінченого і незакінченого складу злочину;

б) кваліфікацію співучасті у злочині;

в) кваліфікацію множинності злочинів;

3) за об'єктом кваліфікації виділяють:

а) кваліфікацію злочинів;

б) кваліфікацію діянь, які визнаються обставинами, що виключають злочинність діяння;

в) кваліфікацію посткримінальної поведінки.

Кваліфікація злочинів може проводитися за різними критеріями, зокрема, С.Д. Шапченко виділяє такі різновиди кваліфікації злочинів:

1) кваліфікація злочинів, як специфічна оціночно-пізнавальна діяльність людини;

2) кваліфікація злочинів, як юридично значуща дія;

3) кваліфікація злочинів, як юридична дія суб'єкта, уповноваженого на її проведення;

4) кваліфікація злочинів, як юридична дія уповноваженого суб'єкта, що має кримінально-процесуальний характер;

5) кваліфікація злочинів, як юридична дія уповноваженого суб'єкта, що має кримінально-правовий характер [179, с. 421].

Проводячи поділ кваліфікації злочинів на види, доцільно керуватися класифікаціями видів злочинів, які містяться у кримінальному законі, враховувати особливості кваліфікації окремих видів злочинів, відображених у нормах чинного кримінального законодавства [7, с. 11-16, 26].

Одним з найбільш розповсюджених видів класифікації кваліфікації злочинів виступає розподіл за суб'єктами, які її здійснюють на неофіційну та офіційну кваліфікацію. Неофіційна кваліфікація є відповідною правовою оцінкою, що дається науковцями у наукових статтях, монографіях, навчальних посібниках тощо. Така кваліфікація не має обов'язкового характеру, адже вона відображає лише позицію

автора, але може враховуватись суб'єктами офіційної кваліфікації. Офіційна, її ще називають легальною, юридичною є кваліфікація, що здійснюється у кримінальних справах уповноваженими на те державними особами. Результати такої кваліфікації закріплюються в процесуальних документах (постановах, ухвалах, вироках) і мають обов'язковий характер. Офіційна кваліфікація розглядається, як визначення певним суб'єктом правового змісту окремої фактичної ситуації [76].

Зміст офіційної кваліфікації розкривають її наступні характеристики:

1) юридична кваліфікація — це перш за все процес розумової діяльності суб'єкта, різновид оціночно-пізнавальної діяльності людини [83, с. 7-8];

2) кінцевий етап зазначеної діяльності призводить до конкретного результату, який завжди формалізується і, тим самим, відокремлюється суб'єктом від власне діяльності (при цьому він, як правило, ще й певним чином об'єктивізується — проголошується, викладається в письмовій формі тощо); у такому вигляді зазначений результат стає поряд з діяльністю відносно самостійним компонентом юридичної кваліфікації [180, с. 135];

3) як специфічний різновид оціночно-пізнавальної діяльності юридична кваліфікація має певний філософський, логічний, психологічний та власне правовий (юридичний) зміст [180, с. 196-226; 103, с. 69-103];

4) оціночно-пізнавальна складова (компонент) юридичної кваліфікації — це перш за все різновид розумової діяльності, що відбувається в межах людської свідомості; виходячи з цього первинний предмет юридичної кваліфікації — фактичні обставини з відповідним об'єктивним («реальним») змістом — трансформується у відображену в свідомості суб'єкта («ідеальну») інформаційно-оціночну модель цих обставин; саме така модель і є безпосереднім предметом юридичної кваліфікації; при цьому в якості первинних стандартів (орієнтирів) оцінки такої моделі виступають певні «фрагменти правової матерії» (нормативні приписи, правові принципи, нормативні юридичні конструкції тощо); однак, будучи «перенесені» у сферу свідомості (правосвідомості), вони також набувають форми певних «ідеальних» моделей і саме такі похідні моделі виступають безпосередніми

орієнтирами визначення правового змісту інформаційно-оціночної моделі фактичних обставин;

5) у найбільш загальному вигляді специфічний правовий зміст юридичної кваліфікації утворюють окремі етапи процесу розумової (оціночно-пізнавальної) діяльності людини (суб'єкта кваліфікації) та формалізація результатів.

6) окремими етапами процесу оціночно-пізнавальної діяльності суб'єкта кваліфікації є:

а) зіставлення інформаційно-оціночної моделі фактичних обставин з моделями відповідних правових орієнтирів;

б) вибір правових орієнтирів, які, на думку суб'єкта, найбільш повно, точно і конкретно визначають правовий зміст зазначеної моделі;

в) формулювання конкретного висновку, щодо правового змісту окремої фактичної ситуації (даний висновок стає згаданим вище результатом оціночно-пізнавальної діяльності суб'єкта);

7) формалізація зробленого на завершальному етапі висновку щодо правового змісту окремої фактичної ситуації передбачає його виклад у певній формі (кількох формах); при цьому дотримання такої форми (форм) в більшості випадках пов'язано з виконанням відповідних техніко-юридичних правил [180, с. 135].

Правового значення юридична кваліфікація набуває тоді, коли її складові пов'язані з реалізацією певних правовідносин. В цьому разі вона стає правовою (юридично значущою) дією, що включається до відповідної форми реалізації права.

Специфіка «механізму» юридичної кваліфікації проявляється у наступних особливостях:

а) «створення» інформаційно-оціночної моделі фактичних обставин не входить до змісту юридичної кваліфікації, а є лише необхідною її передумовою [99, с. 175-176]; в окремих випадках таку модель «створює» один суб'єкт, а здійснює юридичну кваліфікацію — інший;

б) розумова діяльність суб'єкта юридичної кваліфікації в межах окремих етапів відбувається в певних логічних формах, що «представляють» оціночно-пізнавальну природу такої діяльності; основними логічними формами процесу

юридичної кваліфікації є відповідні форми традиційної формальної логіки, в тому числі таких її розділів, як логіка оцінок і логіка норм; водночас специфічний характер правових орієнтирів обумовлює необхідність використання особливих підходів так званої юридичної логіки, які в ряді випадків мають пріоритет перед окремими формами традиційної формальної логіки;

в) в процесі юридичної кваліфікації на першому етапі зіставляються її безпосередній предмет та безпосередні (похідні) правові орієнтири (по суті, відповідні «ідеальні» моделі), а на останньому формулюється правовий зміст первинного предмета юридичної кваліфікації на підставі первинних правових орієнтирів; такий зміст фіксується і в межах формалізації висновку, зробленого на цьому етапі суб'єктом юридичної кваліфікації [180, с. 135].

Окремі вчені, як різновид кримінально-правової кваліфікації (кваліфікації злочинів) виділяють кваліфікацію посткримінальної поведінки. Ю.В. Баулін під кримінально-правовою кваліфікацією розуміє кваліфікацію тільки тих юридичних фактів, які передбачені гіпотезами норм кримінального права, і, залежно від того, який саме з юридичних фактів, що передбачені гіпотезою норми кримінального права, підлягає кваліфікації, виділяє два види кримінально-правової кваліфікації: кваліфікацію злочинів та кваліфікацію посткримінальних юридичних фактів. При цьому Ю.В. Баулін зазначає, що і той і інший вид кримінально-правової кваліфікації здійснюється виключно на досудовому слідстві органами, які його проводять — слідчим або прокурором. Коли йдеться про застосування нетипових (альтернативних) норм, то застосування їх гіпотез зумовлює кримінально-правову кваліфікацію двох юридичних фактів — власне самого злочину, а також посткримінального юридичного факту, з наявністю якого (зокрема, її диспозиція) і пов'язує можливість повного або часткового звільнення від кримінальної відповідальності [11, с. 414]. Системний аналіз кримінально-правових положень кримінального закону України, в яких йдеться про його застосування, приводить до висновку про те, що шляхом застосування норм кримінального права визначаються, по-перше, злочинність діяння; по-друге — кримінальна відповідальність за його вчинення» [11, с. 408].

Кваліфікація посткримінальної поведінки особи, яка вчинила злочин, впливає на застосування окремих інститутів кримінального права. Прикладом такої кваліфікації є урахування (оцінка) судом поведінки засудженого (як сумлінної чи несумлінної) та його ставлення до праці, які в сукупності свідчать про його виправлення, яке є підставою застосування до нього умовно-дострокового звільнення від покарання. Суд повинен давати кримінально-правову оцінку посткримінальної поведінки особи для врахування її як обставини, що пом'якшує покарання:

1) з'явлення із зізнанням, щире каяття або активне сприяння розкриттю злочину (п. 1 ч. 1 ст. 66 КК);

2) добровільне відшкодування завданого збитку або усунення заподіяної шкоди (п. 2 ч. 1 ст. 66 КК) і т.д. [6].

За наявності таких обставин суд на підставі ч. 1 ст. 69 КК може призначити основне покарання нижче від найнижчої межі або перейти до іншого, більш м'якого виду покарання, а за наявності обставин, передбачених пунктами 1 та 2 ч. 1 ст.66 КК, за відсутності обставин, що обтяжують покарання, а також при визнанні підсудним своєї вини, строк або розмір покарання не може перевищувати, згідно зі ст. 691 КК, двох третин максимального строку або розміру найбільш суворого виду покарання, передбаченого відповідною санкцією статті (санкцією частини статті) Особливої частини КК.

За вченим Ю.В. Бауліним «кримінально-правова кваліфікація» в широкому розумінні є оцінкою певної поведінки особи (вчиненого нею діяння та посткримінальної поведінки) при застосуванні кримінально-правових норм, яка (поведінка) є юридичним фактом, що має кримінально-правове значення. В.О. Навроцький звертає увагу на місце посткримінальної поведінки у кваліфікації, зазначаючи, що в цілому ряді випадків посткримінальна поведінка сама підлягає кримінально-правовій кваліфікації, яка тягне для особи, дії якої кваліфікуються, як позитивні, так і негативні наслідки [99, с. 175-176]. Таким чином, у багатьох випадках поведінка особи після вчинення нею злочину (посткримінальна поведінка)

повинна діставати оцінку з позиції кримінального закону, оскільки її характер і зміст можуть тягнути за собою певні кримінально-правові наслідки.

Складовими частинами кримінально-правової кваліфікації є:

1) кримінально-правова кваліфікація вчиненого, здійснювана органами дізнання і досудового слідства;

2) кримінально-правова кваліфікація, здійснювана судом — власне кваліфікація злочину;

3) кримінально-правова оцінка посткримінальної поведінки особи, яка вчинила злочин.

Таким чином, кримінально-правова кваліфікація є більш широким поняттям за кваліфікацію. Кримінально-правова кваліфікація містить у собі не тільки кваліфікацію злочинів, а й кваліфікацію інших діянь, які можуть навіть не бути злочинами. Це процес встановлення уповноваженими на те органами тотожності між юридично-значущими ознаками злочину (фактичний склад злочину) та ознаками злочинів, передбачених кримінальним кодексом України та встановленням між ними відповідності, певного зв'язку. Навіть несуттєві помилки у кваліфікації злочинів можуть призвести до помилок у призначенні покарання або у вирішенні інших питань що стосуються кримінальної відповідальності. Вірне визначення кваліфікації злочинів виступає, за своєю суттю, гарантом встановлення обґрунтованого, законного, справедливого рішення по суті справи.

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

Інформаційні простори торкаються практично кожної сфери людської життєдіяльності, а отже, і злочинність набуває нових, більш досконалих форм. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку являють серйозну загрозу

існуючим суспільним відносинам, адже стрімка інформатизація суспільства слугує, свого роду, активізатором нових форм злочинної поведінки.

Злочин є вчинком людини, тому йому притаманні всі ті об'єктивні і суб'єктивні особливості, що характеризують людську поведінку (фізичні властивості — той чи інший рух або його відсутність, використання фізичних, хімічних, біологічних та інших закономірностей навколишнього світу; психологічні властивості — прояв свідомості і волі, певна мотивація поведінки, її цілеспрямованість).

Злочин можна назвати посяганням на відносини, що відображають найважливіші інтереси, внаслідок чого охороняються законом про кримінальну відповідальність. Об'єктивні закономірності розвитку суспільства, його потреби та інтереси виступають мірилом цінності людської поведінки, її відповідності чи невідповідності цим потребам та інтересам, тому злочин завжди є антисоціальною поведінкою.

Як свідомий вольовий вчинок людини злочин повинен полягати у конкретній дії або бездіяльності. Думки, погляди, переконання, що не виразилися в актах дії або бездіяльності, хоч як би вони не суперечили інтересам суспільства, злочином визнаватися не можуть.

Аналіз ч. 1 ст. 11 КК вказує на три ознаки злочину:

1. Передбаченість у законі про кримінальну відповідальність;
2. Суспільна небезпечність діяння;
3. Винність.

Перша — передбаченість діяння КК — є формальною, що відображає його юридичну, нормативну природу, тобто протиправність. Інші дві ознаки — суспільна небезпечність та винність — є матеріальними, такими, що розкривають соціально-психологічну природу злочину. Аналіз ч. 2 ст. 1 КК, яка визначає завдання КК, дає змогу стверджувати, що передбаченість діяння в кримінальним кодексом України одночасно означає також його обов'язкову караність.

Таким чином, обов'язковими ознаками злочину є: суспільна небезпечність, винність, протиправність та караність. Виходячи з вищезазначеного, злочином

визнається суспільно небезпечне, винне, протиправне та кримінально каране діяння (дія або бездіяльність), вчинене суб'єктом злочину. Кожна з цих ознак злочину відображає його істотні властивості та має свій зміст [77].

Основоположною одиницею злочину, як факта (явища) реальної дійсності, є суспільно небезпечне діяння, яке є обов'язковим та визначальним елементом (ч. 1 ст. 11 КК) і тому, в першу чергу, має бути встановлено та доведено кримінально-процесуальними і криміналістичними засобами у кожному кримінальному провадженні [7, с. 10]. Суспільно небезпечне діяння є конкретним актом суспільно небезпечної (негативної, асоціальної) поведінки особи фізичної (суб'єкта злочину) у формі дії чи бездіяльності. Не випадково у ч. 1 ст. 11 КК злочином визнається: «передбачене кримінальним кодексом України суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом злочину».

Суспільна небезпечність, як ознака діяння полягає у тому, що воно заподіює істотну шкоду суспільним відносинам, охоронюваним кримінальним законом від злочинних посягань, або створює реальну загрозу її заподіяння. Особливе значення для визнання діяння суспільно небезпечним мають характер і цінність суспільних відносин, на які воно посягає, а також характер та тяжкість (розмір) шкоди, яка спричиняється дією чи бездіяльністю цим відносинам або створюється загроза її спричинення. Отже, шкода (шкідливість) притаманна суспільно небезпечному діянню, що визнається злочином, становить його соціальний зміст і сутність. Ще у 1764 р. Чезаре Беккаріа писав: «дійсним мірилом злочинів є шкода, що заподіюється ними суспільству» [12, с. 97].

Високий ступінь суспільної небезпеки злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку обумовлений наступними фактарами:

1. Інтенсивне запровадження інформаційних технологій і процесів, заснованих на використанні електронно-обчислювальних машин, у багатьох сферах людської діяльності;

2. Високий масштабний коефіцієнт зусиль злочинців у цій сфері;

3. Відносна доступність для широкого кола осіб спеціальних знань і техніки, необхідної для вчинення злочину [181, с. 165].

Наслідки діяння, як шкода (збиток), що заподіюється (чи може бути заподіяна) суспільним відносинам, можуть бути матеріальними (шкода, що має особистий (фізичний) або майновий характер) чи нематеріальними (шкода у політичній, організаційній, соціальній сферах).

Суспільна небезпечність, як матеріальна ознака злочину, полягає в тому, що діяння або заподіює шкоду відносинам, що охороняються кримінальним законом, або містить у собі реальну можливість заподіяння такої шкоди. Це об'єктивна властивість злочину, реальне порушення відносин, що склалися в суспільстві. Виникнення, зміна, втрата суспільної небезпечності діяння зумовлені об'єктивними закономірностями суспільного розвитку, нерозривним зв'язком з тими соціально-економічними процесами, що відбуваються у суспільстві. У ч. 1 ст. 11 КК суспільна небезпечність як обов'язкова ознака злочину тільки називається, її зміст закон не розкриває. Суспільна небезпечність діяння, як ознака злочину, оцінюється на двох рівнях:

1) законодавчому, коли законодавець криміналізує певне суспільно небезпечне діяння;

2) правозастосовному, коли орган дізнання, слідчий, прокурор, суддя оцінюють суспільну небезпечність злочину.

Тому суспільна небезпечність належить до оціночних понять. Критерієм оцінки суспільної небезпеки, її ступеня виступають об'єктивні й суб'єктивні ознаки злочину: об'єкт, на який посягає злочин, наслідки, спосіб вчинення злочину, форма вини, мотив, мета та ін. Тільки оцінка всієї їх сукупності може розкрити об'єктивну, реальну небезпечність злочину.

На нашу думку, 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.

Значення суспільної небезпечності як матеріальної ознаки злочину полягає в тому, що вона, по-перше, є основним об’єктивним критерієм визнання діяння злочином, його криміналізації; по-друге, дозволяє класифікувати злочини за ступенем тяжкості (ст. 12 КК); по-третє, визначає межу між злочином та іншими правопорушеннями; по-четверте, є однією із загальних засад індивідуалізації кримінальної відповідальності та покарання (п. 3 ч. 1 ст. 65 КК) [10, с. 74-75].

Тяжкість злочинів у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку законодавець оцінив таким чином: більшість із них належить до злочинів невеликої тяжкості (відповідальність за них встановлена ч. 1 ст. 361, ч. 1 ст. 361-2, ч. 1 ст. 362, ст. 363, ч.1 ст. 363 КК); до злочинів середньої тяжкості належать посягання, передбачені ч. 1 ст. 361, ч. 2 ст. 361 і, ч. 2 ст. 361-2, ч. 2 ст. 362 КК; решта злочинів є тяжкими (ч. 2 ст. 361, ч. 3 ст. 362 КК) [97, с. 13].

Наступною обов’язковою ознакою злочину, що виражає його внутрішній психологічний зміст, є винність. Ця ознака відображає найважливіший принцип кримінального права — суб’єктивного ставлення, тобто відповідальності тільки за наявності вини, що випливає із ст. 62 Конституції України. Частина 2 ст. 2 КК закріпила цей принцип, зазначивши, що особа вважається невинуватою у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду. Отже, закон про кримінальну відповідальність виключає об’єктивне ставлення, тобто відповідальність за шкоду, заподіяну за відсутністю вини, яка відповідно до ст. 23 КК є психічним ставленням особи до вчинюваної дії чи бездіяльності та їх наслідків, вираженим у формі умислу або необережності.

Злочин являє собою єдність об’єктивного й суб’єктивного: діяння і психічного (свідомого, вольового) ставлення до нього. Як діяння не може бути розкрите поза зв’язком з психічним ставленням особи до нього, так і зміст психічного ставлення (вини) не можна визначити поза зв’язком з характером діяння: об’єктом, на який вона посягає, способом, наслідками та іншими об’єктивними ознаками. Вина значною мірою визначає характер діяння і ступінь його тяжкості та є важливим критерієм визнання його злочином.

Обов'язковою ознакою злочину його протиправність. Як формальна ознака злочину протиправність означає його наявність у кримінальному законі. Кримінальна протиправність тісно пов'язана із суспільною небезпечністю: вона є суб'єктивним виразом об'єктивної, реальної небезпечності діяння для суспільних відносин, її законодавчої оцінки. Тому кримінальну протиправність — юридичну, правову оцінку суспільної небезпечності — закріплено в законі. Саме суспільна небезпечність, її ступінь визначають об'єктивні межі протиправності, за якими питання про криміналізацію діяння виникати не може. Виділення законом кримінальної протиправності, як обов'язкової ознаки злочину, являє собою конкретний вираз принципу законності у кримінальному праві: кримінальній відповідальності і покаранню підлягає лише особа, котра вчинила суспільно небезпечне діяння, яке передбачено законом, як злочин. Кримінальний закон дає вичерпний перелік злочинів. Тому, якщо діяння навіть становить небезпечність для суспільства, але не його передбачено законом про кримінальну відповідальність, воно не може розглядатися у якості злочину. Звідси випливає найважливіше положення про неможливість застосування кримінального закону за аналогією до такого діяння, що прямо у ньому не передбачене, адже відповідно до ч. 4 ст. 3 КК застосування закону про кримінальну відповідальність за аналогією заборонено.

Конституція України в ч. 2 ст. 58 містить найважливіший принцип законності: «Ніхто не може відповідати за діяння, які під час їх вчинення не визнавалися законом як правопорушення» і частина 4 ст. 3 чинного КК цілком відповідає такому положенню [10, с. 76-77].

З ознакою протиправності пов'язана четверта обов'язкова ознака злочину — караність, під якою розуміється загроза застосування за злочин покарання, що міститься у кримінально-правових санкціях. Караність за своєю сутністю випливає із суспільної небезпечності і протиправності діяння: воно тому і кримінально каране, що є суспільно небезпечним і передбаченим кримінальним законом як злочин.

У той же час діяння, за яке в законі передбачене кримінальне покарання, не втрачає властивостей злочину, якщо в конкретному випадку його вчинення за нього

не буде призначене покарання (наприклад, унаслідок закінчення строків давності, за амністією та ін.). Ще у 1961 р. В.В. Сташис слушно відзначав, що «зовсім неправильно ототожнювати караність, як ознаку злочину із застосуванням покарання у будь-якому випадку його вчинення. Караність слід розуміти, як встановлення у законі за вчинення певного діяння кримінально-правової санкції, що дає змогу застосовувати в належних випадках (а не завжди) покарання» [159, с. 30]. Науковець С.С. Мірошниченко зазначив, що встановлення кримінальної відповідальності може здійснюватись виходячи із принципу доцільної економії репресії, проте це можливо лише за умови, якщо іншими заходами впливу або більш м'якими правовими засобами запобігти такому діянню неможливо [94, с. 70].

З урахуванням викладеного, підкреслюючи єдність ознак злочину, можна зробити висновок про те, що тільки наявність сукупності чотирьох розглянутих ознак — суспільної небезпечності, винності, протиправності, караності — характеризує діяння, вчинене суб'єктом злочину, як злочин [10]. Встановлення юридичної відповідності ознак злочинного діяння ознакам складу злочину, описаного у конкретній нормі кримінального закону має назву кваліфікація злочину [29, с. 74]. З метою структуризації знань про кримінально-правову кваліфікацію злочинів, перейдемо до дослідження безпосереднього складу злочину, встановлення елементів якого необхідно для визнання діяння злочином. Розуміння складу злочину слугує основоположним важелем на шляху до встановлення вірної кваліфікації.

Склад злочину необхідно відмежовувати від самого злочину, оскільки вони не збігаються один з одним, а тільки співвідносяться між собою як явище (конкретний злочин) та юридичне поняття про нього (склад конкретного виду злочину). Злочин — це конкретне суспільно небезпечне діяння (наприклад, надісланий файл "заразив" вірусом програмне забезпечення ЕОМ), вчинене за певних обстановин, що відрізняється безліччю особливостей від усіх інших злочинів даного виду (наприклад, переславши повідомлення, що мало пагубний характер). Склад же злочину являє собою юридичне поняття про злочини певного виду, у якому об'єднані їх найбільш істотні, типові та універсальні ознаки [29, с. 87].

Під складом злочину розуміють юридичну (нормативно-правову) конструкцію [82], що являє собою систему об'єктивних і суб'єктивних ознак, встановлених кримінальним кодексом України, які у сукупності визначають суспільно небезпечне діяння злочином.

Ознака складу злочину — це певна риса (властивість, якість) злочину, яка задовольняє вимогам:

а) визначає суспільну небезпечність, протиправність та винність діяння;

б) відображає індивідуальні риси й особливості, притаманні конкретному злочину, якими він відрізняється від інших злочинів, а також від діянь, що не є злочинними;

в) безпосередньо вказана в законі чи випливає з його змісту при тлумаченні;

г) притаманна всім злочинам даного виду (типу) і не є виведеною (утвореною) від інших ознак [83, с. 111-115].

Ознаки згруповані в одиниці більш високого (за ступенем узагальнення) рівня, утворюють структуру складу злочину, такі узагальнені одиниці в теорії кримінального права отримали назву **«елементи складу злочину»**. В основу такого рішення покладена, як уявляється, модель акту реальної суспільно небезпечної поведінки особи (як і в цілому — поведінки людини) у формі діяння, структуру якого утворюють об'єкт та суб'єкт, що об'єднані актом поведінки людини, в межах якої виокремлюються об'єктивна і суб'єктивна сторона цієї поведінки (діяння).

У структурі складу злочину (на підставі структурного аналізу акту поведінки особи — її діяння) виокремлюють об'єкт (у низці випадків — також і предмет злочину), об'єктивна сторона (до якої відносять суспільно небезпечне діяння, суспільно небезпечні наслідки, причинний зв'язок між діянням і наслідками, місце, час, обстановку, спосіб, засоби вчинення злочину), суб'єктивна сторона (певна форма вини — умисел чи необережність, мотив та мета злочину), суб'єкт злочину (особа фізична, осудна, що досягла віку кримінальної відповідальності). Ці елементи виступають категоріями кримінального права і мають важливе гносеологічне та юридичне значення. Загальне поняття складу злочину не може виступати юридичною (нормативно-правовою) підставою кримінально-правової кваліфікації, а

також і кримінальної відповідальності, такою підставою може бути лише конкретний склад злочину, який включає у себе найбільш суттєві ознаки злочинів.

Зазначене надає можливість дійти наступних висновків:

1) склад злочину являє собою сукупність об’єктивних і суб’єктивних ознак, що характеризують конкретне суспільно небезпечне діяння як злочин;

2) сукупність зазначених ознак встановлюється тільки в кримінальному законі;

3) перелік складів злочинів, передбачених кримінальним законом, є вичерпним;

4) характер і обсяг відповідальності за скоєний конкретний злочин визначається тільки в складі злочину [165, с. 66-67].

Основною складовою пізнавальної діяльності при кваліфікації злочинів, її кульмінацією є встановлення точної відповідності ознак вчиненого суспільно небезпечного діяння ознакам складу злочину, визначеним у кримінально-правовій нормі і закріпленим у тексті відповідних статей КК. Отже, сутність кваліфікації полягає в послідовному встановленні у вчиненому суспільно небезпечному діянні відповідних елементів і ознак складу злочину, які в сукупності визначають таке діяння злочином [7, с. 13-16, 26]. Поглиблений аналіз елементів складу злочину (об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона), передбачених статтями 361-363-1 Кримінального Кодексу України дозволить провести вірну кримінально-правову кваліфікацію злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, з урахуванням особливостей, притаманних даній категорії злочинів, що в свою чергу забезпечить дотримання принципів законності, презмпції невинуватості та забезпечення додеденості вини, змагальності сторін та безпосередності дослідження доказів у кримінальних справах.

Висновки до розділу 1

Все вищезазначене дає змогу сформувати такі висновки:

1. Кваліфікація злочинів і кримінально-правова кваліфікація визначають якість протиправних посягань та є взаємодіючими частинами. Кримінально-правова кваліфікація має широке застосування у кримінальному праві, адже вона дозволяє

досліджувати не лише злочини, а й правопорушення, малозначність яких не призводити до настання кримінальної відповідальності; в силу латентності; обставин, за яких виключається злочинність діянь. Вона є поглибленим процесом дослідження злочинних виразів, зважаючи на обставини за яких вони відбулись.

2. Склад злочину є досліджуваним елементом кримінально-правової кваліфікації, адже встановлення юридичної відповідальності ознак злочинного діяння ознакам злочину, які містяться у законі про кримінальну відповідальність є саме кваліфікацією злочину.

Ознаками злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, за загальним правилом є: суспільна небезпечність, протиправність, винність та караність. наявність перелічених обставин є необхідною умовою для визнання скоєного злочином. У свою чергу, елементами складу злочину є: об'єкт, об'єктивна сторона, суб'єкт та суб'єктивна сторона. Ці елементи виступають категоріями кримінального права, перелік яких за кримінальним законодавством є вичерпним. Характер і обсяг відповідальності за злочин визначається окремо і є наслідком наявних обставин у справі.

РОЗДІЛ 2 ОСОБЛИВОСТІ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

2.1 Ключові знання про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Історія злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку сягає давніх коренів, про злочини даної категорії згадувалося ще у 5680 році до нашої ери у літописах єгипетських мудреців про так званих Чорних отруйників, які згодовували своїм жертвам розтерті в порошок рахункові палички — так званий прообраз сучасного персонального комп'ютера. У історичному ракурсі вони зародились в Америці у 1945 році, коли була створена перша ЕОМ (комп'ютер), яка використовувалась для розшифровування німецьких військових кодів, а згодом й для іншої діяльності.

Термін «кіберзлочинність» з'явився в американській доктрині на початку 60-х р.р., коли були виявлені перші випадки злочинів, здійснених із використанням комп'ютерів. Саме тоді з'явилися перші «хакери», ними були студенти Масачусетського технологічного інституту, які маніпулювали з програмами нового університетського комп'ютера [143, с. 294]. Електронно обчислювальні машини (ЕОМ) набули широкого застосування як серед працівників правоохоронних органів так і серед вчених, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [33, с. 17].

Після цього, у 1966 р. зафіксовано перший випадок використання ЕОМ як інструмента при пограбуванні банку в Міннесоті. Першою ж людиною, що застосувала ЕОМ для вчинення податкового злочину на суму 620 тис. доларів і постала за це перед американським судом у 1969 р., був Альфонсо Конфессоре.

Подальша історія «комп'ютерних» злочинів відмічена такими найбільш «яскравими» подіями:

• кінець 70-х — пограбування «Секьюріті пасифік банк» (10,2 млн. доларів);

• 1979 р. — комп'ютерне розкрадання у Вільнюсі (78584 крб.);

• 1984 р. — повідомлення про перший в світі «комп'ютерний вірус»;

•1985 р. — виведення з ладу за допомогою «вірусу» електронної системи голосування в конгресі США;

• 1986-1988 рр. — поява першого «комп'ютерного вірусу» в СРСР;

• 1989 р. — блокування американським студентом 6000 ЕОМ Пентагону;

• 1990 р. — міжнародний з'їзд комп'ютерних «піратів» у Голландії з демонстрацією можливості необмеженого втручання в системи ЕОМ;

• 1991 р. — розкрадання коштів Зовнішекономбанку на суму в 125,5 тис. доларів;

• 1992 р. — умисне порушення роботи АСОВІ реакторів Ігналінськой АЕС;

• 1993 р. — електронне шахрайство в Центробанку Росії (68 млрд. крб.);

• 1995 р. — спроба російського громадянина пограбувати Сіті-банк на суму 2,8 млн. доларів [51, с. 133].

Розглянемо більш детально наведені факти вчинення комп'ютерних злочинів.

У 1970 роках у США з'явились «фрікери», які з метою безоплатного телефонування світом, зламували телефонні мережі операторів зв'язку. Одним з таких «фрікерів» був Джон Дрейпер, який звернув увагу на те, що іграшковий свисток, який продавався разом з вівсяними пластівцями Cap'nCrunch видає звук на частоті 2600 герц, що співпадає з частотою сигналу доступу до телефонної мережі далекого зв'язку компанії AT&T. Дрейпер сконструював першу «блакитну коробку» BlueBox, завдяки якій можна було безоплатно телефонувати закордон. У цій коробці, у тому числі знаходився свисток, який свистів у мікрофон телефону на частоті 2600 герц. Одних телефонних мереж фрікерам стає замало і у 1980 роках і вони почали втручатись до комп'ютерних мереж. Ними створюються так звані електронні дошки об'яв – BBS, такі як «SherwoodForest» та «Catch-22» де хакери і фрікери спілкуються та обмінюються досвідом щодо крадіжок паролів та номерів

кредитних карток. З’являються перші хакерські спільноти «LegionofDoom» в США та «ChaosComputerClub» в Німеччині.

Перше створення шкідливого програмного засобу, а саме вірусу відбулось у 1988 році, коли студент Корнельського університету Роберт Морріс розробив «комп’ютерного черв’яка» — програму, яка самостійно розмножувалась та проникла до майже 6000 університетських та урядових комп’ютерів по всій Америці, внаслідок чого було спричинено велику матеріальну шкоду [143, с. 294].

Перший злочин, здійснений із використанням комп'ютера в колишньому Союзі Радянських Соціалістичних Республік (СРСР), було зареєстровано у 1979 р. у Вільнюсі, ним стало розкрадання, збитки від якого складали 78 584 крб. Цей факт було занесено до міжнародного реєстру правопорушень подібного роду і він став своєрідним початком розвитку нового виду злочинів у колишньому СРСР [9, с. 126].

Проте заходів по протидії комп'ютерним злочинам ще не існувало. Створення комп’ютерної безпеки було поставлено на трохи пізніший час, після того, як студент Корнельського університету зумів потрапити до комп’ютерних систем американської розвідки, міністерства оборони та відключив в цих системах кілька тисяч комп’ютерів. Тоді і були зроблені перші заходи протидії: при університеті Карнегі Меллон у Пітсбурзі на кошти Пентагону була створена комп’ютерна група швидкого реагування — CERT (Computer Emergency Response Team), призначена для реєстрації великих «зломів» комп’ютерних мереж і надання допомоги в «латанні» дірок, прооблених злочинцями [57;16, с. 96].

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю було прийнято у 1973 році у Швеції та у 1976 році у США. Перші закони стосовно комп’ютерних злочинів прийняті у 70-80 роки майже усіма індустріально розвинутими країнами. Серед них Computer Fraud and Abuse Act 1984 Сполучені Штати Америки, які найбільше страждають від комп’ютерних злочинів. Згодом і в інших країнах світу були затверджені законодавчі акти стосовно даної категорії злочинів. До боротьби з комп'ютерними злочинами, виходячи з їх широких масштабів та багатоманітних втрат, підключились міждержавні і громадські

організації. Але процес вдосконалення чинного законодавства не припиняється і сьогодні, що пояснюється стрімким розвитком інформаційних технологій [44].

Початок XXI століття ознаменувався широким запровадженням на світовому рівні комп'ютеризованих (автоматичних) інформаційно-технологічних систем у виробничій, комерційній, банківській та інших сферах, у зв'язку з чим головною і водночас невідкладною для вирішення проблемою стала розробка адекватної системи захисту цих систем від несанкціонованого вторгнення. Проблема загострювалась пропорційно до зростання обсягів інформації, переважно завдяки активному функціонуванню глобальної комп'ютерної мережі Інтернет, адже ці злочини не вимагали ані ретельної підготовки, ані часу для втілення злочинного замислу. Широка географія, віддаленість об'єкта посягання (за тисячі і сотні тисяч кілометрів від місця вчинення злочину), складнощі з виявлення, доведення вини, а так само високий дохід, зробили цей вид злочинної діяльності одним з найбільш привабливих для «фахівців» злочинного світу.

Перші кроки щодо протидії кіберзлочинам в Україні були здійснені у 1994 році, коли до Кримінального кодексу 1960 року було внесено зміни, якими в ст. 198-1 «Порушення роботи автоматизованих систем» було передбачено кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення до автоматизованих систем і здатних спричинити перекручення або знищення інформації чи носіїв такої інформації. Однак у 2001 році було прийнято Кримінальний кодекс України (КК України), відповідно до якого ця діяльність вийшла на якісно новий рівень.

Проведено чимало наукових досліджень з цього приводу, у яких вживалися терміни: «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку»; «комп'ютерні злочини»; «кіберзлочини»; «злочини у сфері IT-технологій»; «високотехнологічні злочини»; «інтернет-злочини»; «злочини у сфері високих технологій»; «е-злочини»; «злочини у сфері інформаційно-

телекомунікаційних систем» та ін. Надані визначення є досить схожими, однак у них є і відмінності, які у цій главі ми і спробуємо окреслити.

Відправною точкою для визначення понять, якими оперує законодавець у сфері протидії кіберзлочинності є Конвенція про кіберзлочинність від 23 листопада 2001 року (Конвенція). Сьогодні вона ратифікована 18 державами та підписана 25 країнами, серед яких є і Україна від 7 вересня 2005 року [136]. Згодом, у липні 2006 року, було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Додатковий протокол) [47]. На жаль, терміни, які вживаються в Конвенції та додатковому протоколі до неї, так і не знайшли свого закріплення у вітчизняному законодавстві. Разом з тим, варто зазначити, що у тексті Конвенції та Додаткового протоколу до неї також не міститься визначення поняття «кіберзлочин» та суміжних з ним понять, однак наявний перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність, та наводиться їх умовна класифікація залежно від об'єкта правовідносин [3, с. 4].

Необхідно констатувати, що у вітчизняному законодавстві визначено лише перелік злочинів, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку, закріплених у Розділі XVI КК України. Хоча у деяких законодавчих актах згадуються деякі поняття, проблематику формулювання яких ми розглядаємо, проте в жодному із нормативних актів так і не надано їх визначення.

У «Доктрині інформаційної безпеки України» використовувались категорії «комп'ютерна злочинність» та «комп'ютерний тероризм» [119, ст. 1783]. Стратегія національної безпеки, затверджена Указом Президента України від 8 червня 2012 року № 389/2012, містить терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [161]. Також у Законі України «Про основи національної безпеки України» згадуються поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» [127, ст. 351].

Законом України «Про основні засади забезпечення кібербезпеки України» надано визначення поняття - кіберзлочин. Кіберзлочин (комп'ютерний злочин) є

суспільно небезпечним винним діянням у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [128, ст. 1].

Частково питання визначення термінології мав би вирішити Закон України «Про кібернетичну безпеку України», проект якого було зареєстровано ще 4 червня 2013 року. Проте він не містив визначення кіберзлочину і так і не був прийнятий. Дещо пізніше Указом Президента України від 1 травня 2014 року № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» було поставлено завдання розробити проекти Стратегії кібернетичної безпеки України і Закону України «Про кібернетичну безпеку України», а також привести національне законодавство у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [13, с. 416]. Стратегія кібернетичної безпеки України було затверджено Указом Президента України від 15 березня 2016 року № 96/2016 [160].

Попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення понять, які є відправними у сфері формування державної інфраструктури інформаційної безпеки. Розв'язання проблеми потребує вдосконалення нормативно-правових актів, які є підґрунтям єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації [3, с. 7], тож звернемось до досліджень науковців.

Дослідники Д.С. Азаров [1, с. 53-54] та Н.С. Козак [64, с. 156] більш схильні до вживання понять «злочини у сфері інформаційно-телекомунікаційних систем» та «кіберзлочини», порівняно з поняттям «злочини у сфері електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», вважаючи їх більш глобальними та відповідними

існуючій картині розвитку злочинів у інформаційній сфері. Натомість А.А. Музика та Д.С. Азаров визначають тотожність понять «кіберзлочини» та «злочини у сфері комп'ютерної інформації» [1, с. 5]. Вчені наголошують, що визначати кіберзлочин необхідно, як злочин у сфері комп'ютерної інформації. Вчені Є.А. Бідашко та Н.Л. Волкова пропонують таке визначення даної категорії злочинів, як «передбачені кримінальним законом суспільно небезпечні діяння, в яких машинна інформація є або засобом, або об'єктом злочинного посягання [17, с. 161]. Проте М.А. Погорецький та В.П. Шеломенцев не погоджуються з позицією науковців, які розглядають злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку, як злочини, вчинені в інформаційному середовищі, проти інформаційних ресурсів, тобто у сфері комп'ютерної інформації, або за допомогою інформаційних засобів. Інформаційно телекомунікаційна система — це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [121, ст. 1]. На думку останніх, терміни «інформаційне середовище», «інформаційні ресурси», «інформаційні засоби» є занадто загальними для сфери використання комп'ютерних систем і не розкривають суті процесів автоматизованої обробки інформації. Вчені вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їх вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які, у свою чергу, є середовищем вчинення кіберзлочинів. Комп'ютерні дані при цьому, на їхню думку, слід розглядати як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем. Ґрунтуючись на цій позиції, кіберзлочини слід вважати такими, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [112, с. 90-92].

Кіберзлочини — це злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство, або кібертероризм) [13, с. 417]. О.К. Копатін та Є.Д. Скулишин надають декілька визначеннь поняттю «кіберзлочин»:

1. Кіберзлочин – злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин у кіберпросторі. На відміну від комп'ютерного злочину, поняття якого пов'язане з використанням будь-якої комп'ютерної техніки, кіберзлочин є більш вузьким поняттям, пов'язаним із функціонуванням саме кібернетичних комп'ютерних систем. До протиправного використання кібернетичних комп'ютерних мереж віднесено несанкціоноване отримання прав керування такою системою (наприклад, використання шкідливого програмного забезпечення, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку тощо), її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення та використання в злочинних цілях однієї кібернетичної комп'ютерної системи проти інших (наприклад, створення мережі зомбованих комп'ютерів для здійснення атак на веб-сайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо). [3, с. 6; 71, с. 85-86].

2. Кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [21, с. 85-86].

3. Кібернетичні злочини є передбаченими кримінальним законом суспільно небезпечним винним діянням, що полягає в протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [71, с. 214].

Отже, вчені чітко відмежували кіберзлочин та злочин, що вчиняється з використанням комп'ютерної техніки, де може й не бути кіберпростору.

На думку вчених П.Д. Біленчука та М.А. Зубаня [19, с. 6] — це «суспільно небезпечна діяльність або бездіяльність, яка здійснюється з використанням сучасних технологій і засобів комп'ютерної техніки з метою заподіяння шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи» [60, с. 32-37]. А.Н. Карахан'ян розуміє такі злочини, як протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ [113, с. 77]. В.В. Лісовий вважає, що основною кваліфікуючою ознакою належності злочинів до розряду комп'ютерних є «електронна обробка інформації», незалежно від того, на якій стадії злочину вона застосовувалася [88, с. 87]. В.О. Голубєв визначає таку ознаку як «використання засобів комп'ютерної техніки» [39, с. 39]. В.В. Крилов, як альтернативу пропонує ширше поняття «інформаційні злочини», яке дозволяє абстрагуватися від конкретних технічних засобів [80, с. 11]. На думку вченого В.Г. Телійчука такі злочини слід називати «комп'ютерними злочинами», адже комп’ютерна злочинність — особливий вид злочинів, пов’язаних із незаконним використанням сучасних інформаційних технологій і засобів комп’ютерної техніки [169, с. 31]. Л.В. Сорока також дотримується визначення комп'ютерні злочини, відповідно до якого — це злочини, у яких комп'ютер безпосередньо є предметом та (або) знаряддям здійснення правопорушень у суспільних сферах, які пов'язані з використанням комп'ютерної техніки [157, с. 263].

Визначивши суспільні відносини, яким завдається шкода в результаті вчинення комп’ютерних злочинів, можна сформулювати й саме поняття «комп’ютерні злочини» — як суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є ЕОМ, автоматизовані системи, комп’ютерні мережі або мережі електрозв’язку [3, с. 8].

Таким чином, вчені визначають кіберзлочини як сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи

функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов’язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію. Виходячи із цього, кіберзлочини слід вважати злочинами, які вчиняються за допомогою або через комп’ютерні системи чи пов’язані саме з комп’ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше у відповідності до певної програми виконують автоматичну обробку даних.

Зважаючи на існування різних поглядів на визначення злочинів даної категорії, вважаємо, за потрібне ознайомитись з похідними поняттями від кіберзлочинності.

Кіберправопорушення є суспільно небезпечним діянням, яке здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки знищення) інформації, представленої у вигляді комп’ютерних даних, і тягне за собою юридичну відповідальність. Кіберправопорушення має всі загальні ознаки правопорушення, що виділяються в теорії права та вирізняються лише факультативною частиною юридичного складу, у якому кіберпростір виступає як засіб або мета здійснення правопорушення [71, с. 87]. На думку В.М. Болгова, вислів «кримінальні правопорушення, що вчиняються з використанням інформаційних технологій», є не дуже зручним для вживання у побутовій мові, тому науковець визнає доцільним короткий термін «кіберзлочини», тим більше, що об’єктом цієї категорії правопорушень є інформація та тісно пов’язані з нею технології її обробки – інформаційні технології.

Кіберпроступки — кіберправопорушення, які не несуть суттєвої суспільної небезпеки, за які законодавством передбачена юридична відповідальність (крім кримінальної).

Кіберпростір (кібернетичнийпростір) у науковому світі має декілька визначень:

1) штучне електронне середовище існування інформаційних об’єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп’ютерних

систем управління й обробки інформації та забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання послуг, ведення електронної комерції);
2) простір, сформований інформаційно-комунікаційними системами, у якому відбуваються процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [71, с. 87-88].

Верховний Суд США надав таке визначення кіберпростору: «Унікальний носій, який не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет» [91, с. 152]. Інституціональним втіленням кіберпростору є Інтернет, саме він являє собою глобальну інформаційну систему, яка складається з інформаційних систем та дозволяє користувачам здійснювати обмін інформацією з комп'ютерами у такій системі.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберпростір э середовищем (віртуальним простором), який надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворений у результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [126, ст. 1].

На нашу думку, кіберпростір є матерією зовні невідчуваємого поля інформаційних відносин, який слугує зменшеним прототипом Всесвіту, на тлі якого планети — електронно-обчислювальні машини (ЕОМ) та технічні засоби; осі — системи інформаційної передачі: автоматизована система, комп'ютерна мережа та телекомунікаційна мережа та ін. Тобто, це простір, на якому відбуваються інформаційні відносини у найширшому значенні [192, с. 102].

Висвітлені поняття цієї глави мають під собою нормативно-правову регламентацію, підтвердженні науковими здобутками вчених, думки яких у певних аспектах є протилежними. Виходячи з того, що об'єктом нашого наукового

дослідження є саме злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку, то вище перелічені визначення можуть вживатися у науковій роботі у якості синонімів.

Викликає занепокоєність збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), комп’ютерних систем та мереж як у світі, так і в Україні, оскільки такі злочини не лише гальмують позитивні тенденції розвитку, а й завдають шкоду суспільству, державі, суб’єктам інформаційних відносин в усіх сферах господарювання та окремим громадянам. З такими проявами поки що складно вести ефективну боротьбу, як з точки зору кримінального переслідування, так і застосування організаційно-управлінських і кримінологічних заходів з метою їх попередження [147, с. 267].

Підстави виникнення злочинності у сфері використання ЕОМ доцільно розглядати у комплексі причин залежно від відносин, які їх спричиняють. Перш за все це правові причини, до яких можна віднести:

— відсутність або недостатнє правове регулювання суспільних відносин у сфері інформаційних технологій, як тих, що формуються, так і тих що сформувалися. Відсутність належного законодавчого регулювання в рамках міжнародного права є однією з підстав розвитку кіберзлочинності, адже національним законодавством окремо взятої країни усіх проблем охорони комп'ютерних технологій вирішити неможливо. Виникає необхідність застосовувати єдині підходи, однотипні моделі поведінки, що можливо лише за умови спорідненості або тотожності їх національного карного законодавства або додаткових домовленостей та погоджень щодо переслідування правопорушників [43, с. 93].

— недостатня правова урегульованість інших суспільних відносин, що є одним з основних факторів існування соціально-економічних причин злочинності у сфері використання ЕОМ;

— інформаційні відносини в Україні знаходяться на стадії формування, законодавство про інформаційні відносини регулює в основному загальні питання,

тому лише деякі галузі врегульовані в достатній мірі (захист державної і інших видів таємниць).

Загрози кібербезпеці актуалізуються внаслідок дії таких чинників, зокрема, як:

1. Невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

2. Недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

3. Безсистемність заходів кіберзахисту критичної інфраструктури;

4. Недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів;

5. Недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

6. Недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [160, п. 2].

Головним напрямом державної політики у сфері забезпечення безпеки повинно стати посилення ролі жержави в якості гаранта безпеки особи [74, с. 21]. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури. У свою чергу, критично важливі об’єкти інфраструктури - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей.

Аналіз вітчизняного законодавства вказує на відсутність предмета правового регулювання в питаннях індивідуальної, групової і суспільної свідомості, що як наслідок призводить до відсутності правових актів, що встановлюють відповідальність за дані діяння [147, с. 268].

Кіберзлочини мають низку особливостей суб'єктів, завдяки яким вони посягають через комп'ютерні системи на сфери міжнародного правопорядку, і зокрема — на міжнародний обмін інформацією. Сьюзанн В. Бреннер виділяє наступні ознаки «кіберзлочинів», що відрізняє їх від «звичайних» злочинних посягань та значно підвищує їх суспільну небезпечність:

1. «Кіберзлочин» не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого;

2. Є «автоматизованим» злочином, це означає, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч;

3. Суб'єкт «кіберзлочину» не підвладний обмеженням, які існують у реальному, фізичному світі. Так, «кіберзлочини» можуть бути вчинені моментально, і тому потребують швидкої реакції у відповідь.

4. «Кіберзлочинність» і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це має місце зі злочинами, що вчиняються у реальному, фізичному світі [188].

Відсутність законодавчо закріплених визначень породжує на теоретичному рівні дискусії. Наприклад М.А. Погорецький та В.П. Шеломенцев вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їх вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які у свою чергу є середовищем вчинення кіберзлочинів. Комп'ютерні дані при цьому, на їхню думку, слід розглядати як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем [140].

За В.М. Бутузовим ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є:

— знаряддя вчинення злочину – комп'ютерна техніка;

—специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). До того ж об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації [3, с. 5; 13, с. 415; 27, с. 119].

Об'єктом злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виступають соціальні відносини щодо правового захисту майнових або суспільних інтересів держави, юридичних і фізичних осіб та їхніх прав і свобод в інформаційній сфері.

Водночас об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що має свій прояв у кіберпросторі. При цьому автор посилається на перелік протиправних діянь, які передбачені у Конвенції та Додатковому протоколі до неї. На його думку, тільки діяння із цього переліку можуть бути віднесені до кіберзлочинів.

Предметом таких дій є інформація (інформаційні ресурси) та інформаційні технології [27, с. 119].

Характерними особливостями злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є:

- складність визначення розміру заподіяних збитків;
- значні фінансові витрати на проведення розслідування.

Слід зазначити, що сьогодні існує потреба у фахівцях, які мають необхідні для розкриття «комп'ютерних злочинів» навички та кваліфікацію, а також врегулювання національним законодавством багатьох питань, які виникають під час збору і документування інформації про «комп'ютерні злочини», а також у процесі проведення слідчих дій (наприклад, обшук комп'ютера, пошук слідів у комп'ютері, порядок зняття копій з машинних носіїв даних тощо) [85, с. 230].

Одним з напрямків урегулювання інформаційних процесів є криміналізація суспільно небезпечних діянь, яка здійснюється на основі таких чинників:

— існування самих фактів вчинення подібного діяння;

— визначення ступеня суспільної небезпеки діяння;

— відносна поширеність діяння;

— визначення громадської думки відносно даних діянь.

При вирішенні питання про криміналізацію діяння необхідно також визначити можливості виявлення, запобігання, фіксації діяння, закріплення доказів його вчинення - оцінка наукових, технічних, матеріальних, кадрових та інших можливостей. Наприклад, для боротьби з комп'ютерними злочинами застосовувати спеціальну техніку, за допомогою якої здійснювати контроль за напрямом руху інформації з головних комп'ютерів банків, застосовувати складні системи кодування інформації, використовувати біометричні системи контролю та ідентифікації працівників (наприклад, за малюнком сітківки ока), вдосконалювати пластикові картки, здійснювати страхування спеціальними компаніями таких видів злочинів та вживати інші заходи попередження вчинення злочинів [147, с. 268].

2.2 Види злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Багатонаціональність електронних мереж дозволяє взаємодіяти користувачам різних країн світу. Даний аспект набув рис транснаціональності, саме тому, дослідження особливостей кіберзлочинів міжнародного характеру та злочинів, вчинених за допомогою комп'ютерної техніки потребує поглибленого дослідження.

Міжнародна кіберзлочинність може завдати шкоду як громадянам певних країн, об'єднанням, установам, організаціям і т.д., так і державним інтересам в цілому. Інформаційна безпека є важливим компонентом захисту кожної держави, у якій інформація наділяється надзвичайною цінністю, виступаючи у певних випадках стратегічним ресурсом. Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих

держав, груп та осіб [160]. Тому створення національної системи кібербезпеки є складовою системи забезпечення національної безпеки України.

Під транснаціональною злочинністю новітніх комп’ютерних технологій у науковій праці розуміються види кіберправопорушень, які вчиняються у різних державах світу [150, с. 133].

Міжнародні правопорушення поділяються на:

1. Міжнародні злочини;
2. Злочини міжнародного характеру;
3. Міжнародні делікти.

Міжнародні злочини — це злочини, що порушують міжнародні зобов'язання, які є основними для забезпечення життєво важливих інтересів міжнародного співтовариства і розглядаються як злочини міжнародним співтовариством у цілому.

Міжнародні злочини:

- здійснюються державами, посадовими особами держав, що використовують механізм держави в злочинних цілях, а також рядовими виконавцями;
- здійснюються в безпосередньому зв'язку із державою;
- зазіхають на міжнародний мир і безпеку;
- загрожують основам міжнародного правопорядку;
- спричиняють відповідальність держави як суб'єкта міжнародного права і персональну кримінальну відповідальності виконавців, що наступає в рамках міжнародної, а в деяких випадках внутрішньодержавної (національної) юрисдикції.

Під злочином міжнародного характеру розуміють діяння фізичної особи, що посягає на права й інтереси двох або декількох держав, міжнародних організацій, фізичних і юридичних осіб [32].

Злочинами міжнародного характеру є протиправні діяння, об'єктом посягань яких є: мирне співробітництво і нормальне функціонування міжнародних відносин (за винятком міжнародних злочинів) [184].

Злочини міжнародного характеру:

— торкаються інтересів двох або декількох держав, юридичних осіб і/або громадян;
— здійснюються окремими фізичними особами поза зв'язком із політикою держави;

— спричиняють персональну відповідальність правопорушників у рамках національної юрисдикції [32].

Відповідно до доктрини сучасного міжнародного кримінального права злочини з використанням комп'ютерних технологій (інакше «кіберзлочини») віднесені до злочинів міжнародного характеру.

Зокрема, І.І. Карпець розуміє під «злочинами міжнародного характеру» діяння, передбачені міжнародними угодами (конвенціями), що зазіхають на нормальні відносини між державами, наносять шкоду мирному співробітництву в різних сферах відносин (економічних, соціально-культурних, майнових і т.п.), а також організаціям і громадянам, відповідальність за які настає або відповідно до норм, встановлених у міжнародних угодах (конвенціях), ратифікованих у встановленому порядку, або відповідно до норм національного карного законодавства [59, с. 48].

На нашу думку, комп'ютерні злочини можна віднести як до міжнародних злочинів, так і до злочинів міжнародного характеру [150, с. 134], адже об'єктами кібербезпеки виступають конституційні права і свободи людини і громадянина; суспільство, 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 таоб'єкти критичної інфраструктури.

Об'єктами кіберзахисту в свою чергу є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [128, ст. 4].

Виходячи з вищезазначеного, найбільш розповсюдженими видами кіберзлочинів, які відображені у Конвенції про кіберзлочинність [69], є наступні склади:

a. незаконний доступ до комп'ютерної системи;
b. нелегальне перехоплення технічними засобами комп'ютерних даних;
c. втручання у комп'ютерні данні;
d. втручання у функціонування комп'ютерної системи;
e. підробка та шахрайство, пов'язане з комп'ютерами;
f. правопорушення, пов'язані з дитячою порнографією;
g. правопорушення, пов'язані з порушенням авторських та суміжних прав.

У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками зазначено, що існує дві категорії злочинів:

1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) — будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних;

2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) — будь-яке протиправне діяння, що вчинюється шляхом або у зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [33, с. 338].

Кримінальну відповідальність за кіберзлочини, як у вузькому, так і у широому розумінні врегульовує Конвенція про кіберзлочинність. Кримінальне законодавство окремо взятих країн світу, визначає карну відповідальність за кіберзлочини лише у вузькому розумінні, що можна підтвердити на прикладі України [51, с. 129].

В Особливій частині Кримінального кодексу існує Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Жодна із 6-ти статей цього розділу не містить норми, згідно з якою можна було притягнути до відповідальності особу, що вчинила, наприклад, шахрайство шляхом незаконних операцій з використанням

електронно-обчислювальної техніки (ч. 3 ст. 190 КК), або окремі суспільно-небезпечні дії, передбачені ст. 200 КК [150, с. 134].

Застосування комп’ютерів для вчинення названих діянь є лише певним способом вчинення злочину, який зазвичай не включається до обов’язкових ознак об’єктивної сторони складу злочину. За наявності певних фактичних обставин ці злочини можуть кваліфікуватись за сукупністю зі злочинами, передбаченими Розділом XVI Особливої частини КК України [185, с. 435]. Потрібно також зауважити, що завдяки застосуванню комп’ютерних технологій значна кількість «звичайних» злочинів перейшла сьогодні до категорії «кіберзлочинів». До того ж способи їх вчинення істотно полегшились, а «географія» розширилась [51, с. 129].

За характером їх умовно можна поділити на дві основні групи: воєнно-політичні і економічні.

До воєнно-політичної групи слід віднести кібервійни, обумовлені комп'ютеризацією ракетно-ядерного арсеналу кожної держави.

До економічних злочинів доцільно віднести нелегальне інформаційне брокерство (злам комп'ютерних систем з наступним продажем інформації як самим потерпілим, так і конкурентам); організоване промислове (комерційне, підприємницьке) шпигунство; організоване комп'ютерне піратство. Європейський комітет з проблем злочинності Ради Європи у 1990 році підготував рекомендації з метою визначення в Європі правопорушень, пов'язаних з комп'ютерами, і ввів їх до «Мінімального списку» та «Необов'язкового списку» комп'ютерних злочинів, які були рекомендовані для включення до законодавств європейських країн [20, с. 167].

До Мінімального списку входять такі види протиправних діянь:

I. комп'ютерне шахрайство, комп'ютерний підлог, знищення комп'ютерної інформації та комп'ютерних програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних мереж;

II. несанкціоноване копіювання захищених комп'ютерних програм;

III. незаконне виробництво типографічних копій.

Необов'язковий список включає в себе такі види протиправних діянь:

I. зміна інформації чи комп'ютерних програм;

II. комп'ютерне шпигунство;

III. протизаконне застосування комп'ютера;

IV. несанкціоноване застосування захищених комп'ютерних програм [157, с. 265-266].

Практична сторона. Залишилися не врегульованими низка правових питань у даній сфері, зокрема, щодо визначення місця злочину, вчиненого за допомогою мережі Інтернет. Право якої держави слід застосувати, якщо правопорушник і об'єкт посягання знаходяться у різних країнах? Як має бути вирішено питання про межі можливого та необхідного застосування кримінального права країни до «кіберзлочинів», вчинених поза її територією [51, с. 130]?

Діючий на території України Закон «Про міжнародне приватне право» [123] розтлумачує деякі колізійні норми, що мають місце у міжнародній діяльності держав, однак регулювання кіберзлочинності не зачіпається жодним чином. Закон України «Про основні засади забезпечення кібербезпеки України» у статті 14 визначає, що Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю [128, ст. 14]. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки з дотриманням вимог законів України «Про порядок направлення підрозділів Збройних Сил України до інших держав» [133] та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України» [132]. Відповідно до норм яких, інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. До того ж, така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального

правопорушення з використанням кіберпростору. Проте у разі невідповідності норм законодавства країн, між якими стався злочин, відповідальність за скоєне може і не настати, адже підстав для надання інформації в однієї із країн може і не бути, за умови відсутності відповідальності за нормами законодавства тієї країни.

Аллан Р. Стейн стверджує, що найбільш проблемною характеристикою мережі Інтернет з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [194]. Інтернет сформувався та являє собою позатериторіальний засіб комунікації та обміну інформацією, який не має централізованого управління. Кожнен індивідуум і його комп'ютер діють автономно та формують єдину транснаціональну мережу, яка виходить за межі географічної концепції державних кордонів. Інтернет-адреси, що підтримуються мережею, нематеріальні, і навіть адреси сайтів, які містять URL-індикатори країни походження, наприклад, «ua», «pl» не обов'язково мають бути точними. Інтернет-адреси є довільними та можуть залишатись незмінними, у той час як сервери переміщаються у фізичному просторі. Така особливість Інтернету ставить науку і практику перед необхідністю розроблення нових підходів до протидії злочинам міжнародного характеру з використанням комп'ютерних технологій та побудови юрисдикційної політики стосовно таких злочинних посягань [51, с. 130].

Існує декілька основних напрямів вирішення проблеми подальшого регулювання Інтернету та кримінальної відповідальності за злочини міжнародного характеру з використанням комп'ютерних технологій. Відповідно до першого із них рекомендується пристосувати до злочинів, які вчиняються з використанням новітніх інформаційних технологій, традиційні принципи кримінальної юрисдикції. Що стосується другого, — пропонується розглядати Інтернет як самостійний «віртуальний» кіберпростір та розробляти нові правила застосування кримінальної юрисдикції щодо злочинів, які у ньому вчиняються [150, с. 135-136]. Прихильники першого напряму вважають, що нові Інтернет-технології автоматично не змінюють правову доктрину кримінальної юрисдикції і вона може бути застосована до «кіберзлочинів» міжнародного характеру [51, с. 130].

Конвенція про кіберзлочинність визначає традиційну схему кримінальної юрисдикції щодо регульованих злочинів, допускаючи територіальний та національний принципи кримінальної юрисдикції. Відповідно до частини 1 ст. 22, кожна із Сторін вживає таких законодавчих й інших заходів, які, на її думку, можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, криміналізованого Конвенцією, якщо він вчинений:

- a. на її території;
- b. на борту судна, яке плаває під прапором такої Сторони;
- c. на борту літака, зареєстрованого відповідно до законодавства такої Сторони;
- d. одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

Однак Конвенція не розтлумачує питання, які «кіберзлочини» слід вважати вчиненими на території даної країни, та поняття «місце вчинення злочину» і залишає це на розсуд національних судів. Особливо, зважаючи на особливість комп'ютерних злочинів, якщо, наприклад, місце знаходження зловмисника можливо відшикати за ір адресою пристрою скоєння, що стосується сторони, якій завдано шкоду, ми можемо про це дізнатися після настання наслідків. Загострення набуває ситуація, коли, наприклад, вірус вірус спричинив шкоду інтересам двох чи більше держав, або є, якщо це було логічна бомба, яка спрацьовує при настання певних обставин.

Міжнародна практика засвідчує, що єдиного підходу до вирішення цих питань на національному рівні досі не існує. Різне тлумачення місця вчинення злочинів, що пов’язано з комп’ютерними технологіями, а так само відсутність чіткого правового регулювання на міжнародному рівні можуть призвести з одного боку до конфліктів кримінальних юрисдикцій різних країн, коли дві і більше країни претендують на застосування закону про кримінальну відповідальність щодо одного злочинного діяння, а з іншого — до негативних конфліктів кримінальних юрисдикцій, коли жодна країна не вдається до переслідування вчиненого злочину.

У міжнародній правозастосовчій практиці питання кримінальної юрисдикції поставлене в залежність від існуючого поділу кіберзлочинів за колом об’єктів:

–злочини, що націлені та спричинюють шкоду конкретним об’єктам (наприклад, установі банку, електронній скринці приватної особи тощо);

—злочини, що націлені та посягають на невизначене коло об’єктів (наприклад, у разі розповсюдження комп’ютерних вірусів або порнографічної продукції) [51, с. 131].

Об'єктом кіберзлочинності, відповідно до Конвенції, є широкий спектр суспільних відносин, які охороняються нормами права. Ці відносини 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 областях, де використовуються комп'ютери, комп'ютерні системи і мережі. Серед них, з огляду на підвищену суспільну значимість, відокремлюються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського і суміжних прав [157, с. 267].

Питання застосування закону держави про кримінальну відповідальність до «кіберзлочинів», які посягають на конкретні об’єкти, найчастіше вирішується за правилами об’єктивної територіальності. Знаходячись в одній країні, особа спрямовує злочинне діяння на територію інших юрисдикцій, застосовуючи сучасні комп’ютерні мережі. Правоохоронні органи країни фізичного місця знаходження правопорушника можуть навіть не здогадуватися про вчинені ним кримінальні діяння, а виявляти їх вже за наслідками, які настають в іншій країні. У таких випадках кримінальне переслідування злочинця стає неможливим без міждержавного співробітництва. Правопорушник притягується до відповідальності на території країни перебування, або ж видається «потерпілій» країні за умов наявності відповідних міжнародних договорів та задоволення інших правових вимог, які супроводжують процедуру екстрадиції. Однак процедура екстрадиції є

досить складною і є скоріше винятком, ніж правилом розв’язання подібних питань [51, с. 131].

Відповідно до Європейської конвенції про видачу правопорушників, договірні Сторони зобов'язуються видавати одна одній осіб, які переслідуються компетентними органами запитуючої Сторони за вчинення правопорушення або які розшукуються зазначеними органами з метою виконання вироку або постанови про утримання під вартою [50, ст. 1]. Однак Україна так і не приєдналась до даної конвенції [137], тому дії суб'єктів комп'ютерних злочинів, що пов'язані з українськими територіями, не регулюються вищезазначеними нормами.

Міжнародний досвід також демонструє виняткові випадки, коли «потерпіла» країна вирішує питання про притягнення злочинця до кримінальної відповідальності без звернення до країни його місця знаходження. Питання застосування кримінальної юрисдикції країни до «кіберзлочинів», які посягають на невизначене коло об’єктів та відповідно порушують правопорядок у невизначеній кількості країн. Притягнення особи до кримінальної відповідальності можливе за правилами екстериторіальності, проте із застереженням — за умови наявності в ній кримінальної заборони щодо «кіберзлочинів» [51, с. 132].

Конвенцією про кіберзлочинність встановлені обов’язкові вимоги для врахування у законодавстві країн, які до неї приєдналися:

1. вживання заходів, необхідних для термінового збереження комп'ютерних даних (ч. 1 ст. 16);
2. збереження провайдерськими установами даних про трафік інформації у термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16);
3. зобов'язання зберігання конфіденційності отриманих даних у процесі проведення розслідування (ч. 3 ст. 16) [69].

Враховуючи прагнення України як до європейської так і до євроатлантичної інтеграції, для підвищення ефективності боротьби з кіберзлочинністю необхідний глобальний міжнародний обмін інформацією з протидії кібернетичній злочинності, враховуючи досвід країн, які не входять до членів конвенції про кіберзлочинність.

Набуло широкого розповсюдження створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Україні, Швейцарії, Швеції та ін. Основними функціями підрозділів кіберполіції виділяють: – моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення; – здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців; – розслідування кіберзлочинів, надання методичної та практичної допомоги галузевим службам і правоохоронним органам у межах своєї компетенції; – накопичення, узагальнення та аналіз інформації про кіберзлочинність; – профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації; – навчання працівників поліції та ін. [152, с. 193].

Виступаючи «сусідом» України — Польща, через яку так само проходять інформаційні мережі кіберзлочинності, бореться за допомогою «кібервійськ», чисельність яких поступово збільшується. Створення «кібервійськ» стало можливим завдяки фінансуванню з боку держави (близько 460 млн євро). В Індії кіберполіція залучає до своєї діяльності «хакерів». Можливо «кіберзлочинці» України, замість знаходження у місцях позбавлення волі під суворим наглядом кіберполіції стануть тим ідейним проривом, який нам необхідний. Допоможуть знайти шляхи подолання кіберзлочинності через поглиблене вивчення їх діяльності. У Сполучених Штатах Америки (США) створено підрозділ секретної служби, який взаємодіє між службами та правоохоронними органами штатів та приватним сектором виявляючи і запобігаючи кіберзлочинам. Окремо слід зазначити про боротьбу Канади з кібернетичною злочинністю. Підрозділ Королівської канадської кінної поліції, використовуючи показники інформаційного центру та співпрацюючи з іншими країнами, проводить розслідування та розкриття кібернетичних злочинів.

Динаміка формування міждержавних взаємовідносин у питанні співробітництва у боротьбі зі злочинністю завжди вимагала використання або однотипної поведінки переслідування правопорушника за умови співпадіння положень кримінального законодавства договірних сторін, або формування

міжнародного стандарту відповідної протиправної поведінки міжнародно-правовими механізмами. У внутрішньому кримінальному праві склад злочину уособлює протиправну поведінку і являє собою сукупність встановлених карним законом ознак, що характеризують конкретне суспільно небезпечне діяння як злочин. Для забезпечення належного співробітництва держав протиправність поведінки індивіда сприймається як факт і зазвичай криміналізується усіма договірними сторонами. Отже, як міжнародно-правове явище, «злочин міжнародного характеру» — це відповідний стандарт протиправної поведінки індивіда, закріплений нормами міжнародного права і визнаний державами, які приймають участь у міжнародному співробітництві з питань боротьби зі злочинністю [43, с. 94].

На підставі викладеного можна дійти висновку, що сьогодні країнами світу до «кіберзлочинів» застосовуються традиційні принципи кримінальної юрисдикції, засновані на ідеології географічної територіальності. Оскільки технологія сучасних комп'ютерних мереж функціонує поза межами територіального суверенітету та є позатериторіальною за своєю природою, існуючі принципи кримінальної юрисдикції стають неефективними та породжують низку юридичних питань.

Між тим, право на існування має й інший підхід до регулювання правових відносин в мережі Інтернет, пропонується вважати місцем вчинення «кіберзлочину» не територію певної країни або будь-яку іншу географічну територію, а безпосередньо кіберпростір [51, с. 132]. За компетентними прогнозами в недалекому майбутньому можливе стрімке зростання кількості «кіберзлочинів», і передусім таких особливо небезпечних як «кібервійни», «кібертероризм», «кібершпигунство» тощо [51, с. 135]. Прогнозування такого розвитку подій спонукає до пошуку і впровадження адекватних засобів протидії, що мають базуватись насамперед на досягненнях в галузі кримінального права і криміналістики, ґрунтовних наукових дослідженнях міжнародного та національного значення [157, с. 269].

Для України, кіберпростір може стати місцем проведення бойових дій, саме тому проблеми захисту від несанкціонованого доступу стають надзвичайно актуальними. Важливо розширити правову і законодавчу інформованість фахівців та

посадових осіб, зацікавлених у боротьбі з комп’ютерними злочинами. Оскільки, високий ступінь залежності України від імпортних комп'ютерів та інших інформаційних систем, що вже сьогодні створює додаткові ризики організованих хакерських атак, здатних серйозно пошкодити урядові, банківські, енергетичні, транспортні та інші інформаційно-комунікаційні мережі, правове реагування на проблеми посилення комп'ютерної злочинності є надзвичайно важливим. Стимулом цього є також взяті Україною зобов'язання щодо інтеграції в світове співтовариство, в тому числі згідно з Програмою інтеграції України до Європейського Союзу [85, с. 230].

Кібернетичну безпеку визначено сферою національної безпеки. Законом України «Про основні засади забезпечення кібербезпеки України» встановлено принципи забезпечення кібербезпеки, об'єкти та суб'єкти кібербезпеки та кіберзахисту. Визначено національну систему кібернетичної безпеки та розподілено зобов'язання між органами, на які покладено підтримання мирного кібернетичного простору. Цілком природно, що можливості, надані комп’ютерними технологіями, знайшли широке застосування при вчиненні багатьох злочинів [3, с. 1]. Кіберпростір набув величезних масштабів, що стало підґрунтям до розвитку злочинності. Законодавче врегулювання кіберпростору в одній окремо взятій країні не забезпечує дотримання законності в іншій. Тому, вважаємо за необхідне, надати правовому режиму Інтернет статус, аналогічний територіям спільного користування, на нашу думку, це дозволить запровадити відповідальність за протиправні діяння у кіберпросторі згідно з принципом кримінальної юрисдикції, який діє і на інших територіях загального користування. Тобто особа, яка вчинила злочин у кіберпросторі, буде нести відповідальність перед країною свого громадянства, однак це правило може набути чинності лише за умови прийняття універсального зводу правил користування Інтернетом та запровадження принципу обов’язкового співробітництва між країнами у розслідуванні злочинів, що вчиняються у кіберпросторі та підписання міжнародних договорів про співпрацю [91, с. 156].

З метою розкриття ключових аспектів кібернетичної злочинності, перейдемо до видів комп'ютерних злочинів за національним законодавством України.

Інформаційні відносини виникають в усіх сферах життя та діяльності суспільства і держави при одержанні, використанні, розповсюдженні та зберіганні інформації [122]. М.В. Фігель характеризує інформаційні правовідносини, як урегульовані нормами інформаційного права суспільні відносини, учасники яких виступають носіями юридичних прав і обов'язків, що регулюють приписи щодо створення, розподілу та використання інформації, які містяться в цих нормах [172, с. 234].

Найбільшого розвитку у сфері інформаційно-телекомунікаційних систем (**кіберзлочинів**) набули технології, пов'язані з глобальною комп'ютерною мережею Інтернет, що призвело до появи нових категорій, таких як: електронна торгівля, електронний бізнес та навіть електронний уряд [157, с. 262]. Значні переваги Інтернет-технологій для проведення наукових досліджень, електронного бізнесу та комерційної діяльності в інформаційному суспільстві вносять із собою загрози, основна з яких — активне використання злочинним світом нових технологій для шахрайства, крадіжок, «відмивання брудних коштів» тощо [192, с. 101-102].

Кібернетичні злочини мають багатогранний характер — комп'ютерне піратство, комп'ютерний підлог, комп'ютерне шахрайство з даними і програмами, комп'ютерний саботаж, несанкціонований доступ до систем ЕОМ [155, с. 263].

До правопорушень у сфері комп'ютерних технологій відносяться всі протизаконні дії, при яких електронна обробка інформації була знаряддям їх вчинення або предметом. В цілому це:

- незаконне використання комп'ютера з метою аналізу або моделювання злочинних дій для їх здійснення в комп'ютерних системах;
- несанкціоноване проникнення в інформаційно-обчислювальну мережу або масиви інформації з корисливою метою;
- розкрадання системного і прикладного програмного забезпечення;
- несанкціоноване копіювання, зміна або знищення інформації;
- шантаж, інформаційна блокада та інші методи комп'ютерного тиску;
- комп'ютерний шпіонаж і передача комп'ютерної інформації особам, які не мають права доступу до неї;

- фальсифікація комп'ютерної інформації;
- розробка і розповсюдження комп'ютерних вірусів в інформаційно-обчислювальних системах і мережах;
- несанкціонований перегляд або розкрадання інформації з банків даних баз знань і автоматизованих систем;
- недбалість при розробленні, створенні інформаційно-обчислювальних мереж і програмного забезпечення, що призводить до небажаних наслідків і втрати ресурсів;
- механічні, електричні, електромагнітні та інші види впливу на інформаційно-обчислювальні системи та лінії телекомунікації, що викликають їх пошкодження [20, с. 63].

Але цей перелік на сьогоднішній день є невичерпним і постійно збільшується. Комп'ютерні правопорушення в юридичній літературі групуються по-різному, найчастіше в три групи.

До першої групи належать правопорушення, де сам комп'ютер чи інформація у ньому є предметом вчинення протиправних дій.

До другої групи відносять правопорушення, у яких сам комп'ютер виступає у якості знаряддя вчинення злочину.

До третьої групи входять правопорушення, доказом яких є інформація, що міститься в комп’ютерних системах [157, с. 264-265].

Кіберзлочини, як і інформаційні технології постійно вдосконалюються, у зв'язку з чим з'являються нові види злочинних посягань. Деякі вчені під терміном «кіберзлочин» розуміють злочинне діяння, здійснене в мережі Інтернеті, під час якого комп'ютер є або знаряддям, або предметом посягань у віртуальному просторі. З цього випливає безліч типів кібернетичних злочинів: онлайн-шахрайство, наклеп, зневага, екстремізм у мережах, Dos-атаки, дефейс, поширення шкідливих програм. кардерство, комп'ютерне шпигунство та ін. [75, с. 77].

До найбільш розповсюджених видів кібернетичних злочинів можливо віднести: у сфері використання платіжних систем: скімінг (шимінг), кеш-трепінг, кардінг, несанкціоноване списанням коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування; у сфері електронної комерції та

господарської діяльності: онлайншахрайство, фішинг; у сфері інтелектуальної власності: піратство, кардшарінг; у сфері інформаційної безпеки: соціальна інженерія, мальваре, протиправний контент, рефайлінг та ін. [65].

Розглянемо більш детально перелічені види кіберзлочинів.

І. У сфері використання платіжних систем:

1. Скімінг (шимінг) — незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток. З метою заволодіння інформацією з банківських карток злодії можуть записувати дані клієнтів (пін-коди) на замасковані камери. У той же час до щілини, у яку вводять картку, прилаштовують спеціальний мініатюрний пристрій, який зчитує та копіює інформацію про рахунок з магнітної стрічки. Одним з варіантів вчинення такого роду злочинного діяння є накладення на клавіатуру з цифрами точної копії, яка також фіксує пін-код користувача. Отримані дані злочинці переносять на чисті картки («White Plastics»), які зазвичай виготовляють у іншій країні, та привласнюють на власний рахунок грошові кошти. Жертва може навіть не помічати, що в неї викрадають гроші, адже справжня картка залишається у власника.

2. Кеш-трепінг — викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки. З метою вчинення такого роду злочину закривають отвір для видачі грошей в банкоматі спеціальною накладкою (планкою) з липкою стрічкою на іншій стороні. При проведенні громадянами операцій по зняттю готівки здійснюється перезахват купюр — гроші немов приліпають до скотчу, що перешкоджає їх видачі законому власнику карти. У більшості випадках користувачі банкоматів, не отримавши грошей, вирішують, що виникли несправності у роботі, збій чи закінчилася готівка та йдуть не підозрюючи про факт шахрайства, після чого, шахраї забирають готівку.

3. Кардінг — це незаконні фінансові операції з використанням платіжних карток або їх реквізитів, що не ініційовані або не підтверджені її володільцем. Реквізити платіжних карток можуть отримувати з електронно-обчислювальних машин, зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем (або безпосередньо, або через програми віддаленого доступу, наприклад за допомогою

«троянів» або «черв'яків»). Одним з наймасштабніших злочинів в області кардінгу вважається злом глобального процесингу кредитних карт Worldpay та крадіжка за його допомогою даних більше ніж на 9 мільйонів доларів США.

4. Несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування [182, с. 194].

Несанкціонований доступ до електронно-банківських рахунків і модифікація інформації, що знаходиться в них. Так відбувається перерахування коштів на рахунки злочинців. Наприклад, у США збитки від шахрайства з магнітними кредитними картками у 1992 р. перевищили 1 трильйон доларів. Доходи злочинців стоять на третьому місці після доходів від торгівлі наркотиками і зброєю. Коли фінансовими установами Канади було випущено близько 25 мільйонів кредитних карток, правоохоронними органами було встановлено, що з них більше 55 тисяч використовувалося виключно шляхом обману [157, с. 265].

II. У сфері електронної комерції та господарської діяльності:

1. Фішинг — виманювання з користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо. Загалом шахрайські дії звернені на те, аби користувачі-власники інформації самотужки розкрили їм їх вміст, наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів. Фішинг є одним з різновидів соціальної інженерії, який існує завдяки необізнаності користувачів основам комп'ютерної безпеки у мережах.

2. Онлайн шахрайство є заволодінням коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

III. У сфері інтелектуальної власності розповсюдженими злочинами є:

1. Піратство — незаконне розповсюдження інтелектуальної власності в Інтернеті.

Основними видами інтернет-піратства виступають:

- аудіопіратство — копіювання та розповсюдження копій музичних композицій;
- відеопіратство — розповсюдження копій фільмів або телепередач на дисках, касетах та шляхом створення копій;

- піратство літературних творів — незаконне розповсюдження авторських творів;
- піратство комп’ютерних ігор;
- піратство програмного забезпечення — нелегальне копіювання та розповсюдження програмних продуктів на дисках та через комп’ютерні мережі, що включає, також, зняття різноманітних систем захисту від нелегального використання.

2. Кардшарінг — надання незаконного доступу до перегляду супутникового та кабельного TV.

IV. У сфері інформаційної безпеки:

1. Соціальна інженерія — технологія управління людьми в Інтернет просторі;

2. Мальваре — створення та розповсюдження вірусів і шкідливого програмного забезпечення;

3. Протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;

4. Рефайлінг — незаконна підміна телефонного трафіку [183, с. 201].

Новітні технології крокують впевненою ходою, безперечно будуть з'являтися нові види злочинних посягань, до чого слід бути підготовленими. З наданої класифікації очевидно, що **кіберзлочини** не стоять на місці, вони усе частіше пронизують наше життя, яке вже неможливо уявити без інформаційних систем. Найбільшу небезпеку складають злочини IV типу, адже вини безпосередньо направлені на найцінніші людські здобутки — свободу та незалежність. Не можна оминати і загрози, що переховуються — віруси, яких існує безліч, які спроможні нанести непоправну шкоду як інформації, що зберігається на ЕОМ, комп'ютерних мережах, так і самій електронно-обчислювальній машині [192, с. 102-104].

Висновки до розділу 2

1. Виходячи з наявності у Конвенції про кіберзлочинність та Законі України «Про основні засади забезпечення кібербезпеки України» поняття «кіберзлочин(комп'ютерний злочин)», пропонуємо замінити назву Розділу XVI кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» та «Кіберзлочини». З метою уніфікації норма законодавства та уникнення непорозумінь 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, як єдине ціле.

2. Пропонуємо уніфікувати норми, що стосуються кіберзлочинності національного законодавства з нормами законодавства країн-членів Конвенції, що дозволить притягувати дійсних порушників до відповідальності та розробити механізм реалізації даного задуму.

3. Пропонуємо надати правовому режиму мережі Інтернет статус, подібний до статусу територій загального користування.

4. Норми Розділу XVI кримінального кодексу України визначають у більшій мірі відповідальність фізичних осіб, що проживають на території України, проте на нашу думку, їх доцільно доповнити нормами, що передбачають відповідальність держав. Доповнити норми Розділу найбільш розповсюдженими видами міжнародних злочинів, такими як:

— Шахрайство з використанням ЕОМ;

— Нелегальне інформаційне брокерство;

— Порушення авторських прав;

— Кіберпіратство;

— Кібершпигунство;

— Кібервійна. (Додаток **Б**).

5. У зв'язку з появою нових видів комп'ютерних злочинів, норми КК України доцільно доповними такими злочинами:

— У сфері фінансових злочинів: скімінг, кеш-трепінг, кардінг;

— У сфері електронної комерції та господарської діяльності — фішингом;

— У сфері інтелектуальної власності: піратством, кардшарінгом;

— Злочинами у сфері інформаційної безпеки.

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

На сьогоднішній день «комп'ютерні» злочини є однією з найдинамічніших груп суспільно небезпечних посягань світового рівня. Стрімке розповсюдження цих злочинів стало зворотною, негативною стороною інформатизації.

У кримінальному кодексі України містяться норми, прямо пов'язані із використанням комп'ютерних систем, вони розміщені у Розділі XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а саме у статтях 361–363-1 [78]. Норма **статті 361 КК України** передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; **статті 361-1.** Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; **статті 361-2.** Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; **статті 362.** Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; **ст. 363**. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; **ст. 363-1.** Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [78].

Станом на 1 січня 2018 року населення України складало 42 386 403 осіб [178], за даними дослідження Інтернет Асоціації України на 31 січня 2018 року нараховано 25,59 млн користувачів Інтернет [87], тобто 58 % українців є користувачам мережі Інтернет «Додаток **В**». За показниками Державної Судової Адміністрації, згідно зі звітом судів першої інстанції про розгляд матеріалів кримінального провадження за 2017 рік, за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст. 361-363-1 КК) надійшло 79 проваджень [53], згідно зі звітом про склад засуджених за 2017 рік (інформація станом на 1 березня 2018року) (ст. 361-363-1 КК) засуджено 42 особи [53]. Не можна стверджувати, що це були злочини безпосередньо пов'язані з мережею Інтернет, проте можливо допустити, що приблизно половина з них має до них безпосереднє відношення.

Дослідження елементів складу комп'ютерних злочинів дозволить розкрити особливості проведення кримінально-правової кваліфікації кібернетичних злочинів та попередити їх вчинення, тож перейдемо до кваліфікації.

3.1 Об'єкт, предмет злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Стрімкий розвиток злочинності у напрямку комп'ютерних технологій зумовлює необхідність проведення всебічного та глибокого дослідження елементів складів злочинів, та, перш за все, дослідити їх об'єкт та предмет, чому і присвячено 1 главу ІІІ розділу дисертаційного дослідження.

Науковець В.В. Сухонос під об'єктом злочину розуміє суспільні відносини, які перебувають під охороною закону і на які здійснено злочинне посягання, які закріплені у ст. 1 КК України, яка, формулюючи завдання Кримінального кодексу України, практично подає перелік найбільш значущих суспільних відносин, що охороняються кримінальним законом від суспільно небезпечних посягань. Тому, щоб визначити коло цих суспільних відносин, достатньо звернутися до Особливої

частини КК України, яка має вичерпний перелік видів злочинів, у тому числі і їх об’єктів. Інакше кажучи, суспільні відносини, що не підпадають під захист кримінального закону, як правило, регулюються іншими галузями права [165, с. 79]. В.Д. Спасович визнавав об’єктом злочину будь чиє право, яке охороняється державою за допомогою покарання [158, с. 94]. С.Б. Гавриш під об’єктом злочину розумів правове благо як певну цінність, тобто матеріальні явища: життя, здоров’я, гідність, майно, природні об’єкти тощо [37, с. 49, 56].

Найбільш розповсюдженими підходами до визначення сутності суспільних відносин, як об'єкта злочину є:

а) теорія, згідно з якою об'єктом злочину є певно визначені суспільні відносини;

б) теорія, яка виходить з того, що об'єктом злочину є правове благо, інтерес, цінності;

в) теорія, яка об'єднує два попередні вчення.

На нашу думку, об’єктом будь-якого злочину виступають об’єктивно існуючі в суспільстві відносини між людьми, які охороняються на законодавчому рівні, адже їх наслідки можуть завдати шкоду найбільш значущим суспільним відносинам. Встановлення об'єкта злочину з ряду суспільних відносин здійснюється шляхом виділення тих суспільних відносин, які несуть найбільшу соціальну цінність та відіграють найважливішу роль у всій системі суспільних відносин. Соціальна обумовленість кримінально-правової заборони визначається, головним чином, соціальною цінністю суспільних відносин і необхідністю забезпечити їх повну і всебічну охорону.

Відповідно до існуючого у науці кримінального права підходу, об’єкт злочину «по вертикалі» поділяють на: загальний, родовий (видовий) та безпосередній. Деякі автори зазначають про поділ об’єкта по «горизонталі» на основний, додатковий та факультативний [1, с. 44].

До загального об’єкта злочинів, передбачених статтями 361–363-1 КК [78] України, відносять сукупність суспільних відносин як цілісну систему, що охороняється кримінальним законодавством.

Родовим об’єктом даних злочинів є врегульовані законом суспільні відносини автоматизованої обробки інформації (зокрема, забезпечення безпеки її обробки) [25, с. 21]; інформаційні відносини, засобом забезпечення яких є комп’ютери, комп’ютерні системи і мережі, мережі електрозв’язку [60, с. 28]; суспільні відносини у сфері комп’ютерної інформації, зміст яких полягає у здійсненні суб’єктом відносин правомірної інформаційної діяльності щодо предмета цих відносин та обов’язків інших учасників цьому не перешкоджати [1, с. 266]; інформаційна безпека [10, с. 458]. Відповідно до Закону України «Про інформацію» інформаційні відносини виникають у всіх сферах життя і діяльності суспільства й держави при одержанні, використанні, поширенні та зберіганні інформації [122]. До того ж, це мають бути саме інформаційні відносини у сфері комп’ютерної інформації із передбаченим захистом інтересів осіб, а не будь-які інформаційні відносини [78].

Родовим (видовим) об'єктом комп'ютерних злочинів, тобто тим, яким заподіюється основна шкода від злочинів виступає інформація, яка звертається або зберігається в ЕОМ, системах ЕОМ, їх мережах або на машинних носіях. Родовий об'єкт дозволяє проводити класифікацію злочинів за певними групами, сприяє з'ясуванню характеру суспільної небезпеки злочинних діянь, що входять до кожної окремої групи та надає можливість розташувати "законодавчий матеріал " в певній системі.

Точка зору вчених Ю.М. Батурина і А.М. Жодзішского, яка полягає у тому, що родовим об'єктом комп'ютерних злочинів є відносини громадської безпеки є цілком прийнятною [8, с. 30-31]. М.С. Грінберг визначає громадську безпеку, як вид суспільних відносин, який являє собою систему соціальної взаємодії людей, що забезпечує утримання технічних систем в упорядкованому, безпечному стані; вироблення, впровадження і фактичне використання коштів придушення руху даних систем до зменшення порядку, а злочинне зазіхання на ці відносини — як невикористання або недостатнє використання даних коштів [42, с. 35]. Сутність громадської безпеки також розглядалася В.К. Бабаєвим і В.М. Барановим. Вчені визначали громадську безпеку у вигляді сукупності відносин, що врегульовані

юридичними, технічними та організаційними нормами з метою запобігання та усунення загрози життю і здоров'ю людей, матеріальних цінностей та довкілля. За Ю.П. Битяком, В.В. Богуцьким, В.М. Гаращуком громадська безпека залежить від багатьох соціальних чинників, зокрема, стану правопорядку в країні, благоустрою міст, обладнання об’єктів, що призначені для масового відвідування тощо [18, с. 128]. Тож особливість злочинів проти громадської безпеки полягає у тому, що вони завдають шкоду широкому колу суспільних відносин (безпеці особистості, нормальній діяльності підприємств, установ, організацій, безпеці держави та інших соціальних інститутів).

У системі суспільних відносин XXI сторіччя мають місце інформаційні комп'ютерні технології, які певним чином забезпечують підтримку громадської безпеки. Сучасні комп'ютерні технології охопили настільки широке коло суспільних відносин, що майже в кожному розділі КК України є статті про злочини, які можуть бути здійснені (і відбуваються) за допомогою комп'ютерних (інформаційних) технологій. В українському законодавстві наявне визначення поняття «технологія» — це результат науково-технічної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік, строк, порядок та послідовність виконання операцій, процесу виробництва та/або реалізації і зберігання продукції, надання послуг [118, ст. 1]. Проте визначення поняття комп'ютерна технологія закріплене на законодавчому рівні відсутє, проте існує поняття інформаційних технологій. **Інформаційна технологія** є цілеспрямованою організованою сукупністю інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [124, ст. 1]. Тому, досліджуючи злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, доцільно аналізувати й злочини, що трапляються у процесі інформаційних відносин загалом.

Основним безпосереднім об’єктом є відносини, що виникають у зв’язку із здійсненням інформаційних процесів [66, с. 156]: нормальна робота електронно-

обчислювальних машин (ЕОМ), автоматизованих систем (АС), комп'ютерних мереж і мереж електрозв'язку, встановлений порядок їх використання (ст. 361 КК України); нормальна робота обладнання (ст. 361-1, 363-1 КК України); право власності на комп'ютерну інформацію, оскільки головним чинником суспільної небезпечності такого злочину є значущість інформації (ст. 361-2 КК України); встановлений порядок експлуатації ЕОМ, АС, комп'ютерних мереж і мереж електрозв'язку (ст. 363 КК України) [1, с. 47, 52].

Шкода при вчиненні несанкціонованого втручання складається не з приводу комп'ютерної техніки, безпеки або порядку її використання чи безпеки використання мереж електрозв'язку, а з приводу інформації, яка опрацьовується ЕОМ, системами, комп'ютерними мережами, та інформації, яка отримується або передається з використанням мереж електрозв'язку» [66, с. 155-156; 60, с. 54, 127].

Безпосередній об'єкт комп'ютерних злочинів поділяють на:

а) основний – окремо взяті суспільні відносини у сфері комп'ютерної інформації, що виникли та існують з приводу здійснення певною особою (особами) інформаційної діяльності щодо комп'ютерної інформації, та яким завдано істотної шкоди конкретним злочином або які поставлені ним під загрозу заподіяння такої шкоди;

б) додатковий – відносини власності щодо комп'ютерної інформації;

в) факультативний – ті суспільні відносини, у сфері яких здійснюється інформаційна діяльність щодо комп'ютерної інформації [1, с. 266].

Переважна більшість складів злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є матеріальними, а тому виявляються за наслідками.

Під час кваліфікації цих злочинів та їх відмежування від суміжних складів злочинів, необхідно оцінювати розмір та характер заподіяної шкоди з точки зору характеристики її предмету.

Об'єктом злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, наприклад, передбачених **ст. 361 КК** України є «нормальна» робота електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж і мереж електрозв’язку, опосередкованим об'єктом виступає громадська безпека [67]. Сенс норми полягає у тому, що вона забезпечує охорону суспільних відносин двох видів: власності на комп'ютерну інформацію та надання послуг електрозв'язку. Власність на комп'ютерну інформацію є сукупністю прав та можливостей особи: володіти носієм інформації; використовувати інформацію, яка міститься на ньому, для задоволення своєї інформаційної потреби; дозволяти іншим особам використовувати інформацію, яка міститься на його носії, змінювати її, визначати долю носія [49]. Додатковим факультативним об’єктом може бути право власності на комп’ютерну інформацію.

Дії, заборонені статтею **361-1** «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» визнані небезпечними, оскільки вони несуть загрозу для роботи ЕОМ, АС, комп’ютерних мереж і мереж електрозв’язку, а іноді і безпосередньо завдають їм шкоду. Також, внаслідок таких дій створюється програмно-технічний інструментарій для вчинення комп'ютерних злочинів, тому основним об’єктом даного злочину слід вважати нормальну роботу ЕОМ, АС, комп’ютерних мереж і мереж електрозв’язку, а додатковим факультативним об’єктом – право власності на комп’ютерну інформацію.

Об’єктом злочину, передбаченого **статтею 361-2** КК України виступає право власності на комп’ютерну інформацію з обмеженим доступом [67]. Відповідно до Закону України «Про інформацію», інформація з обмеженим доступом може бути конфіденційною, таємною та службовою.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Вона може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Громадяни, юридичні особи, які володіють певною інформацією, самостійно визначають режим доступу до неї, а у разі віднесення її до категорії конфіденційної самостійно встановлюють для неї систему (способи) захисту. Проте не може бути оголошена конфіденційною інформація, приховування

якої являє загрозу життю і здоров'ю людей. Для окремих категорій інформації ВР за поданням КМ може бути встановлено спеціальний правовий режим, який, зокрема, може передбачати і вільний доступ до такої інформації. В окремих випадках статус конфіденційної може бути надано також і інформації, що є власністю держави і знаходиться у користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, за винятком відомостей: про стан довкілля, якість харчових продуктів і предметів побуту; про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян; іншої інформації, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана ВР, не може бути обмеженим.

Таємною є інформація, яка містить відомості, які становлять державну та іншу передбачену законом таємницю (комерційну, банківську, лікарську, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі. Режим доступу до таємної інформації встановлюється законом, який визначає обсяг відомостей, що є державною чи іншою таємницею.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист [122, ст. 21].

Будь-яка інформація є предметом злочину, передбаченого статтею 361-2 КК України лише у тому разі, якщо вона створена на законних підставах і захищена відповідно до чинного законодавства. Захист комп'ютерної інформації від несанкціонованого доступу здійснюється її власником на його розсуд, однак законодавство передбачає випадки, коли певна інформація захищається в обов'язковому порядку із застосуванням спеціально визначених для цього засобів, такими засобами можуть служити паролі, які вимагаються для доступу у відповідну програму, АС чи мережу, програми та пристрої, які здійснюють кодування інформації, програми, які відстежують і блокують несанкціоноване втручання в роботу ЕОМ, АС чи комп'ютерної мережі, спеціальні пристрої, які виключають

можливість негласного одержання інформації за допомогою технічних засобів (наприклад, тих, що працюють на основі фіксації випромінювання працюючого комп’ютера) тощо [67].

Безпосереднім об'єктом злочину, передбаченого статтею **362** КК України є нормальне функціонування електронно-обчислювальних машин (комп’ютерів), автоматизованих систем чи комп’ютерних мереж, комп’ютерної інформації [10, с. 457-473].

Безпосереднім об'єктом злочину, передбаченого статтею **363** та **363-1** КК України виступає нормальне функціонування ЕОМ (комп’ютерів), АС, комп’ютерних мереж чи мереж електрозв’язку [10, с. 470].

Таким чином, виходячи з існуючої структури об'єкта злочину, 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 об'єктом комп'ютерних злочинів виступають врегульовані законом суспільні відносини автоматизованої обробки інформації. 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. З метою глибокого дослідження даної теми, пропонуємо перейти до предмета кібернетичних злочинів.

Охоронювані законом України про кримінальну відповідальність суспільні відносини, що утворюють зміст об’єкта кримінально караного посягання, завжди виникають із приводу певного суспільно значущого інтересу чи блага. У деяких випадках зазначений інтерес має матеріальне (предметне) вираження, тобто наділений певними фізичними ознаками, властивими речам. Суспільні відносини, що виникають із приводу названих елементів матеріального світу, називаються предметними, завдяки тому, що їхньою обов’язковою ознакою є певна річ, тобто предмет. При вчиненні злочинів, що посягають на предметні відносини, винний впливає на окремий предмет, і тим самим заподіює шкоду об’єкту [92, с. 157].

Традиційно предметом злочинів вважається будь-яка річ матеріального світу, з приводу якої або шляхом дії (впливу) на яку вчиняється злочин, проте з урахуванням сучасних тенденцій розвитку суспільних відносин та інформаційного суспільства, цілком доцільно до предмета даних злочинів додати й комп'ютерну інформацію та інші об'єктивні матеріальні утворення [1, с. 266], наприклад, комп'ютерні віруси, програмні та технічні засоби та ін. [40, с. 76-77].

Аналізуючи інформацію, як предмет злочину науковець О.Е. Радутний зазначає, що сьогоденні реалії вимагають визнавати в подальшому під предметом злочину «речі або інші явища об'єктивного світу (інформація, енергія тощо), з певними властивостями яких кримінальний закон пов'язує наявність у діянні особи складу конкретного злочину» [141, с. 10]. Вчений В.Б. Вехов дотримується позиції, відповідно до якої предметом комп'ютерних злочинів є машинна інформація, комп'ютер, комп'ютерна система або комп'ютерна мережа [30, с. 23], з огляду на властивості комп'ютера, які визначаються специфікою його архітектури. Під архітектурою розуміється концепція взаємозв'язку елементів складної структури, що включає в себе компоненти логічної, фізичної та програмної структур. На сьогоднішній день вже використовуються комп'ютери V покоління, відмінною рисою яких є наявність принципу штучного інтеллекта [110, с. 27]. Цікаво й те, що при скоєнні комп'ютерних злочинів використовуючи комп'ютери IV і V поколінь можливе виникнення необхідності у різній кваліфікації одних і тих же злочинів, але скоєних із застосуванням комп'ютерів різних поколінь (наприклад IV і V поколіннь). Основна відмінність між комп'ютерами IV та V поколінь, яка нас цікавить у даному випадку, полягає у швидкості вчинення дій, що може стати у пригоді для швидкого приховування слідів вчинення злочину (більш детально розглянуто в об'єктивній стороні) та наявності принципів штучного інтелекту. **Інтелект** є рівнем розумового розвитку [154], головна особливість штучного інтелекту(ШІ) полягає у розв'язанні задач, для яких практично не існує способів розв'язання, або вони не коректні, наприклад, внаслідок обмеження у часі, або особливості людської пом'яті. Що фактично надає ЕОМ перевагу над людськими здібностями. Штучний інтелект створюється в першу чергу людьми, так що ж заважає їм ввести (закодувати) до

програми штучного інтелекту розроблення та вчинення певних дій, які за законодавством визнані злочинними? — Нічого. На сьогоднішній день інформація про вчинення злочинів комп'ютерами V покоління відсутня, це і не дивно, вони більш досконалі, тому навряд чи про їх вчинення стане відомо, це вже комп'ютерні злочини більш високого рівня, для доказування яких без глибоких знань у галузі програмування та досвіду роботи розв'язати практично неможливо.

Під інформацією слід вважати різноманітні відомості, факти, дані про явища і процеси, що відбуваються в природі і суспільстві, в технічних пристроях і живих організмах [36, с. 26; 177, ст. 200]. На законодавчому рівні затверджено наступне визначення інформації — це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [36, с. 27-28]. Поняття інформації тісно пов'язане з поняттями повідомлення, сигналу, складності, структури і різноманітності. Розрізняють чимало видів інформації.

За змістом інформація поділяється на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- інші види інформації [122, ст. 10].

За режимом доступу:

- відкрита (загальнодоступна);
- обмеженого доступу (конфіденційна, таємна, службова інформація [120]).

За змістом:

- позитивна;
- нейтральна;
- негативна.

Предметом більшості комп'ютерних злочинів виступає комп'ютерна інформація [106, с. 308] або комп'ютерна система (під якою слід розуміти будь-яку із систем: ЕОМ (комп'ютер), автоматизовану систему, комп'ютерну мережу чи мережу електрозв'язку) [28, с. 35], а саме:

1) Електронно-обчислювальна машина (ЕОМ) — комп'ютер — комплекс електронних технічних засобів, які побудовані на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань. Як правило ЕОМ складається із трьох частин: системного блока, який включає в себе мікропроцесор та інші пристрої, необхідні для її роботи (накопичувачі даних, блок живлення тощо), клавіатури, за допомогою якої вводяться в ЕОМ символи, та монітора, на якому відображається текстова і графічна інформація [10, с. 458]. Враховуючи сучасні здобутки науки і техніки, до ЕОМ доцільно додати такі пристрої, як: ноутбук, нетбук, планшет, телефон та ін.;

2) Автоматизовані системи (АС) — системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення. У склад АС входить принаймні одна ЕОМ та периферійні пристрої, що працюють на основі такої ЕОМ: принтер, сканер, модем, мережевий адаптер та ін. АС включають у себе комп'ютерні мережі і мережі електрозв'язку. До того ж. на нашу думку, до складу автоматизованих систем можна включити банкомати та термінали, адже відповідно до Закону України «Про платіжні системи та переказ коштів в Україні», банківський автомат самообслуговування (банківський автомат) — програмно-технічний комплекс, який надає можливість держателю електронного платіжного засобу здійснити самообслуговування за операціями одержання коштів у готівковій формі, внесення їх для зарахування на відповідні рахунки, одержання інформації щодо стану рахунків, а також виконати інші операції згідно з функціональними можливостями цього комплексу [129, ст. 1]. Вчиняється багато

злочинів, пов'язаних з роботою саме банкоматів та терміналів, тому вважаємо за потрібне включити їх до предметів злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж та мереж електрозв'язку.

3) Комп’ютерні мережі (мережа ЕОМ) — це об’єднання кількох комп’ютерів (ЕОМ) і комп’ютерних систем, взаємопов’язаних і розподілених за фіксованою територією орієнтованих на колективне використання загальномережевих ресурсів. Вони передбачають спільне використання ресурсів обчислювальних центрів (ОЦ), запуск загальних програм, що входять до комп’ютерних систем; можуть включати дві чи більше автоматизованих комп’ютерних системи (АКС), як сукупність взаємопов’язаного ЕОМ, периферійного устаткування та програмного забезпечення, призначених для автоматизації прийому, збереження, обробки, пошуку та видачі інформації споживачам. Комп’ютерні мережі можуть бути регіонального і галузевого характеру [10, с. 458-459];

4) Мережі електрозв’язку — це сукупність технічних засобів та споруд зв’язку, об’єднаних у єдиний технологічний процес забезпечення інформаційного обміну — маршрутизації, комунікації, передачі, випромінювання або прийому знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах (телефонний, телеграфний, телетайпний та факсимільний зв’язок).

Предмети мережі електрозв’язку включають: телефони, факси, телетайпи, телеграфи, інші апарати, пристрої і обладнання мереж електрозв’язку, призначені для передачі й обміну інформацією;

5) Комп’ютерна інформація може бути у різних формах фіксації: текстовою, цифровою, графічною чи іншого виду (дані, відомості) про осіб, предмети, події, явища, що існують в електронному вигляді і знаходиться в ЕОМ, АС чи в комп’ютерній мережі, а також зберігається на відповідних електронних носіях, до яких належать гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти та ін., така інформація носіїв може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп’ютерів);

6) Враховуючи, що одним з різновидів мереж електрозв'язку виступають комп'ютерні мережі, то інформація, що передається мережами електрозв’язку (телекомунікаційними мережами) — будь-які відомості, подані у вигляді сигналів, знаків, звуків, зображень чи в інший спосіб (телефонні повідомлення, радіо- та телепередачі тощо), у тому числі і за допомогою комп’ютера, якщо вона передається через мережі електрозв’язку [10, с. 459; 66, с. 156]. Така інформація, що передається мережами електрозв’язку, може бути предметом даних злочинів лише тоді, коли цими мережами передається комп’ютерна інформація від однієї комп’ютерної системи до іншої [1, с. 103, 104; 60, с. 58]. Саме злочинний вплив на ці предмети або їх злочинне використання дає підстави визначити наявність об’єкту цих злочинів, тому що вони є невід’ємною частиною охоронюваних розглядуваними нормами суспільних відносин [28, с. 35].

Якщо розглядати предмет комп'ютерних злочинів взагалі, то одним з них виступає саме інформація, під якою розуміються відомості про осіб, предмети, факти, події, явища і процеси зафіксовані на машинному носії, в ЕОМ, системі ЕОМ або їх мережах. Конкретизуючи предмети злочинів, відповідальність за які передбачена статтями 361, 361-1, 361-2, 362, 363, 363-1 слід зазначити, що предмети тут дещо відрізняються.

Предметом злочинних посягань несанкціонованого втручання у роботу автоматизованих електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку (**ст. 361** КК України), згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», можуть бути:

а) інформація, що обробляється в системі;

б) програмне забезпечення, яке призначено для обробки цієї інформації [121, ст. 2].

До предметів злочину, передбаченого ст. 361 КК, відносяться комп'ютерна інформація та інформація, що передається каналами зв'язку. Проаналізуємо поняття «інформація», «комп'ютерна інформація» та «інформація, що передається мережами електрозв'язку».

Інформація — відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [139, ст. 1].

Комп'ютерна інформація — відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну.

Інформацією, що передається мережами електрозв'язку, є відомості, подані у формі, що дозволяє їх приймати або передавати засобами електрозв'язку [49].

Отже, виходячи з вищезазначених понять, інформація може мати різну форму, до того ж, виступати предметом комп'ютерних злочинів вона буде, якщо внаслідок певних дій комп'ютерів, систем, комп'ютерних мереж і мереж електрозв'язку з цією інформацією відбулися непоправні дії. які порушили права суб'єктів обігу такої інформації (фізичні, юридичні особи, організації та ін.).

Якщо дивитися у корінь статті 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», можна дійти до висновку, що предметами злочину вважаються:

1) електронно-обчислювальні машини (комп’ютери, ЕОМ);

2) автоматизовані системи (АС);

3) комп’ютерні мережі;

4) мережі електрозв’язку [49], проте це не так, адже ключову роль відіграє саме інформація, яка обертається у зазначених елементах.

Предметом злочину передбаченого ст. **361-1** «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» є один із різновидів комп'ютерної інформації — комп'ютерні програми — шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп’ютерів), автоматизованих систем, комп’ютерних мереж та мереж електрозв’язку.

Згідно з Законом України «Про авторське право і суміжні права» **комп’ютерні програми є** набором інструкцій у вигляді слів, цифр, кодів, схем, символів чи у

будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату [117]. Предметом злочину, передбаченого статтею 361-1 Кримінального кодексу України повинні бути саме шкідливі комп’ютерні програми (програмні засоби), тобто здатні забезпечити несанкціонований доступ до інформації, а також змінити, знищити, пошкодити, заблокувати комп’ютерну інформацію чи ту, яка передається мережами електрозв’язку [10, с. 464]. Шкідливі програмні та технічні засоби, операції з якими заборонені, можуть мати вигляд шкідливих комп’ютерних програм або ж технічних пристроїв, які працюють з використанням таких програм [145, с. 90].

Найбільш розповсюдженими видами шкідливих програмних засобів є:

1. комп’ютерні віруси – комп’ютерні програми, здатні після проникнення до операційної системи ЕОМ чи до АС порушити нормальну роботу комп’ютера, АС чи комп’ютерної мережі, а також знищити, пошкодити чи змінити комп’ютерну інформацію;
2. програми, призначені для нейтралізації паролів та інших засобів захисту комп’ютерних програм чи комп’ютерної інформації від несанкціонованого доступу;
3. програми-шпигуни, які після їх проникнення до певної АС, комп’ютерної мережі, операційної системи ЕОМ чи окремої комп’ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається у ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі [67].

Шкідливими програмними засобами є прилади, обладнання, устаткування, за допомогою яких вчинюється несанкціонований доступ до ЕОМ чи АС. Такі засоби здатні призвести до витоку, втрати (знищення), підробки (фальсифікації), блокування інформації, спотворення процесу її обробки, що функціонує в ЕОМ, автоматизованих системах, комп’ютерних системах чи мережах електрозв’язку, або до порушення встановленого порядку її маршрутизації [10, с. 464-465]. Одним з

різновидів шкідливих комп’ютерних програм є комп’ютерні віруси. **Програма-вірус** — це спеціально створена програма, яка здатна сама приєднуватись до інших програм (тобто пристосовуватись і «заражати» їх) і, наприклад, при запуску спричиняти різні негативні наслідки: псування файлів і каталогів, перекручування інформації, у тому числі результатів обчислення, засмічення чи спотворення пам’яті ЕОМ, створювати інші перешкоди у роботі ЕОМ чи АС.

Програма, що містить комп'ютерний вірус, має реальну і дуже високу ступінь можливості знищення, блокування, модифікації комп'ютерної інформації, порушення роботи ЕОМ, їх систем або мереж. Тому поширення комп'ютерного вірусу («злам» комп'ютерних систем і мереж за допомогою «вірусної атаки») становить підвищену небезпеку для суспільних відносин у сфері комп'ютерної безпеки [102].

Однією з **програм, призначених для нейтралізації паролів** та інших засобів захисту комп’ютерних програм чи комп’ютерної інформації від несанкціонованого доступу є програма "кейлоггер", вона ж програма для «відновлення» паролів поштових облікових записів, та по виконуваним функціям і є **програмою-шпигуном**. Суть якої полягає у тому, що у спеціальний файл він записує усе, що користувач вводить з клавіатури, включаючи й паролі облікових записів. Проте така програма має і недоліки, наприклад, — визначення антивірусами; запис великої кількості інформації.,адже зловмисникам частіше за все потрібно ще відшукати серед усього «зайвого» те, що потрібно - паролі. Якщо жертва використовує поштовий клієнт, а не веб-інтерфейс, то кейлоггер не допоможе, адже пароль вже введено до пошти клієнтом і його запам'ятовано, тому жертва не вводить його щоразу при перевірці, наприклад, пошти. Він має ще один недолік — якщо обраний кейлоггер не підтримує відправку результуючого файлу по e-mail, то необхідно буде ще раз наближатися до комп'ютера, проте це є і перевагою для добропорядних громадян, виступаючи засобом захисту від шахраїв.

Програми для «відновлення» паролів поштових облікових записів дозволяють відразу отримати всі паролі без необхідності читання мегабайтів тексту в пошуку потрібного пароля і на них не реагує антивірус. Однією з таких програм є Mail

PassView, яка дозволяє відновити паролі поштових облікових записів: Outlook Express, Microsoft Outlook 2000 (POP3 and SMTP Accounts only), Microsoft Outlook 2002/2003/2007/2010/2013 (POP3, IMAP, HTTP and SMTP Accounts), Windows Mail, IncrediMail, Eudora, Netscape 6.x / 7.x, Mozilla Thunderbird, Group Mail Free, Yahoo! Mail - якщо пароль збережений в додатку Yahoo! Messenger., Hotmail / MSN mail — якщо пароль збережений в додатку MSN Messenger., Gmail — якщо пароль збережений в додатках Gmail Notifier, Google Desktop або Google Talk. До того ж, Mail PassView — не єдина програма в своєму роді, існують й інші програми: Outlook Password Decryptor — дозволяє відновлювати паролі з Outlook, у тому числі самих останніх версій (Outlook 2015 року, що працює під управлінням Windows 10); PstPassword — програма для відновлення паролів, збережених в Outlook; WebBrowserPassView — програма для відновлення паролів, що зберігаються в браузері. Підтримуються браузери IE, Chrome, Opera, Safari, Firefox. Все, що потрібхідно — знати, який поштовий клієнт використовує жертва [187]. Такі практичні поради можна зустріти на кожному другому сайті.

За допомогою таких засобів можливо переглядати особисту інформацію іншої людини або й стежити за нею за допомогою спеціального розширення через веб-камеру. Відповідно до статті 31 Конституції України: " Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігання злочинові чи з'ясування істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо"; статті 32: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [70, ст. 31, 32]. Кримінальним кодексом України передбачено покарання за втручання у особисте життя людини, згідно зі статтею 163 КК України: «Порушення таємниці листування, телефонних розмов,

телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, — караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років. Ті самі дії, вчинені повторно або щодо державних чи громадських діячів, журналіста, або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, — караються позбавленням волі на строк від трьох до семи років». Відповідно до норми статті 182 КК: «Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями КК України караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк» [78].

Таким чином, незаконне збирання, зберігання конфіденційної інформації про особу підпадає під кваліфікацію за статтею 182 КК. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, якщо це не призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації підлягає кваліфікації за ст. 163 КК України. Тобто, комп'ютерна техніка та інформаційні ресурси у таких випадках виступають засобами вчинення даного злочину.

Обов’язковою ознакою предметів розглядуваного злочину є те, що їх призначення полягає у несанкціонованому втручанні в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Відсутність цієї ознаки виключає можливість

визнати вказані програмні чи технічні засоби предметом злочину, передбаченого ст. 361-1 КК [10, с. 465].

Таким чином, під шкідливою програмою, слід розуміти такий програмний засіб, який було створено для виконання несанкціонованих власником та іншими законними власниками інформації, ЕОМ, системи ЕОМ або їх мережі функцій. Під небажаними функціями мається на увазі несанкціоноване знищення, блокування, модифікація або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мереж, а також виведення з ладу системи захисту інформації.

Предметом злочину передбаченого статтею **361-2** «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» виступає інформація з обмеженим доступом, яка зберігається в ЕОМ, АС, комп'ютерних мережах або на носіях такої інформації, тобто комп'ютерна інформація з обмеженим доступом [67] (про інформацію з обмеженим доступом див. у п. 1.1.1 Розділу 3).

Інформація з обмеженим доступом як предмет злочину має зберігатися на ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах. До того ж, інформація, яка зберігається в мережах електрозв'язку, до предмета даного злочину не належить. Ознакою такої інформації є її створення та захист відповідно до чинного законодавства [10, с. 466-467].

Предметом злочину передбаченого **ст. 362** КК «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» виступає інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Ознакою предмета цього злочину є те, що ця інформація обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах. Обробкою інформації є виконання певних дій за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи

комп’ютерних мереж, які включають у себе різні види маніпуляцій з такою інформацією згідно з відповідними комп’ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ і т. ін. та зберігання такої інформації.

Предметом даного злочину є також і інформація, яка зберігається на носіях цієї інформації [10, с. 468].

Предметами злочинів відповідно до ст. **363** та ст. **363-1** КК визначено ЕОМ (комп’ютери), АС, комп’ютерні мережі, мережі електрозв’язку, комп’ютерну інформацію та інформацію, яка передається мережами електрозв’язку.

Під час проведення кримінально-правової кваліфікації важливо розмежовувати предмети і знаряддя скоєння злочину. Знаряддями і засобами вчинення злочину є предмети матеріального світу, які за своїми об'єктивними властивостями можуть бути використані для вчинення злочину незалежно від того, мали вони такі властивості з самого початку чи були відповідним чином пристосовані винною особою. Ці предмети можуть бути призначені тільки для реалізації злочинного наміру або ж використовуватись і для досягнення інших, незлочинних, цілей. Знаряддя і засоби є обов'язковою ознакою об'єктивної сторони складу злочину, якщо вони вказані у диспозиції статті Особливої частини КК або їх визначення випливає з неї [100].

Наукою кримінального права розроблені такі правила розмежування знарядь і засобів вчинення злочину від предмета злочину, які мають застосовуватись у сукупності:

1) знаряддя і засоби є "активними" ознаками злочину, тобто завжди використовуються злочинцем для досягнення певного результату;

2) знаряддя і засоби не підлягають впливу з використанням предмета злочину, останній є "пасивним" — на нього спрямовано діяння злочинця;

3) властивості предмета, як правило, передбачається використовувати у більш-менш віддаленому майбутньому, а властивості знарядь і засобів завжди використовуються злочинцем при вчиненні злочину;

4) якщо предмет злочину вказує на охоронювані кримінальним законом відносини, а також характеризується злочинним впливом на нього у вигляді діяння, то знаряддя і

засоби, навпаки, характеризують дії злочинця і не перебувають у взаємозв'язку з охоронюваними КК відносинами;

5) знаряддя і засоби залежать від наявності предмета або потерпілого від злочину, і, навпаки, предмет злочину не залежить від наявності тих чи інших знарядь і засобів вчинення злочину;

6) предмет злочину виділяється у складах злочинів з будь-якою формою вини, у той час, як знаряддя і засоби — лише у складах умисних злочинів.

Одні і ті самі предмети матеріального світу при вчиненні різних злочинів можуть виступати або у якості предмета, або у якості засобу чи знаряддя. Підхід більшості фахівців полягає у тому, що чужі для об'єктів кримінально-правової охорони предмети або, інакше кажучи, вилучені "антиблага" є не засобами вчинення відповідних злочинів, а їх предметами [100].

Якщо предмет злочину — це те, на що впливає злочинець, то знаряддя — це предмети, за допомогою яких вчиняється злочинне діяння [92, с. 158]. Розмежування можливо проводити за характером використання речей та інших предметів в процесі вчинення злочину. Якщо це використання має активний характер — предмет використовується, як інструмент впливу на об'єкт, то перед нами знаряддя або засіб скоєння злочину. Навпаки, якщо над річчю здійснюється дія, вона "зазнає" впливу (знищується, вилучається, змінюється і т.д.), то ця річ повинна бути визнана предметом злочину [173, с. 225]. З'ясування знарядь вчинення злочину необхідно для того, аби відмежувати комп'ютерні злочини від зовні схожих протиправних діянь, тобто, якщо шкода буде завдана безпосередньо ЕОМ, за умови, що існуючій на ній інформації не буде завдана шкода, даний злочин доцільно розглядати відповідно до норм розділу VI «Злочини проти власності» КК України.

Таким чином, у комп'ютерних злочинах машинна інформація може виступати як у якості предмета, так і у якості знаряддя вчинення злочину. Предметом комп’ютерних злочинів виступає комп’ютерна інформація та комп’ютерні системи. До предмету злочину, передбаченого ст. 361 КК, відносяться комп'ютерна інформація та інформація, що передається каналами зв'язку; інформація, що перебуває у обігу електронно-обчислювальних машин (комп’ютерів, ЕОМ);

інформація, що міститься у автоматизованих системах (АС); передається по комп'ютерним мережам та мережам електрозв'язку. Предметом злочину передбаченого ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» є шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку. Предметом злочину передбаченого статтею 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації» виступає інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, системах, комп'ютерних мережах або на носіях такої інформації. Предметами злочинів відповідно до ст. 363 та ст. 363-1 КК визначено ЕОМ (комп'ютери), АС, комп'ютерні мережі, мережі електрозв'язку, комп'ютерну інформацію та інформацію, яка передається мережами електрозв'язку.

3.2 Об'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Об'єктивна сторона злочину є зовнішньою стороною соціально небезпечного посягання, яка характеризується діями, наслідками, причинно-наслідковими зв'язками між ними, вчиненими за певних умов, місці та часі. При виявленні злочину визначається чи призвела діяльність суб'єкта, в певному об'єктивному середовищі, при певному місці і часі, до порушення прав осіб, у нашому випадку, у сфері кібернетичних відносин.

Відповідно до Конвенції про кіберзлочинність об'єктивна сторона комп'ютерних злочинів характеризується виокремленням чотирьох груп суспільно небезпечних діянь, а саме:

А) проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, до числа яких можна віднести:

- одержання доступу до комп'ютерної системи чи її частини без права на це, якщо його було вчинено шляхом оминання заходів безпеки зі злочинним наміром, наприклад, з метою заволодіння особистими даними, або по відношенню до комп'ютерних систем, які об'єднані між собою;
- протизаконне перехоплення даних, здійснюване з використанням технічних засобів без права на це;
- порушення цілісності даних без права на це, якщо такі діяння потягли за собою серйозні наслідки: зміну, псування, пошкодження, блокування чи стирання комп'ютерних даних;
- створення перешкод функціонуванню комп'ютерної системи шляхом введення, передачі, ушкодження, видалення, псування, зміни чи блокування комп'ютерних даних;
- протиправне використання пристроїв:

а) виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми використання пристроїв (включаючи комп'ютерні програми, розроблені чи адаптовані, насамперед для цілей здійснення злочинів), комп'ютерних паролів, кодів доступу чи інших подібних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частині, з наміром використовувати їх з метою здійснення злочинів;

б) володіння одним із вищезазначених предметів, з наміром використання їх із злочинним наміром;

Б) пов'язані з використанням комп'ютерів [157, с. 262-270]:

- підробка з використанням електронно-обчислювальних машин — введення, зміна, стирання, блокування комп'ютерних даних, що призвело до порушення автентичності даних;
- шахрайство з використанням комп'ютерів — позбавлення осіб їх власності шляхом введення, зміни, стирання, приховування комп'ютерних даних чи втручання у

функціонування комп'ютера чи системи з метою неправомірного одержання економічної вигоди для себе чи інших осіб;

В) пов'язані із змістом даних:

- правопорушення, пов'язані з дитячою порнографією (порнографічні матеріали, що візуально відображають участь неповнолітнього чи такого, який удавав з себе неповнолітньою особою, у сексуально відвертих діях; реалістичні зображення, що представляють неповнолітніх, що приймають участь у сексуально відвертих діях), а саме: виробництво з метою розповсюдження через комп'ютерні системи; пропозиції чи представлення через комп'ютерні системи; придбання через комп'ютерну систему для себе чи для іншої особи; володіння дитячою порнографією, що знаходиться у комп'ютерній системі чи в середовищі для збереження комп'ютерних даних.

Г) пов'язані з порушенням авторських і суміжних прав:

- порушення авторського права, передбаченого нормами внутрішньодержавного законодавства, відповідно до Закону України «Про авторське право і суміжні права» [117], з урахуванням вимог Паризького акта від 24 липня 1971 року до Бернської конвенції про захист творів літератури і мистецтва [14], договору про авторське право Всесвітньої організації інтелектуальної власності (ВОІВ) [46], за виключенням будь-яких моральних прав, наданих цими конвенціями, коли такі дії навмисно відбуваються в комерційному масштабі і за допомогою комп'ютерної системи;

- порушення прав, пов'язаних з авторським правом (суміжних прав), передбачених нормами внутрішньодержавного законодавства, з урахуванням вимог: Міжнародної конвенції про захист прав споживачів, виробників звукозаписів і радіомовних організацій (Римська конвенція) [93], Про захист прав споживачів в дистанційних контрактах [45], Договору ВОІВ про виконавців і звукозаписи, за винятком будь-яких моральних прав, що представляються цими конвенціями, коли такі дії відбуваються навмисно в комерційному масштабі і з використанням комп’ютерної системи.

Об’єктивна сторона кібернетичних злочинів може виражатися як в активних діях (наприклад, при несанкціонованому втручанні в роботу електронно-

обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) — ст. 361 КК або у злочинній бездіяльності (наприклад, при порушенні правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, — ст. 363 КК) [10, с. 460]. Отже, 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) тощо [28, с. 35].

В залежності від розміру завданої шкоди, встановлюється наявність складу злочину, наприклад, злочин, передбачений ст. 363 КК України, вважається закінченим, лише якщо було заподіяно саме значну шкоду, а при наявності такого ж розміру шкоди при вчиненні злочину, передбаченого ст. 361 КК України, кваліфікацію слід проводити за ч. 2 цієї статті. Шкода у статтях 361–363-1 КК України може полягати у заподіянні матеріальних збитків, які оцінюються, виходячи з витрат власника на придбання комп'ютерної інформації, пропорційно до зниження цієї вартості, спричиненої злочином, або виходячи з вартості компонентів комп'ютерної системи (програмних чи технічних), які зазнали негативного злочинного впливу, або виходячи із витрат на відновлення комп'ютерної інформації чи компонентів комп'ютерної системи. Також збитки комп'ютерних злочинів можуть виражатися в упущеній вигоді, що є результатом, наприклад, укладання завідомо невигідної угоди, зниження авторитету, невиконання умов договорів [28, с. 36; 73, с. 144]; у порушенні нормальної роботи підприємств (установ чи організацій), зупиненні або порушенні технологічних процесів, навіть призвести до зниження обороноздатності держави, підриву авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю чи здоров'ю громадян та ін.

На нашу думку наслідки до яких можуть призвести кібернетичні злочини залежать саме від змісту комп’ютерної інформації, яка зазнала шкоди. До того ж, характер шкоди в кожному конкретному злочині, залежить від тих суспільних відносини, які виступають не основним безпосереднім, а додатковим об’єктом.

Важливе значення для доведення комп'ютерних злочинів мають сліди, які, загалом, рідко залишаються у вигляді видимих змін навколишнього середовища та у більшості випадках є змінами комп’ютерної інформації, що виражається у формі її блокування, копіювання, модифікації чи знищення [48, с. 263]. Сліди комп’ютерних злочинів, називають по різному: «віртуальні сліди», «сліди засобів комп’ютерної техніки», «інформаційні сліди» [48, с. 264]. Проте, при вчиненні комп’ютерних злочинів утворюються і традиційні — матеріальні сліди. Вони мають опосередкований характер, адже вони не завжди мають яскраво виражений характер, а тому часто відсутні дані про місце скоєння злочину, але відоме місце настання протиправних наслідків. У більшості випадках вони залишаються на ЕОМ (комп’ютерних) магнітних носіях інформації і відображають зміни даних інформації, що зберігається (сліди модифікації баз даних, програм, текстових файлів на твердих дисках, дискетах, магнітних стрічках, лазерних і магнітооптичних дисках) [167, с. 65]; роздруківки тексту, графічного малюнка або схеми, компакт-диски з інформацією, віртуальні образи, інформація на радіохвилях, в інфрачервономих променях, уявний образ зображення тощо [167, с. 265]. При вчиненні комп’ютерного злочину утворюється індивідуальна слідова картина. Зазвичай, сутність комп’ютерних слідів обумовлює труднощі при їх виявленні та дослідженні, а також при використанні в доказуванні [48, с. 265].

Характер злочинних наслідків та їх розмір залежать від особливостей діянь та умов, за яких вони вчиняються. Як показує практика, основним знаряддям вчинення кібернетичних злочинів є саме інформаційні технології.

Характер діянь, які вчиняються у сфері використання ЕОМ (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку дозволяє виокремити щонайменше **шість моделей злочинного посягання**:

1. Якщо наслідки спричинені діями особи, яка не мала права доступу до комп'ютерної інформації — ці дії мають явні 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, ці дії слід кваліфікувати за ст. 361 КК України [28, с. 37-38]. Доступ до комп'ютерної інформації без подолання засобів захисту; дії, що призвели до наслідків, зазначених в 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. 361-1КК 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) [66, с. 157]. Якщо наслідки спричинені діями особи, яка мала право доступу до комп'ютерної інформації, але не мала права вчиняти з нею певні дії — змінювати, знищувати, блокувати, перехоплювати або копіювати її, такі дії слід кваліфікувати за ст. 362 КК України.

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 вчинені з порушенням правил експлуатації або

порядку чи правил захисту інформації, яка в них оброблюється, то таке діяння повинне 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 слід кваліфікувати за ст. 363-1 КК України.

Злочини, склади яких відносяться до формальних (статті 361-1 та 361-2 КК України), найчастіше виявляються в ході розслідування інших злочинів, або шляхом отримання правоохоронними органами інформації від заявників, які не є потерпілими від злочину, чи з інших джерел [28, с. 38].

Цікавим залишається і те, що розповсюдження «СПАМу», в силу того, що такі діяння не порушують і не припиняють роботу ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку; масове розповсюдження мережами електрозв'язку сигналів, які не містять для когось певних відомостей, що призвело до порушення або припинення роботи ЕОМ (комп'ютерів); діяння, що призводить до спотворення процесу обробки інформації (щодо ст. 363-1 КК України) [66, с. 157] не є злочинами, адже зазначені діяння не містять у собі підвищеної суспільної небезпеки. До того ж відсутність на підприємстві, установі чи організації правил, які регламентують порядок роботи з ЕОМ, АС, комп'ютерними мережами та мережам електрозв'язку, відсутність порядку і правил захисту недержавної інформації, виключає наявність у діяннях особи складу злочину, передбаченого ст. 363 КК України [1, с. 6]. Для отримання підтвердження ознак певного виду злочину слід провести слідчі (розшукові) дії (огляд, обшук), в необхідних випадках — негласні (контроль за вчиненням злочину). Під час яких оцінити дії осіб, що підозрюються або їх результати на предмет наявності в них ознак об'єктивної сторони певного складу злочину (збут, розповсюдження шкідливих програмних чи технічних засобів або інформації з обмеженим доступом) [28, с. 38].

З метою більш детального дослідження об'єктивної сторони злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пропонуємо перейти до особливостей, притаманних окремим злочинним діянням передбачених КК України.

Об'єктивна сторона злочину є одним з необхідних елементів складу злочину, який характеризує зовнішній прояв злочину та його наслідків у світі. Аналіз показників злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за показниками 2017 року показав, що найбільшу кількість складають злочини передбачені саме нормою статті 361 КК України (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [53].

Доцільно розтлумачити зміст **несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**, — це самочинне, без дозволу власника або уповноваженої особи проникнення у електронні системи чи мережі [10, с. 461]. З цього слідує, що об'єктивна сторона злочину, відповідальність за який передбачена **ст. 361 КК України**, виходячи з норми диспозиції, полягає у неправомірному доступі до охоронюваної законом комп'ютерної інформації, якщо це діяння призвело до знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі.

При тлумаченні об'єктивної сторони має сенс розглянути її складові частини, якими у даному випадку є:

1) дія у вигляді несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

2) суспільно небезпечні наслідки у формі: витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації;

3) причинний зв'язок між дією та зазначеними наслідками [10, с. 461].

Саме тому, для визнання факту вчинення злочину, склад якого передбачено статтею 361 КК, суд має встановити не лише вчинення діяння, а й настання хоча б одного із зазначених в законі наслідків: витоку, втрати, підроблення, блокування

інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації, тобто встановити причинний зв’язок [164].

Неправомірний доступ до комп'ютерної інформації здійснюється шляхом вивчення дій. Об'єктивна сторона злочину полягає в двох формах:

1) у незаконному втручанні в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж;

2) у несанкціонованому втручанні в роботу мереж електрозв'язку.

Під незаконним втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж вбачається таке втручання, відповідно до якого особа не мала ні дійсного, ні передбачуваного права тта за умов, що електронно-обчислювальні машини не належать винному ні на праві власності, ні на якій-небудь іншій законній підставі (наприклад, на умовах оренди). Як показує практика. у більшості випадках має місце злам і проникнення (вторгнення) у програму чужого комп'ютера, системи або мережі ЕО [102].

Видається цікавою точка зору, висловлена Є.І. Панфіловою та А.С. Поповим, які під неправомірним доступом до комп'ютерної інформації розуміють — незаконне отримання можливості маніпулювати інформацією, тобто сприймати її, збирати, обробляти, накопичувати, аналізувати, зберігати, шукати, поширювати і здійснювати з нею інші дії, при відсутності на це у винного дійсного або гаданого права [107, с. 28]. В.А. Бессонов під доступом до комп'ютерної інформації пропонує розуміти "санкціоновану і упорядковану власником інформаційної системи взаємодію особи з пристроями ЕОМ, з подальшою будь-якою формою проникнення до інформації з можливістю ознайомлення з нею або без такого, що дозволяє нею маніпулювати" [15, с. 20]·. Нам вбачається, що під неправомірним доступом до комп'ютерної інформації слід вважати несанкціоноване власником комп'ютерної інформації проникнення до неї з можливістю розпорядження (знищення, блокування, змінення, копіювання), що призводить до непоправних пошкоджень іонформації чим створює небезпеку інтересам власника такої інформації. На сьогоднішній день на законодавчому рівні відсутнє поняття «неправомірний доступ», але існує думка, що для визнання доступу неправомірним, необхідно, аби

інформація була захищена від довільного копіювання, проте даний аспект не є обов'язковою ознакою складу злочину передбаченого ст. 361 КК України [34, с. 71]. Особиста інформація, доступ до якої закрит, наприклад, поштова електронна скринька, листи якого не підлягають розголошенню і є конфеденційною інформацією. У разі потреби у захисті від довільного копіювання інформації, це можливо зробити за допомогою шифрування, однак це не впливає на кваліфікацію даного злочину, а є лише додатковим засобом захисту.

У зв'язку з тим, що злочин сконструйовано за матеріальним складом, для його наявності слід встановити не тільки вчинення діяння, а й настання хоча б одного з вказаних у законі наслідків: витоку, втрати, підробки (зміни, модифікації), блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації.

З метою поглибленого дослідження об'єктивної сторони злочинного діяння розглянемо більш детально перелічені наслідки. Витік інформації має місце, коли стає відомою (доступною) хоча б одній особі, яка не мала на це права, наприклад, у наслідок ознайомлення з її змістом, шляхом копіювання, навіть якщо власник не позбавляється інформації, яка йому належить.

Втрата інформації є припиненням існування інформації відносно осіб, які мають право власності на неї. Втрата інформації може бути результатом її знищення, «викрадання», внаслідок чого власник позбавляється належної йому інформації [10, с. 461-463]. На нашу думку, знищення є процесом, внаслідок якого інформація не може бути відновлена; натомість стиранням є видалення інформації, з можливістю її відновлення.

Підробкою інформації є дії, що призводять до перекручення (модифікації) змісту інформації, яка обробляється в ЕОМ чи АС, або створення інформації, що за змістом не відповідає дійсності (фальсифікація інформації).

Під модифікацією комп'ютерної інформації слід розуміти несанкціоновані зміни її початкового стану, наприклад, внесення змін до змісту інформації аби її зміст став інакшим або й взагалі призводив до порушення виконання нею певних функцій. Конвенцією про кіберзлочинність передбачено кримінальну

відповідальність країн, у разі навмисного вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерної інформації, що призводить до створення недійсних даних, це проводиться аби вони вважались/відповідно до них проводились законні дії(як з дійсними), незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Для встановлення кримінального покарання сторона може навіть вимагати наявності наміру обману або подібної нечесної поведінки країни-порушника [69, ст. 7; 136].

Блокуванням інформації є таке порушення інформаційних потоків мереж електрозв'язку, внаслідок чого суб'єкт, що передає інформацію не може донести її до абонента, а той, відповідно, не може отримати таку інформацію. Блокування інформації має місце у випадках, коли внаслідок несанкціонованого втручання в роботу ЕОМ та АС власник чи уповноважена особа не має доступу до інформації, не отримує її і не має можливості користування нею. Тут може мати місце приховування чи стримування інформації для запобігання користуванню нею в процесі її обробки. За умови, що внаслідок блокування здійснення нею своїх функцій, стає неможливим, яке може бути як постійним, так і тимчасовим, або ж залежити від застосування спеціальних засобів.

Під спотворенням процесу обробки інформації розуміється зміна послідовності обробки інформації, тобто, може порушуватись порядок: збирання, ведення, записування, перетворення, зчитування, знищення, реєстрація, прийняття, отримання, передавання інформації, внаслідок чого одержується інший результат, ніж очікувався [10, с. 461-463].

Маршрутизація інформації є порушенням обрання послідовності вузлів мережі передачі інформації, якою інформація передається від джерела до приймача інформації [102]. Порушення встановленого порядку маршрутизації є протиправним, внаслідок несанкціонованого втручання, зміненням адресата інформації, яка передається телекомунікаційними каналами, унаслідок чого адресат не отримує інформації, яка була для нього направлена, або таку інформацію отримують і інші особи, яким ця інформація не була адресована [10, с. 461-463].

Якщо невиконання комп'ютером охорони інформації від несанкціонованого доступу вважати порушенням роботи ЕОМ, то проблема безкарності за порушення захисту інформаційних ресурсів стає вирішуваною. Тоді несанкціонований обхід програмних засобів захисту інформації можна вважати закінченим складом ст. 361 КК України, а невдалу спробу несанкціонованого проникнення до охоронюваної законом інформації розцінювати як замах на неправомірний доступ до комп'ютерної інформації. Тобто дії особи, хоча і пов'язані з неправомірним доступом до комп'ютерної інформації, але не призвели до порушення роботи ЕОМ, системи ЕОМ або їх мережі з незалежних від цієї особи обставин, утворюють попередню злочинну діяльність і кваліфікуються з посиланням на ч. 3 ст. 14 КК.

Моментом закінчення доступу до комп'ютерної інформації дослідник Ю.І. Ляпунов вважає "момент відсилання користувачем комп'ютера останньої интерфейсной команди (голосовий, натисканням клавіші і т.п.) виклику зберігається, незалежно від настання подальших наслідків". Однак, на його думку, злочином це діяння стане лише в разі настання вказаних в диспозиції наслідків. Всі дії, виконані до подачі останньої команди, становитимуть склад незакінченого злочину [90, с. 11]. На думку науковця С.А. Пашина, злочин може бути закінчено і після нейтралізації інтелектуальних засобів її захисту (МСЗ), якщо при цьому не настали наслідки у вигляді знищення, блокування, модифікації або копіювання комп'ютерної інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі, то такі дії (нейтралізація НСЗ) повинні розглядатися як замах на неправомірний доступ до комп'ютерної інформації. Таким чином, моментом закінчення неправомірного доступу до комп'ютерної інформації (ст. 361 КК України) слід вважати витік, втрату, блокування, підробку, спотворення процесу обробки комп'ютерної інформації та порушення встановленого порядку її маршрутизації.

Крім обов'язкових ознак складу злочину, в кримінальному праві виділяються такі факультативні ознаки, як: місце, час, засоби і знаряддя, а також спосіб вчинення злочину. Місцем вчинення злочину є певна територія, на якій вчинюється передбачене кримінальним кодексом України суспільно небезпечне діяння. Зв'язок злочинного діяння з місцем його вчинення може бути таким: діяння вчинюється у

певному місці; діяння полягає у залишенні того чи іншого місця; діяння посягає на певне місце [100]. Місце вчинення комп'ютерного злочину відіграє важливу роль, особливо, у разі скоєння злочину відносно інших країн. Час вчинення злочину, як ознака складу злочинного діяння є певним періодом часу, протягом якого скоюється злочин, проте у кібернетичних злочинах час вчинення не відіграє ключову роль.

Способами втручання до роботи систем і мереж можуть бути: виявлення слабких місць у захисті, шляхом автоматичного перебирання абонентських номерів («угадування коду»), дії «хакерів», з'єднання з тим чи іншим комп'ютером, підключеним до телефонної мережі, використання чужого імені (пароля) за допомогою існуючої помилки в логіці побудови програми та ін. Способи незаконного вторгнення в роботу мереж електрозв'язку можуть бути різними: шляхом підключення до ліній зв'язку, використання різних технічних пристроїв («жучків») для прослуховування і фіксування інформації, яка є в обігу систем електрозв'язку та ін. [102]. За винятком способу вчинення неправомірного доступу до комп'ютерної інформації, інші факультативні ознаки об'єктивної сторони злочину на кваліфікацію скоєного не впливають, але можуть враховуватися при призначенні покарання.

Таким чином, об'єктивна сторона злочину, відповідальність за яке передбачена ст. 361 КК України, полягає у діях — несанкціонованому втручанні у роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, за умови, що саме ці дії призвели до: витоку, втрати, підробки, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації та між зазначеними діями та наслідками існує зв'язок.

Найбільш небезпечним різновидом комп'ютерної злочинності є **створення з метою використання, розповсюдження або збуту шкідливих програмних та технічних засобів, призначених для ЕОМ, автоматизованих систем та мереж електрозв'язку**, особливо в вигляді комп'ютерних вірусів. На даний час поширеність комп'ютерних вірусів є масштабною проблемою світового рівня.

Об'єктивна сторона злочину, передбаченого **ст. 361-1 КК України**, полягає у створенні шкідливих програм для ЕОМ або внесенні змін до існуючих програм, використанні або розповсюдженні подібних програм або машинних носіїв з такими програмами.

Об’єктивна сторона складу злочину характеризується:

I. Діями у вигляді:

1) створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку;

2) розповсюдження таких програмних чи технічних засобів;

3) збуту вказаних програмних чи технічних засобів.

II. Наслідками — наявності шкідливих програмних чи технічних засобів;

III. Причинно-наслідковим зв'язком між зазначеними діями та настанням наслідків.

Створення вказаних програмних чи технічних засобів — це виготовлення програмних чи технічних засобів, внаслідок чого виникають нові шкідливі предмети (яких раніше не існувало), здатні до несанкціонованого втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку [10, с. 461-463].

Під створенням програмного продукту розуміється процес написання програми починаючи від виникнення ідеї до її компіляції. Для створення шкідливих програм необхідна наявність знань у сфері програмування. На сьогоднішній день навчитися створювати віруси різної складності та різних галузей застосування, контролювати будь-який комп'ютер чи здобути паролі від систем, проводити махінації з метою отримання грошових коштів від жертв не складає особливих труднощів. Ввівши до пошукової строки потрібне запитання відповідь знаходиться сама-собою, тож, провівши такий експеримент ми з легкістю знайшли детальне керівництво до застосування хакера.

Виявилось, що можна з легкістю створити вірус, комп'ютерний вірус являє собою зловмисну комп'ютерну програму, в якій міститься частина коду, який починає свою дію після запуску вірусу в комп'ютерній системі. Він діє таким чином, що під час своєї роботи вірус заражає інші програми копіями самого себе у

результаті чого можливе настання несприятливих наслідків від легкого роздратування користувача до повного знищення всіх даних в системі [96]. Певні види вірусів можуть копіювати самих себе та розповсюджуватися до інших систем, що, у свою чергу, ускладнює локалізацію вірусів і захист від них. Віруси можна передавати лініями зв'язку або поширювати на вже інфікованих носіях, що ускладнює локалізацію творця вірусу. До того ж, деякі віруси можуть переховуватися усередині інших програм або проникати безпосередньо до операційної системи комп'ютера. Шляхи потрапляння вірусів до комп'ютерів різні, але загальне в них одне — віруси входять до комп'ютерних систем виключно з зовнішніх джерел і як тільки вірус входить у систему, він може почати свою руйнівну діяльність відразу, або ж очікувати активації якоюсь подією, наприклад, отриманням певних даних або настанням заданої дати або часу [145, с. 90].

Відомі кілька різновидів комп'ютерних вірусів. **Троянський кінь** являє собою комп'ютерну програму, яка маскується або ховається в частині програми. Навідміну від інших вірусів, вони не реплікують самих себе в системі, а деякі форми троянських коней можуть бути запрограмовані на саморуйнування і не залишати жодних слідів, крім заподіяних ними руйнувань. Хакери використовують троянських коней для отримання паролів, зокрема вони можуть використовуватися у сфері банківських шахрайств, коли невеликі суми грошей знімаються з законних рахунків і передаються до секретних рахунків. За допомогою трояну можливо отримати доступ до чужого поштового ящику. Для цього проводиться розсилання електронних листів з вбудованими вірусами, вірус вбудовується не в сам лист, а лист лише містить посилання на вірус, зазвичай зміст листа має чимось «зачепити» користувача, він повинен бути таким, на який користувач не зможе не відреагувати. Прикладами троянів є : DarkComet RAT, SpyEye, Carberp та ін.

Наступним вірусам, яким ми хотіли б приділити увагу є "**хробаки**" — це програми, які руйнують комп'ютерні системи, можуть проникати до програм обробки даних і підміняти або руйнувати дані. Вони можуть завдавати великі руйнування, якщо їх вчасно не виявити, набагато простіше ліквідувати хробака або троянського коня, якщо існує тільки єдина копія програми-руйнівника [31], що у

більшості випадках малоймовірно. Ми з легкістю знайшли в Інтернеті статтю, присвячену створенню хробака, під назвою .bat вірус. Тож аби створити .bat-вірус потрібен текстовий редактор, для чого підійде Блокнот. Створивши і відкривши новий текстовий документ, потрібно вписати туди той код (команди), які він повинен виконати. Після чого, за допомогою меню зберегти, задавши йому ім'я з розширенням .bat та зазначив тип файлу "Все файлы". Вікна командного рядка, які нескінченно і дуже швидко відкриваються не дадуть користувачеві спокійно працювати. Закрити їх не встигне ніхто і дуже скоро вони заб'ють оперативну пам'ять комп'ютера, що в свою чергу загальмує роботу комп'ютера, аж до повного зависання [58].

Щє одним видом комп'ютерних вірусів є **логічні бомби** подібні до програм, що використовуються для троянських коней, однак вони мають таймер, який підриває їх в задану дату і час. Наприклад, **вірус Michelangelo** має тригер, встановлений на день народження знаменитого художника Мікеланджело - 6 березня. Чималу шкоду заподіяла шкідлива **програма "Чорнобиль"**, яка поєднує як особливості "вірусів", так і особливості "тимчасових бомб" (шкідлива активізація цієї програми відбувається 26 квітня кожного року, тобто, в день, коли сталася чорнобильська катастрофа). Завдяки вбудованому механізму затримки логічні бомби активно використовуються для шантажа. Наприклад, шантажист може послати повідомлення, що якщо йому буде виплачена певна сума грошей, він надасть інструкцію для відключення логічної бомби [145, с. 91]. **Наприклад**, 27 червня 2017 року відбулась хакерська атака всесвітнього масштабу України, Італії, Ізраїлю, Сербії, Угорщини, Румунії, Польщі, Аргентини, Чехії, Німеччини, Великобританії, США, Данії, Нідерландів, Іспанії, Індії, Франції та Естонії [194; 195], яка мала суттєвий вплив на українські провайдери. У результаті атаки виникли складності у обслуговуванні клієнків банків та проведенні банківських операцій. Кібернапади відбувалися за допомогою вірусу Petya, який використовує недоліки операційних систем, зафіксовані на серверах і персональні комп'ютери , — передає "Урядовий портал". У Кабміні повідомили, що зараженню піддалися системи Міністерства інфраструктури, Укртелекому, Укрпошти, "Нової пошти "офіс"

Укренерго", аеропорт "Бориспіль ","Київенерго", київське метро і ряд банківських установ [174]. Вірус Petya (також відомий як Petya.A, Petya.D, Trojan.Ransom.Petya, PetrWrap, NotPetya, ExPetr, GoldenEye [104]) є шкідливою програмою, мережевим черв'яком і програмою-вимогачем, яка вражає комп'ютери під управлінням Microsoft Windows. Програма шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує і шифрує MBR — дані, необхідні для завантаження операційної системи [191]. Під впливом програми комп'ютерні файли стали недоступними, після чого вимагали грошовий викуп у сумі 300 доларів у біткоінах за розшифровку і відновлення доступу до файлів. Про дійсну мету цієї хакерської атаки можливо лише здогадуватися, адже суттєвих збитків не було завдано. Можливо напад було спричинено з метою отримання інформації (коди доступу до сайтів, паролів та іншої необхідної інформації), аби підготуватися до більш серйозного нападу. Описані події можна назвати цільовою атакою, адже вони направлені на зараження мереж компаній, організацій, та можливо навіть їх сітьової інфраструктури [176].

Вбачаючи, що першою у світі цифровою валютою та найбільш розповсюдженою криптовалютою у світі є Bitkoin(курс біткоіну станом на 13.01.2018р. дорівнює $ 14 092,3), валюта, створюється і зберігається в електронному вигляді й наділена такими якостями, як: децентралізованість; легкість налаштування; анонімність та швидкість [149, с. 522]. Криптовалюта є ідеальним знаряддям тіньової економіки, вона є децентралізованою, тобто ні держава, ні банки не мають над нею контролю, що в свою чергу зручно як користувачам так і злочинцям і тому ідеально підходить для тіньової економіки.

Створення шкідливої програми слід вважати закінченим з моменту завершення компіляції цієї програми, а попередній етап створення програми необхідно розцінювати як замах на злочин. До створення слід віднести і модифікацію (перероблення) програмних чи технічних засобів, які звичайно використовуються в роботі ЕОМ, АС, у комп’ютерних мережах чи мережах електрозв’язку, а внаслідок перероблення набувають якості шкідливих і здатних до несанкціонованого втручання в ЕОМ, АС, комп’ютерні мережі чи мережі електрозв’язку [10, с. 465]. Внесення змін до існуючих програм для ЕОМ означає

зміну тексту програми шляхом виключення його окремих фрагментів, заміни їх іншими або їх доповнення новими. Злочином це діяння буде і в тому випадку, якщо винний змінив існуючу програму за допомогою спеціального програмного продукту. Необхідно відзначити, що стосовно ст. 361-1 КК України мається на увазі, що програма, у яку було внесено зміни, стає шкідливою саме у результаті таких змін. Використання шкідливих програмних чи технічних засобів – це дії, спрямовані на застосування цих засобів відповідно до їх властивостей і призначення. Таким чином, під використанням шкідливих програм ми маємо на увазі застосування цих програм за прямим призначенням.

Розповсюдження шкідливих програмних чи технічних засобів є оплатною чи безоплатною передачею у будь-який спосіб зазначених засобів відносно широкому і невизначеному колу осіб (фізичних чи юридичних), навіть через систему Інтернет [67]. Під поширенням шкідливих програм для ЕОМ слід розуміти надання доступу до програми для ЕОМ в компілюваному вигляді, в тому числі мережевими (наприклад по мережі Інтернет) та іншими способами, а також шляхом продажу, прокату, здавання під найм, надання в борг (включаючи імпорт для будь-якої з цих цілей) або створення умов для поширення програми.

Шкідливі програми можуть бути поширені по комп'ютерній мережі як в робочому вигляді, так і у вигляді вихідних текстів програм, однак, кримінально-караним це діяння буде лише при поширенні шкідливих програм у компілюваному вигляді. Продаж подібних програм через електронні магазини також є поширенням. Розповсюдження машинних носіїв з шкідливими програмами означає передачу (як на платній, так і на безоплатній основі) машинних носіїв будь-якій особі або надання можливості користуватися цими носіями іншим особам (наприклад, підкидання заражених дискет в приміщення, де працює група операторів ЕОМ). Нерідко на ринках, які торгують різного роду програмними продуктами можна зустріти компакт-диски для "хакерів", на яких іноді містяться комп'ютерні віруси або інші шкідливі програми.

У разі вчинення злочину у формі розповсюдження його слід вважати закінченим з моменту надання доступу до такого засобу іншим особам, або ж дій,

після яких починається його автоматичне відтворення і поширення. У разі збуту таких засобів злочин є закінченим з моменту передачі іншій особі хоча б однієї програми чи технічного пристрою, які є шкідливими програмними чи технічними засобами.

Збут шкідливих програмних чи технічних засобів полягає в оплатній (як правило) чи безоплатній (наприклад у формі подарунку) передачі вказаних засобів іншій, будь-якій особі. Даний злочин (ч. 1 ст. 361-1 КК) є злочином з формальним складом, тому для наявності його об’єктивної сторони не потрібно встановлювати настання суспільно небезпечних наслідків [10, с. 465], злочин є закінченим з моменту завершення процесу створення хоча б одного такого засобу. Головною умовою є те, що настання шкідливих наслідків при використанні потенційними користувачами відповідних програм має бути реально можливим.

У випадку використання особою раніше створеного нею шкідливого програмного чи технічного засобу для несанкціонованого втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку такі дії, за умови настання відповідних наслідків, мають кваліфікуватись як сукупність злочинів, передбачених ст. 361 та ст. 361-1 КК [67].

Особливістю шкідливих програм, загалом "вірусів" є процес заподіяння шкоди, який найчастіше відбувається без участі людини, позбавляючи безпосереднього винуватця (людини) можливості контролювати цей процес. Дана особливість нерідко призводить до заподіяння більшої шкоди, ніж та, на яку очікував винний. Таким чином, діяльність, пов'язана з розповсюдженням, створенням і використанням шкідливих програм може розглядатися у якості джерела підвищеної небезпеки. Однак джерелом підвищеної небезпеки є не сама програма, а її функціонування, адже відповідальність за шкоду настає тільки у разі виникнення шкоди у результаті дії джерела підвищеної небезпеки.

Не можна не враховувати світову практику в цій галузі, яка передбачає кримінальну відповідальність не тільки за виготовлення "вірусу", але і за підготовчі дії. Звичайно, вирішальним фактором у прийнятті такого рішення повинні грати

завдані нею збитки або загроза її заподіяння, що утворилися в результаті розробки і поширення комп'ютерного вірусу.

Зустріч комп'ютера зі шкідливими програмними та технічними засобами може спричиняти такі наслідки:

* Появу незвичайних системних повідомлень;
* Зникнення файлів або збільшення їх розмірів;
* Уповільнення роботи системи;
* Раптова нестача дискового простору;
* Недоступність диску.

Важливим методом захисту від вірусів виступає розгортання антивірусних програм, які мають три основні завдання: виявлення вірусу, видалення вірусу та превентивний захист [31]. Проте антивірус не завжди може допомогти, адже принцип його дії побудовано на відстеженні коду вірусу, який прописано у його програмі. Якщо певного коду вірусу немає у такому переліку, то антивірус на його не відреагує і він проникне до ЕОМ (це ж стосується і нових вірусів).

Використання комп'ютерних технологій суттєво полегшує вчинення злочинів і дозволяє заподіяти більшу шкоду, ніж при здійсненні такої ж злочину, але без використання електронних/комп'ютерних технологій. Злочини, вчинені з використанням шкідливих програм, характеризуються високим ступенем суспільної небезпеки і тому вимагають глибокого аналізу і всебічного вивчення. Комп'ютерні технології все швидше розповсюджуються, ускладнюються, тим самим розкриваючи нові можливості для використання їх у злочинних цілях.

Таким чином, об'єктивна сторона злочину, передбаченого ст. 361-1 КК України, полягає в створенні шкідливих програм для ЕОМ або внесенні змін до існуючих програми, використанні або розповсюдженні таких програм (або машинних носіїв містять їх), що створюють реальну загрозу настання суспільно небезпечних наслідків.

Об’єктивна сторона злочину, передбаченого нормою **статті 361-2 КК України,** полягає у вчиненні **несанкціонованого збуту або розповсюдженні комп’ютерної інформації з обмеженим доступом, яка зберігається на ЕОМ**

(комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації [10, с. 467].Збутом комп'ютерної інформації з обмеженим доступом є її оплатна чи безоплатна передача хоча б одній особі, яка не має до неї доступу; розповсюдженням — розміщення в АС чи комп'ютерній мережі з наданням вільного доступу до неї або шляхом вчинення інших дій, які створюють можливість вільного доступу до неї невизначеного кола осіб. Збут та розповсюдження слід вважати несанкціонованими, якщо такі дії вчинені без дозволу (згоди) власника інформації. До того ж, несанкціоновані збут та розповсюдження містять ознаки злочину як у тому випадку, коли вони вчинені особою, якій в установленому порядку було надано доступ до відповідної інформації, так і у випадку вчинення їх особою, яка такого доступу не мала. Несанкціонований збут або розповсюдження комп'ютерної інформації з обмеженим доступом, вчинені після одержання такої інформації внаслідок несанкціонованого втручання у роботу ЕОМ, їх систем, комп'ютерних мереж чи мереж електрозв'язку, утворюють сукупність злочинів і мають кваліфікуватись за статтею 361 та статтею 361-2 [67].

Несанкціонований збут інформації з обмеженим доступом, яка зберігається на комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації є несанкціонованим розповсюдженням такої інформації без згоди її власника на платній основі, наприклад, шляхом купівлі-продажу, міни або ін. чином. Несанкціоноване розповсюдження такої інформації є вчиненням будь-яких дій, якими без згоди власника така інформація безпосередньо чи опосередковано надається іншим особам чи доводиться до їх відома, вводиться в обіг шляхом будь-якої, крім оплатної, форми. Розглядуваний злочин (ч. 1 ст. 361-2 КК) є злочином з формальним складом і тому вважається закінченим з моменту вчинення суспільно небезпечних дій, зазначених у законодавстві, без настання суспільно-небезпечних наслідків [10, с. 467-468].

У випадках умисного розповсюдження чи збуту комп'ютерної інформації, яка є державною таємницею чи іншою конфіденційною інформацією, що є власністю держави, дії винного мають кваліфікуватись за даною статтею та, за наявності відповідних ознак, за статтями 111, 114, 328 або 330 КК України. У випадках

вчинення таких же дій щодо захищеної інформації, яка є комерційною чи банківською таємницею, вони, за наявності відповідних ознак, мають додатково кваліфікуватись за ст. 231 або ст. 232 КК України; щодо такої ж інформації, яка є лікарською таємницею – за ст. 145 КК України; щодо відповідної інформації, яка є таємницею усиновлення (удочеріння) – за ст. 168 КК України; щодо захищеної інформації, яка є листуванням чи іншою приватною кореспонденцією громадянина — за ст. 163 КК України [67].

Об’єктивна сторона злочину, передбаченого статтею 362 КК України, за ч.1 норми статті полягає у несанкціонованій зміні, знищенні або блокуванні комп’ютерної інформації, відповідно до ч. 2 у несанкціонованому перехопленні або копіюванні такої інформації. Почнемо з аналізу ч. 1 статті. Обов’язковими ознаками зміни, знищення або блокування комп’ютерної інформації є несанкціоновані дії, тобто на вчинення яких особа має доступ до такої інформації, але не має права на її зміну, знищення та блокування (більш детально дані поняття описані раніше у об'єктивній стороні статті 361 КК України) [10, с. 457-473].

Частиною 2 статті 362 КК України передбачено кримінальну відповідальність за вчинення несанкціонованого перехоплення або копіювання інформації, наслідком яких є витік останньої. І копіювання і її перехоплення полягають в одержанні копії інформації, відмінність між ними полягає у способі одержання відповідних копій. Наприклад, якщо при здійсненні копіювання передбачається доступ до такої, то при здійсненні перехоплення такий доступ відсутній, з чого випливає, що перехоплення зазначеної законодавцем інформації не підпадає під кваліфікацію ч. 2 статті 362 КК України, адже нормою передбачено право доступу до останньої.

Таким чином, об'єктивна сторона злочину, передбаченого статтею 361-2 КК України, полягає у вчиненні несанкціонованого збуту або розповсюдженні комп’ютерної інформації з обмеженим доступом, яка зберігається в ЕОМ (комп’ютерах), АС, комп’ютерних мережах або на носіях такої інформації. Об’єктивна сторона злочину, передбаченого статтею 362 КК України, полягає у вчиненні несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах(комп'ютерах), автоматизованих системах, комп'ютерних

мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї: несанкціонованій зміні, знищенні або блокуванні комп’ютерної інформації; несанкціонованому перехопленні, копіюванні інформації, що призвело до її витоку.

У зв'язку з тим, що ЕОМ (комп'ютер) є програмно-технічним комплексом, то його експлуатація регламентована спеціальними правилами, які встановлюють порядок обслуговування та експлуатації комп'ютерів, системм та їх мереж.

Об'єктивна сторона злочину, відповідальність за який передбачена **ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється»**, полягає у порушенні правил експлуатації ЕОМ, систем ЕОМ або їх мереж, що призвело до знищення, блокування або модифікації інформації ЕОМ, якщо таке діяння заподіяло істотну шкоду.

Об’єктивна сторона характеризується певними обов’язковими ознаками:

а) суспільно небезпечними діяннями (діями чи бездіяльністю) у формі: порушення правил експлуатації ЕОМ (комп’ютерів), АС, комп’ютерних мереж чи мереж електрозв’язку або порушенням порядку чи правил захисту інформації, яка в них оброблюється;

б) суспільно небезпечними наслідками у вигляді знищення, блокування або модифікації інформації на ЕОМ, системах та їх мережах у значних обсягах;

в) причинним зв’язком між зазначеними суспільно небезпечними діяннями та наслідками.

Порушення правил експлуатації може виражатися у недотриманні, неналежному дотриманні або прямому порушенні правил, що забезпечують збереження інформації і цілісність (працездатність) комп'ютерного обладнання. Порушення правил може бути вчинено як шляхом вчинення дій, так і внаслідок бездіяльності (невиконання винним вимог, закріплених в правилах) [10, с. 470-471]. До того ж, диспозиція ст. 363 КК України є бланкетною, тобто для встановлення змісту об'єктивної сторони злочину норма статті відсилає до інших правових

документів — правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється. Проте нормативно-правовий акт, який би визначав правила використання згаданих машин, систем і мереж на рівні держави — відсутній. Загальні засади захисту лише окремих видів інформації передбачені Законом України від 5 липня 1994 р. «Про захист інформації в автоматизованих системах» [121], Указами Президента України від 22 травня 1998 р. «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» [130] та від 27 вересня 1999 р. «Про Положення про технічний захист інформації в Україні» [131].

Можливо виділити два види правил експлуатації ЕОМ, якими повинні керуватися в своїй діяльності особи, що працюють з ЕОМ, системами або їх мережами:

I. Інструкції по роботі з ЕОМ і машинними носіями інформації, розроблені виробником ЕОМ і периферійних технічних пристроїв, які поставляються разом з даним екземпляром ЕОМ (ці правила обов'язкові для дотримання користувачами ЕОМ), як правило, під загрозою втрати прав на гарантійний ремонт і обслуговування.

II. Правила, встановлені власником інформації або власником інформаційних ресурсів, інформаційних систем, технологій та засобів їх забезпечення, що визначають порядок користування ЕОМ, системою ЕОМ і мережею ЕОМ, а також іншими машинними носіями [81, с. 88].

Таким чином, під правилами експлуатації ЕОМ слід розуміти як правила, які можуть бути встановлені компетентними органами, так і правила, встановлені виробниками ЕОМ або розробниками програмного забезпечення, а також правила, встановлені власником інформації або власником ЕОМ, системи ЕОМ або їх мережі. Відповідальність за порушення зазначених правил може наступати тільки в тому випадку, якщо ці правила були прийняті належним чином (розроблені фахівцями і підписані керівником установи, підрозділу і т.д.), закріплені (як правило на папері) і доведені до користувача (краще - під розпис). До таких правил відносяться: відомчі положення; правила, встановлені конкретною організацією; паспорта якості;

технічні описи та інструкції по експлуатації; інструкції по використанню програм для ЕОМ (відповідні інструкції можуть додаватися як на паперових, так і на машинних носіях) і ін. З чого випливає, що відсутність на підприємстві, в установі чи організації таких правил виключає наявність в діяннях особи складу аналізованого злочину.

Із загальної групи дослідників цікавим видається дослідження Ю.І. Ляпунова та С.А. Пашина, які вважають, що оскільки мова йде про правила експлуатації ЕОМ (апаратно-технічної структури), то і порушення повинно торкатися лише технічної сторони недотримання вимог безпеки комп'ютерної інформації, а не їх організаційної чи правової сторони. Дана точка зору представляється справедливою, але вимагає невеликого доповнення і уточнення. При роботі на ЕОМ експлуатується не тільки апаратно-технічна, а й програмна частина електронно-обчислювальної машини, тому що ЕОМ є програмно-технічним комплексом. Тому, під правилами експлуатації ЕОМ слід розуміти як вимоги технічного характеру (напруга, вологість, механічний та хімічний вплив, сумісність пристроїв, електромагнітне поле і т.п.), так і положення, що регулюють роботу з програмами (послідовність подачі команд або виконання процедур, заборона на виконання будь-яких операцій з програмним забезпеченням, контроль за сумісністю різних програмних продуктів, обов'язкове виконання певних процедур при настанні певних обставин і т.д.). А такі заходи, як резервне копіювання інформації, використання джерел безперебійного живлення при роботі на ЕОМ слід віднести до організаційних вимог безпеки комп'ютерної інформації, тому що вимоги виконувати встановлені правила залежать від особливостей діяльності тієї чи іншої організації, установи або підприємства.

Порушення правил експлуатації ЕОМ (комп’ютерів), АС, комп’ютерних мереж чи мереж електрозв’язку може виражатися у невиконанні або неналежному виконанні уповноваженою особою обов’язків із виконання таких правил, це може виражатися у порушенні правил апаратного забезпечення, так і правил експлуатації їх програмного забезпечення.

Таким чином, до правил експлуатації ЕОМ, систем ЕОМ або їх мереж, порушення яких тягне за собою кримінальну відповідальність передбачену ст. 363

КК України, слід віднести як вимоги технічного характеру, так і вимоги по роботі з програмною частиною ЕОМ, а також, у деяких випадках — вимоги організаційного характеру. Крім діяння (порушення правил), особливу увагу слід звернути на один з елементів об'єктивної сторони складу злочину — наслідки, настання яких для даного злочину є обов'язковими: витік (у тому числі викрадання, копіювання, втрата повна чи часткова інформації), модифікація, блокування інформації, підробка, а також порушення встановленого порядку її маршрутизації та ін. Ознакою цих наслідків є те, що вказані дії повинні заподіяти значну шкоду власнику інформації [10, с. 471]. До того ж, встотність шкоди залежить у кожному конкретному випадку від багатьох показників, наприклад, від змісту інформації, ступеня її ушкодження, можливого пошкодження самого комп'ютера або комп'ютерної мережі, заподіяння матеріальної шкоди власнику чи користувачу інформації і т.д.

Важливо і те, що значною шкодою не може вважатися знищення чи пошкодження комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, протиправне заволодіння відповідним технічним обладнанням, адже перелічені діяння не містять складу злочину, передбченого Розділом XVI КК України, за наявності підстав мають кваліфікуватися за статтями розділу VI Особливої частини КК «Злочини проти власності» або ст. 360 КК України. «Порушення правил експлуатації ЕОМ» буде закінченим злочином тільки при настанні певних несприятливих наслідків.

На нашу думку, причинний зв'язок даної статті розвивається у два етапи:

I. Порушення правил експлуатації ЕОМ з первинними несприятливими наслідками, такими як, знищення, блокування або модифікація інформації;

II. Настання вторинних наслідків — у заподіянні значної (істотної) шкоди.

Таким чином, зі змісту диспозиції ст. 363 КК України виходить, що знищення, блокування або модифікація інформації є необхідною умовою для заподіяння істотної шкоди. З метою поліпшення стану боротьби з даним видом комп'ютерних злочинів, зважаючи на те, що ст. 363 КК України є бланкетною нормою, пропонуємо визначити приблизний перелік правил експлуатації ЕОМ, систем ЕОМ або їх мереж

та здійснити судове або правозастосовне тлумачення цієї норми, у вигляді роз'яснень, наприклад, на рівні Постанов Пленуму Верховного Суду.

Перейдемо до дослідження об'єктивної сторони **перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку вчиненого шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК).**

Розвиток інформаційних технологій настиг свого апогею і тепер можливо доносити інформацію до масс, навіть знаходячись перед екраном електронно-обчислювальної машини, зокрема й інформації рекламного характеру. Внаслідок отримання надмірно кількості таких повідомлень, можна порушити звичайний режиму роботи комп'ютера, автоматизованих систем та комп'ютерних мереж, або ж призвести до припинення їх роботи та призвести до значних перешкод у роботі організацій [68]. Тому дослідження механізму перешкоджання роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку є невід'ємною частиною системи протидії комп'ютерній злочинності.

Об’єктивна сторона описаного діяння характеризується:

а) суспільно небезпечними діями у вигляді масового розповсюдження повідомлень електрозв’язку, здійсненого без попередньої згоди адресатів;

б) суспільно небезпечними наслідками у вигляді порушення чи припинення роботи автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку;

в) причинним зв’язком між зазначеними діями та наслідками;

г) особливим знаряддям вчинення злочину — повідомленням електрозв'язку.

Масовим розповсюдженням повідомлень електрозв’язку є надання значній кількості адресатів (широкому невизначеному колу осіб) без їх попередньої згоди як однакових, так і різних за змістом повідомлень.

Важливо й те, що передавання незначної кількості повідомлень одному адресатові або чітко визначеним особам не може розглядатися як масове розповсюдження, а тому не становить складу злочину передбаченого статтею 363-1 КК України.

Повідомлення електрозв’язку є певною інформацією (відомостями), які сповіщаються комусь і передаються мережами електрозв’язку. Такі повідомлення можуть містити судження, які містять у собі певні факти. Сигнали електрозв’язку, які не містять визначених відомостей, не охоплюються даним поняттям. При вчиненні цього злочину повідомлення електрозв’язку розповсюджуються через систему ЕОМ (комп’ютери), АС, комп’ютерні мережі чи мережі електрозв’язку, отже й через чережу Інтернет. Отримання адресатами повідомлень електрозв’язку (навіть коли вони мають масовий характер) за їх попередньою згодою не містить складу злочину за статтею 363-1 КК України. Напевне кожен стикався з подібним, наприклад, коли перебуваючи у мережі з'являється неочікуване повідомлення з запитанням про надання доступу до місцезнаходження або отримання оповіщень від окремих сайтів. Мається на увазі, що у випадку підтвердження таких запитів, якщо внаслідок масової розсилки таких повідомлень ваш комп'ютер відчує збій, то складу злочину у цьому не буде. Це може бути повним або частковим порушенням процесу функціонування ЕОМ або повною чи частковою втратою контролю над ними. Унаслідок порушення роботи мережі електрозв’язку втрачається і здатність забезпечувати захист інформації, що передається нею, від знищення, перекручення, блокування, несанкціонованого витоку або від порушення встановленого порядку маршрутизації. У наш час нформація є цінним об'єктом, тому не слід забувати про захист електронних даних та бути обачними. Під припиненням роботи ЕОМ (комп’ютерів), АС чи комп’ютерних мереж мається на увазі, що вони перестають працювати і не можуть виконувати операцій по збереженню, введенню, записуванню, фіксуванню, перетворенню, зчитуванню, знищенню або ж реєстрації інформації. Під припиненням роботи мережі електрозв’язку слід розуміти припинення виконання мережами електрозв’язку функцій з передавання або прийняття знаків, сигналів, письмового тексту, зображень та звуків або інших повідомлень по радіо-, проводових, оптичних або інших електромагнітних системах [10, с. 472-473].

Злочин має матеріальний склад, тобто вважається закінченим з моменту настання суспільно небезпечних наслідків, які зазначені, як у диспозиції статті 361-1

КК України, так і тих, які опосередковано маються на увазі — несанкціонованому доступу до особистої інформації.

3.3 Суб'єкт злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

На сьогоднішній день суб'єктивно-особистісні властивості осіб, які займаються злочинністю у сфері комп'ютерних технологій недостатньо досліджені, тому цю главу присвячено дослідженню суб'єктів даної категорії злочинів. Комплексне дослідження особи злочинця та його діяльності, причинних комплексів, мотивації, об'єктивних ознак, які відображають соціальні позиції і роль людини, її діяльність і соціально-ролеве поле; суб'єктивні ознаки, які частково обумовлюють мотивацію до комп'ютерних злочинів; цінністо-нормативна характеристика свідомості; дані про характер, мотив, форми організованої злочинної діяльності, види учасників та їх ролі, судимість і т.д. виступають важливими елементами дослідження суб'єктів комп'ютерних злочинів.

За К.Е. Ігошевим суб'єктом злочину є особа, що скоїла злочин, з наявністю об'єктивних ознак, які необхідні аби притягнути її до кримінальної відповідальності. Ми згодні з позицією вченого, що особистісні якості людини та зовнішнє середовище певною мірою визначають мотивацію до прийняття рішення щодо початку злочинної діяльності, у даному разі, у сфері використання комп'ютерних технологій.

Науковці О.П. Снігерьов та О.І. Сергач зазначають, що суб’єктом комп'ютерних злочинів можуть бути особи, які мають доступ до комп’ютерної системи (програмісти, оператори ЕОМ, наладчик обладнання, користувачі), так і сторонні громадяни [155, с. 60]. Згідно зі статтею 20 КК України, суб'єктом злочину передбаченого ч.1 ст. 361 КК України, може бути будь-яка фізична особа, яка на момент скоєння злочину досягла шістнадцятирічного віку, — це загальна кримінальна правосуб'єктність. Обов'язковою умовою притягнення особи до кримінальної відповідальності за вчинене суспільно небезпечне протиправне діяння

є її осудність — здатність розуміти суспільну значимість своїх дій та керувати ними. Неосудні особи не підлягають кримінальній відповідальності (ст. 21 КК України) [146, с. 122-123].

Керуючись типовими характеристиками окремих груп злочинців, можливо вирішувати загальні завдання розслідування і протидії комп'ютерних злочинів.

Можливо виділити такі групи осіб, які ймовірно можуть бути комп'ютерними злочинцям:

Перша група злочинців — особи, які використовують можливості комп'ютерних мереж та не належать ні до числа працівників організацій, ні до числа тих, хто займається сервісним обслуговуванням комп'ютерних систем.

До другої групи належать працівники організації з законним доступом до устаткування, що входить до локальних та комп'ютерних телекомунікаційних мереж, а також особи, які не є такими, але мають доступ до комп'ютерних систем по комп'ютерним мережам.

До третьої групи належать працівники усіх рангів, навіть такі, що не мають глибоких знань у роботі комп'ютерних систем, але сприяють вчиненню комп'ютерного злочину.

Четверта група — працівники, які згідно зі своєю посадою мають санкціонований доступ до приміщень з комп'ютерними системами та периферією і виконують на ЕОМ певні дії, що входять до їхніх обов'язків [22, с. 78-79].

П'ята група — це особи, які за родом своєї діяльності безпосередньо пов'язані з комп'ютерними системами або відповідають за функціонування та є працівникамии такої організації. На нашу думку такі злочинці є найбільш обізнаними у комп'ютерних технологіях та, відповідно, є найнебезпечнішими з вищеперелічених осіб.

Можливо провести градацію суб'єктів комп'ютерних злочинів за видами злочинів, в залежності від сфери їх діяльності:

1. Комп'ютерні злочини, які вчиняються операторами ЕОМ, периферійних пристроїв введення інформації до ЕОМ і обслуговуючими лінії телекомунікації.

2. Злочини, пов'язані з використанням програмного забезпечення, зазвичай скоюються системними програмістами; особами у віданні яких знаходяться бібліотеки програм; прикладними програмістами або ж добре підготовленими користувачами.

3. З апаратурної частини комп'ютерних систем небезпеку скоєння злочинів становлять: системні адміністратори, інженери, інженери термінальних пристроїв, інженери-електронщики, інженери-зв'язківці.

4. Співробітники, які займаються організаційною роботою: управлінням комп'ютерною мережею, керівництво операторами; керівництвом роботи з використанням програмного забезпечення; управління базами даних.

5. Працівники служби безпеки, працівники, які контролюють функціонування ЕОМ.

6. Спеціалісти у випадку змови з керівниками підрозділів і служб, а також з організованими злочинними групами [41, с. 111].

Суб'єктів вчинення комп'ютерних злочинів можна розділити на дві великі групи:

1. Особи, які мають з потерпілим трудові або інші ділові стосунки;

2. Особи, не пов'язані діловими стосунками з потерпілим.

До першої групи можна віднести співробітників, які зловживають своїм службовим становищем.

До другої групи належать особи, які у більшості випадках керуються корисливими мотивами, які мають вагомі знання в області комп'ютерних технологій та інколи сприймають комп'ютерні технології, як виклик своєму професіоналізму — «хакери», вони і становлять підвищену небезпеку. Одним з таких хакерів ми вважаємо Адріана Ламо, на прізвисько «Бездомний хакер». Він досліджував системи безпеки найбільших компаній: Microsoft, NY Times, Yahoo, Bank of America, зламував їх та, надавав інформацію про прогалини баз компаній. Можна стверджувати, що він ім навіть допомагав [146, с. 123].

На нашу думку особливу групу комп'ютерних злочинців становлять саме хакери. Хакер є особою, яка зламує комп’ютерні системи та мережі з метою фінансової наживи чи з інших злодіянь, або ж заради завоювання авторитету в

хакерських колах, також «хакерами» називають осіб, які, володіючи вміннями та досвідом, спрямовують свою діяльність на шкоду іншим особам, вчиняючи злочини в комп'ютерних системах. Тому, використовуючи термін «хакерство», перш за все розуміють несанкціонований доступ до комп'ютерних систем, він має скоріш негативне, аніж позитивне значення [181, с. 165-166]. Глобальні оцінки хакерства варіюються у відповідності до екстраполяцій журналу Jane's Intelligence Review, що базуються на оцінках 1990-х років, наведених В. Стерлінгом у його дослідженнях «Падіння хакера: закон і безладдя на електронній границі». Згідно з цими оцінками, загальна кількість хакерів дорівнює близько 100 тисяч, з яких 10 тисяч є відданими ентузіастами комп'ютерної справи. Група чисельністю 250-1000 чоловік утворює еліту хакерів, які є спеціалістами високого фаху, спроможними здійснити проникнення в корпоративні мережі й зруйнувати корпоративну безпеку [22, с. 77]. До найвідоміших хакерів світу належать: Кевін Митник, Кевін Поулсен («Темний Данте»), Адріан Ламо («Бездомний хакер»), Джон Шифер, Володимир Левін, Фред Коен, Марк Абенов, Нейшон Івен-Чейм («Фенікс»), Роберт Тэппэн Морріс, Ерік Корлі та ін.

До ознак, притаманних комп'ютерним злочинцям можливо віднести: наявність необхідник знань, навичок і вмінь у роботі з ЕОМ та можливість доступу до комп'ютерних мереж.

До того ж, можна констатувати, що коло суб'єктів комп'ютерної злочинності не має жодних обмежень, тому правопорушники можуть мати стосунок до різних сфер діяльності та мати різний рівень підготовки. У більшості випадках комп'ютерні злочини вчиняються особами, які мають високу кваліфікацію, тому чим складніший спосіб вчинення злочину, тим вужче коло вірогідних злочинців [146, с. 123].

Проводячи комплексний аналіз суб'єктів комп'ютерних злочинів виявилося, що станом на 1 січня 2017 року населення України складало 42 584,5 тис. осіб [101], за даними дослідження Інтернет Асоціації України на початок 2017 року нараховано 21,6 млн користувачів Інтернет [35], тобто 58 відсотків українців є користувачам мережі Інтернет «Додаток **В**». За показниками Державної Судової Адміністрації, згідно зі звітом судів першої інстанції про розгляд матеріалів

кримінального провадження у 2017 році надійшло 79 проваджень [53] за злочини у сфері використання електронно-обчислювальних машин(комп'ютерів) систем та комп'ютерних мереж (ст. 361-363-1 КК) [146, с. 123].

Відповідно до звіту Державної судової адміністрації України про склад засуджених у 2017 році за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст. 361-363-1 КК) було засуджено 42 особи. З яких 32 злочини (76%) було вчинено чоловіками та 9 відповідно жінками (24%) «Додаток **Д**». У 26% комп'ютерних категорія злочинів вчинялася у складі груп (11 у 2017 році та 12 у 2018 році). Найбільш розповсюдженими комп'ютерними злодіями на протязі 2017- 2018 років стали особи віком від 29 до 39 років (у 2017 р.- 47/у 2018р. - 37), трохи менше віком від 18 до 28 років (36/45), від 40 до 54 років (22/22), у 2018 році відмічається збільшення суб'єктів кіберзлочинів віком від 60 років і вище - 15 осіб, у порівнянні з 2 у 2017 році; віком від 16 до 17 років (3/4) та від 55 до 59 років (3/3)«Додаток **Е**». Проводячи класифікацію суб'єктів вчинення комп'ютерних злочинів за сферами їх діяльності виявилося, що 55% злочинів вчинялися працездатними, які не працювали та не навчалися (найвищий показник); працівники господарських товариств складають 2% «Додаток **Ж**» [53].

У професійно-кваліфікаційному плані коло комп'ютерних злочинців надзвичайно широке: комерційні директори, банківські службовці, фінансисти, програмісти, інженери-наладчики; монтажники комп'ютерного устаткування, бухгалтери, тощо. Серйозною проблемою для слідчого є суміщення професій при експлуатації обчислювальної техніки (бухгалтер є програмістом і оператором). Як результат взаємні перевірки ускладнюються, ймовірність зловживань зростає, а це ускладнює слідчі дії [22, с. 78]. Має місце й скоєння злочинів співробітниками організацій, які займають відповідні посади. Експертами встановлено, що більше 25% комп'ютерних злочинів вчиняються керівниками організацій. Сучасні керівники, як правило, спеціалісти високого рівня, володіють достатньою комп'ютерною підготовкою і професійними знаннями, мають доступ до інформації

широкого кола і можуть віддавати розпорядження, й при цьому безпосередньо не відповідати за роботу комп'ютерної системи.

Опитувані представники служб безпеки організацій вважають, що найбільшу небезпеку становлять користувачі, ними вчиняється 94 % злочинів, при цьому 70 % є клієнтами-користувачами комп'ютерної системи, 24 % — обслуговуючим персоналом «Додаток **З»** [9, с. 42]. З проведеного аналізу можна зробити декілька висновків: комп'ютерні злочини можливо вчиняти без особливих знань у області комп'ютерної техніки при наявності вільного часу; діаметрально протилежна думка — чим нижчий рівень знань у сфері ЕОМ, автоматизованих систем — тим більший ризик бути виявленим.

Перейдемо до більш детального розгляду складів злочинів, відповідно до норм Кримінального кодексу України. У відповідності з ч.1 ст. 18, ч. 1 ст. 19, ч. ч. 1,2 ст. 22 КК, суб'єкт злочину, передбачений ст. 361 КК, є загальним, тобто, кримінальній відповідальності підлягає фізична осудна особа, якій на момент вчинення злочину виповнилось шістнадцять років. Обов'язковим є встановлення дійсної можливості вчинювати операції з комп'ютерними системами, адже відсутність навичок роботи на комп'ютері буде свідчити про неможливість вчинення злочинних дій. Також обов'язково потрібно встановити наявність можливості входу до комп'ютерної мережі з персонального комп'ютеру, і (або) наявність ЕОМ, з якої буде вчинено злочини [5, с. 68].

Суб'єктом умисного комп'ютерного злочину передбаченого **ст. 361 КК**, є особа, яка всі свої знання і волю спрямовує на досягнення злочинного результату — доступу до інформації, її перекручення, розповсюдження комп'ютерного вірусу, або інших шкідливих комп'ютерних програм. Якщо припустити, що злочин буде вчинено неосудною особою, то у його діях буде відсутня форма вини, за відсутністю якої у юридичному складі злочину не можуть бути визначені не лише суб'єкт, а й суб'єктивна сторона злочину, при цьому, не можна й повністю виключати випадків вчинення комп'ютерних злочинів неосудними особами [146, с. 123-124]. Однак, не зважаючи на це, наприклад, малолітні кібер-злочинці спроможні завдати значну шкоду охоронюваним суспільним інтересам і у мережі часто публікуються

повідомлення, які це підтверджують. Напевне, що на малолітніх — «хакерів» впливає комп'ютеризація, у процесі якої вони не можуть завжди сприймати комп’ютерну злочинність як таку, вважаючи це просто цікавим проведенням часу. До того ж, вони не наділені свідомістю дорослої людини, як здатна усвідомлювати протиправність таких вчинків. Під впливом інформаційного навантаження малолітні діють фактично під психологічним примусом з боку засобів масової інформації, преси, загальних кумирів, моди на комп’ютерні правопорушення [151]. Можливе подальше зниження віку настання кримінальної відповідальності, що обумовлено великою кількістю правопорушеннь, які пов'язані з незаконним доступом до комп'ютерної інформації, що вчиняються неповнолітніми [146, с. 124].

Науковець В.Г. Гончаренко фактично розмежовує юридичні склади, передбачені статтями 361 та 361-1 КК, в межах ст. 361 КК: «Суб’єктом злочинів може бути будь-яка фізична осудна особа, що досягла 16-річного віку, у першу чергу це ті особи, яких власник або уповноважена ним особа чи розпорядник АС призначили обслуговувати АС та сторонні особи; щодо розповсюдників комп’ютерних вірусів **(ст. 361-1 КК),** то ними, перш за все, виступають розробники програмних і технічних засобів проникнення до АС (хакери), здатні спричинити перекручення або знищення комп’ютерної інформації чи її носіїв, виготовлювачі програм і засобів та інші особи» [115]. П.П. Андрушко вважаючи, що суб’єктом злочину, передбаченого **ст. 361 КК** є особа, яка досягла шістнадцятирічного віку, конкретизує, що ним можуть бути особи з персоналу «АЕОМ, їх систем та комп’ютерних мереж», а відповідно до норм **ст. 361-1 КК:** «суб’єктами злочину у формі розповсюдження комп’ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи та комп’ютерні мережі і здатні спричинити перекручення або знищення комп’ютерної інформації, її носіїв, можуть бути розробники таких програм та технічних засобів, їх виготовлювачі, зокрема, виробники (розробники) програм з комп’ютерними вірусами» [186, с. 786].

Суб’єктом злочину, передбаченого нормою **ст. 361-2 КК** та **ст. 363-1 КК** є фізична осудна особа, тобто суб'єкт загальний.

Специфічний суб'єкт міститься у **статті 362 КК** України «Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігаються на носіях такої інформації, вчинені особою, яка має право доступу до неї», — це той випадок, коли певні якості суб'єкта прописані навіть у диспозиції статті КК — наявність в особи права доступу до інформації, що обробляється в ЕОМ, АС чи комп'ютерних мережах або зберігається на носіях такої інформації. Право доступу до інформації так чи інакше пов'язане з виконанням суб'єктом злочину трудових чи службових обов'язків, або ж внаслідок наданого власником інформації дозволу. На думку В.М. Бутузова, С.Л. Остапця та В.П. Шелонцева, така особа має право доступу до інформації, яка є предметом злочину, у зв'язку із займаною посадою або виконанням спеціальних повноважень. Доступ до такої інформації здійснюється лише згідно з правилами розмежування доступу, встановленими власником такої інформації чи уповноваженою ним особою, а користувачі інформації визначаються власником інформації або уповноваженою ним особою, ними ж встановлюються їх повноваження [26, с. 31]. Досліджуючи суб'вчинення комп'ютерних злочинів Д.С. Азаров вважає, що правом доступу до інформації, зазначеній нормою **ст. 362 КК** України є право отримання користувачем можливості її обробляти в системі та не означає, що особа має таку можливість. На підставі чого доцільно вивести пропозицію, щодо зміни закону таким чином, аби «право доступу до інформації означало право обробляти цю інформацію, а не лише право одержання можливості такого оброблення [1, с. 181]. Отже наявність в особи права доступу до інформації не означає, що це право буде використано при вчиненні злочину. Доцільно доповнити норму закону таким чином: «...наявності в особи права доступу до інформації та реалізації цієї можливості зі злочинним наміром» [111, с. 115].

Особливістю злочину, передбаченого **ст. 363 КК**, є те, що відповідальність за його вчинення може нести лише спеціальний суб'єкт — особа, яка відповідає за експлуатацію автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж. Стаття 363 КК України встановлює відповідальність за порушення правил експлуатації автоматизованих електронно-обчислювальних

машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту або до незаконного копіювання комп'ютерної інформації, істотного порушення роботи таких машин, їх систем чи комп'ютерних мереж, за умови, що це заподіяло значну шкоду. Норма КК не містить конкретних технічних вимог та відсилає до відомчих інструкцій і правил, що визначають порядок роботи та які повинні встановлюватися спеціально уповноваженою особою і доводитися до користувачів, тому застосування зазначеної статті можливе тільки для локальних мереж організацій. До того ж, між фактом порушення правил експлуатації автоматизованих електронно-обчислювальних машин та істотною шкодою, що настала, повинен бути встановлений причинний зв'язок та доведено, що наслідки є результатом саме порушення правил експлуатації [4].

Таким чином, суб'єктами комп'ютерних злочинів згідно з Кримінальним кодексом України можуть бути:

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, яка 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).

Про спеціальний суб’єкт йдеться у двох випадках: особа, що 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**). Суб’єкт інших злочинів — загальний (особи, які не мають права доступу до комп’ютерної інформації) [66, с. 157].

Оцінка ознак суб’єкта злочину в сфері використання ЕОМ (комп’ютерів), систем, комп’ютерних мереж і мереж електрозв’язку набуває особливого значення у зв'язку з пониженим віком користувачів комп’ютерних технологій адже вони не досягли віку, з якого може наставати кримінальна відповідальність.

На думку вчених А.А. Васильєва та Д.В. Пашнєва останнім часом наявність нових психічних хвороб, пов’язаних із використанням комп’ютерних технологій, наприклад, людина, бажаючи отримати потрібний результат (здобути останню версію комп'ютерної гри або найновіший драйвер) може не віддавати собі звіт у тому, що він домагається цього злочинним шляхом (наприклад, здійснюючи неправомірний доступ до комп'ютерної інформації) [144, с. 87-88]. Отже, слід приділити окрему увагу поведінці підозрюваного в ході слідства та відображення її у механізмі злочинної поведінки для оцінки осудності такої особи з метою встановлення об'єднуючих ознак суб'єктів комп'ютерних злочинів.

3.4 Суб'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

У кримінально-правовій літературі суб'єктивна сторона злочину трактується як психічне ставлення суб'єкта до свого суспільно небезпечного діяння і його наслідків, що може виражатися у формі умислу або необережності. До змісту суб'єктивної сторони входять факультативні ознаки, такі як: мотиви, цілі та у певних випадках — особливий емоційний стан.

У зв'язку з високою складністю комп'ютерних технологій і процесів, що відбуваються в ЕОМ, системі ЕОМ, або їх мережі, часом виникають труднощі при відмежуванні комп'ютерних злочинів, здійснених навмисно, від аналогічних злочинів, скоєних з необережності та необережних діянь від невинних, які формально містять ознаки злочинів у сфері комп'ютерної інформації.

Психічне ставлення 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 (Розділ XVI КК України), характеризується умисною формою вини. Винний усвідомлює фактичний характер і суспільну небезпеку своїх дій, передбачає настання суспільно небезпечних наслідків і бажає або допускає їх настання, або ж ставиться до них байдуже. І тільки злочинні

діяння, відповідальність за які передбачена ч. 2 ст. 361-1 і ст. 363 КК, поєднують в собі умисел і необережність (злочин з двома формами вини). В цілому ж такі злочини визнаються вчиненими навмисне.

Відносно суб'єктивної сторони складу злочину, передбаченого статтею **361 КК** України, на думку таких авторів як С.А. Пашин, У.А. Усманов, А.Н. Попов, даний злочин може бути вчинено як умисно, так і з необережності. На думку С.А. Пашина, необережна форма вини може проявлятися при оцінці особою свого доступу, а також щодо несприятливих наслідків доступу, передбачених диспозицією ст. 361 КК. З даним судженням важко не погодитися, оскільки встановлення в діянні винного наміру, а не необережності, як уже нами зазначалося, буде істотно ускладнено, хоча б тому, що при різних станах обчислювальної системи (причому, часто невідомих злочинцю) одні й ті ж дії можуть призводити до різних наслідків. На думку О.М. Попова, можливість залучення до кримінальної відповідальності за вчинення злочину передбаченого ст. 361 КК через необережність, проте необхідно враховувати, що дії можуть бути здійснені як навмисне, так і з необережності. Таку точку зору розділяє і У.А. Усманов, вважаючи, що розглядуваний злочин може бути вчинено як умисно, так і з необережності. Є автори, які займають іншу позицію по відношенню до даного питання, так, М.М. Кареліна вважає, що суб'єктивна сторона складу злочину, відповідно до ст. 361 КК України характеризується тільки прямим умислом. Ми поділяємо точку зору тих вчених-юристів, які вважають, що вчинення злочину, відповідальність за яке передбачена ст. 361 КК, характеризується виною у формі умислу, тобто, особа усвідомлює суспільну небезпеку несанкціонованого втручання до роботи ЕОМ, систем, комп'ютерних мереж, мереж електрозв'язку, передбачає можливість чи неминучість настання суспільно небезпечних наслідків (у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації) і бажає, або свідомо допускає їх настання, або ставиться до них байдуже. Свідоме допущення, або байдуже ставлення до настання наслідків свідчить про наявність непрямого умислу при вчиненні неправомірного доступу.

Спираючись на результати вивчення зарубіжних і вітчизняних авторів, що спеціалізуються на питаннях комп'ютерних злочинів, відповідно до оцінок експертої комісії Інтерполу на даний час можна виділити п'ять найбільш розповсюджених мотивів вчинення комп'ютерних злочинів:

- корисливі мотиви - 66%;
- політичні мотиви (тероризм, політичні акції) - 17%;
- дослідницька цікавість - 7%;
- хуліганські мотиви і бешкетництво - 5%;
- помста - 4% «Додаток **К**» [41, с. 106].

Розглядаючи суб'єктивну сторону неправомірного доступу до комп'ютерної інформації, вважаємо за потрібне приділити увагу відхиленню в людській психіці — комп'ютерній фобії. Багато психіатрів вважають хворобливе захоплення "Інтернетом" новим видом маніакальної залежності. Професор Стенфордського університету Джозеф Левицькі вивчає випадки, коли надмірне захоплення «Інтернетом» призводить до деградації особистості. Комп'ютерна фобія — це така зміна в психіці людини, яка не дозволяє з достатньою часткою впевненості говорити про наявність провини в злочинній поведінці цієї людини. З розвитком комп'ютерних технологій продовжує збільшуватися кількість людей, які знаходяться на різних стадіях розвитку подібних відхилень психіки. Віртуальна реальність дозволяє максимально збільшити реалістичність відчуттів при роботі або грі на комп'ютері, тому ризик відхилення від нормального свого стану психіки збільшується [41, с. 105].У осіб, які захворіли на комп'ютерну фобію, може бути підвищена агресивність, розмитість меж дозволеного і злочинного. Людина, бажаючи отримати потрібний результат (наприклад, добути останню версію комп'ютерної гри або найновіший драйвер) не віддає собі повного звіту у тому, що він домагається цього злочинним шляхом (здійснюючи неправомірний доступ до комп'ютерної інформації). До того ж, комп'ютерні фобії можуть провокувати розвиток або загострення інших психічних захворювань [144, с. 87].

Мотивація є важливим елементом психології особи злочинця та тісно пов'язана з об'єктивними умовами соціального середовища, вона немов пронизує її

основні структурні утворення: спрямованість особистості, характер, емоції, здібності, діяльність, психічні процеси та включає у себе: виникнення, формування мотиву злочинної певедінки та цілі. За визначенням К. Є. Ігошева: «Мотив злочинної поведінки можна визначити як сформоване під впливом соціального середовища і життєвого досвіду особи спонукання, яке є внутрішньою безпосередньою причиною злочинної діяльності та виражає особистісне ставлення до того, на що спрямована злочинна діяльність» [56, с. 66]. Мотиви вчинення комп'ютерних злочинів різноманітні й частину з них можна віднести до «вічних»: жадоба, цікавість чи помста. Вважаємо, що значне місце в цьому списку мотивів займає унікальний за своєю суттю мотив — інтелектуальна боротьба між людиною і комп'ютерною системою. За висловом Ю. М. Батуріна «основним чинником, який спрощує розслідування, звичайно є обмежене коло здібних вчинити хитріший комп'ютерний злочин, що полегшує «виявлення» злочинця» [8, с. 41].

Аналізуючи склад злочину, передбачений ст. 361-1 КК «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ми також спостерігаємо різницю в підходах авторів до визначення форми вини, вчені Ю.І. Ляпунов, А.І. Рарог, С.А. Пашин вважають, що психічне ставлення особи до виконання дій, що утворюють об'єктивну сторону даного складу, характеризується прямим умислом. Винний усвідомлює фактичний характер і суспільну небезпеку своїх дій і бажає їх настання. Усвідомлення суспільно небезпечних наслідків залишається за рамками «формального» складу аналізованого діяння, така точка зору є практично загальноприйнятою серед вітчизняних вчених-криміналістів [54, с. 363; 89, с. 13; 142, с. 220; 153, с. 415].

Разом з тим, у юридичній літературі не приділялося достатньої уваги специфічній ознаці інтелектуального моменту прямого умислу при взаємодії з шкідливими програмами — усвідомлення винним характеристик предмета злочину. Усвідомлення особою суспільної небезпеки своїх дій визначається обізнаністю винного про ступінь шкідливості програм, з якими він взаємодіє, оскільки дії, що утворюють об'єктивну сторону складу злочину, передбаченого ст. 361-1 КК, поза

зв'язком з предметом не являють самостійної суспільної небезпеки, **таким чином, предмет злочину стає головним елементом складу неправомірного поводження з шкідливими програмами та впливає на визначення суб'єктивної сторони цього злочину.**

Необхідно встановити, що винний знав про шкідливість програм, про це прямо зазначено у ст. 361-1 КК. До того ж, вважаємо, що при створенні, використанні та поширенні шкідливих програм наявність такої риси інтелектуального моменту, як допущення винним того, що ці програми призводять до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі, ще не означає, що умисел винного є непрямим, адже свідоме допущення характеризується скоріш не як інтелектуальний, а як вольовий момент непрямого умислу в матеріальному складі. Така ознака замінює собою одну з ознак прямого умислу — передбачення можливості настання суспільно небезпечних наслідків у матеріальному складі злочину, в той час як ознака знання тих же обставин замінює ознаку передбачення неминучості настання таких наслідків.

На даний час чинний КК визначає, що у "формальних" складах, де є характеристика інтелектуального моменту умислу — завідомість, умисел може бути тільки прямим. При цьому винний може як допускати наявність одного з об'єктивних ознак, так і знати про це (точно так само, як в матеріальних складах винний може передбачити як конкретну можливість настання бажаного ним наслідку, так і очевидну неминучість його настання). Пропонуємо доповнити існуючі форми вини — злочинною необачністю, яка б включала у себе ознаки непрямого умислу та злочинної самовпевненості (легковажності). Таким чином, інтелектуальний момент прямого умислу при поводженні з 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. Даний підхід, на нашу думку, дозволить в значній мірі сприяти застосуванню ст. 361-1 КК, тому що не вимагатиме

встановлення абсолютно чіткого знання винним властивостей предмета злочину (шкідливої програми), що, як правило, досягається тільки визнанням винного та бажанням вчинити дії, які утворюють об'єктивну сторону такого складу, оскільки склад цього злочину є «формальним».

При аналізі **ч. 2 ст. 361-1 КК** (ті самі діяння, якщо вони заподіяли значну шкоду) ми стикаємося з так званою "змішаною" формою вини, наявність якої можливо тільки в «матеріальних» складах. За загальним правилом, «змішана» форма вини полягає в об'єднанні двох форм вини в одному злочині, тобто по відношенню до злочинного діяння це умисна форма вини (для даного складу — прямий умисел), а по відношенню до настання наслідків — необережність. Дослідник С.А. Пашин вважає, що особа, яка створила або використовувала шкідливу програму, або яка її розповсюджувала через третіх осіб, відповідає за виниклу значну шкоду, якщо вона передбачала можливість настання цих наслідків. Злочинна недбалість в даному випадку не ставиться у провину, тому що між створенням, використанням і поширенням шкідливих програм і настанням відповідних тяжких наслідків такий складний причинно-наслідковий зв'язок, що суб'єкт не може повною мірою передбачити настання суспільно небезпечного результату. Нам же видається, що для кваліфікації незаконного поводження зі шкідливими програмами, що спричинило з необережності значну шкоду, не має значення, в результаті злочинної самовпевненості або злочинної недбалості настали тяжкі наслідки. Важливим є тільки необережність по відношенню до настання наслідків. Якщо ж щодо тяжких наслідків присутній прямий або непрямий умисел, то злочин, передбачений ст. 361-1 КК, буде виступати у якості способу вчинення іншого злочину і кваліфікація повинна проводитися за сукупністю ч. 1 ст. 361-1 КК з іншими статтями КК, в залежності від спрямованості умислу.

Вчені Ю.М. Батурин і А.М. Жодзішскій вважають, що не має великого значення, комп'ютерна неграмотність (в даному випадку недалекоглядність, непередбачливість) або легковажне поводження з комп'ютерною системою, що викликає ризик, спричинили суспільно небезпечні наслідки, адже і легковажність і недбалість можуть покласти початок катастрофічним подіям [8, с. 32], у цьому є

логіка, до того ж, виходячи з наслідків може виникнути необхідність кваліфікації такого злочину за сукупністю з іншими в залежності від характеру наслідків. Раніше нами зазначалося, що у разі умисного заподіяння значної шкоди, створення, використання або розповсюдження шкідливих програмних чи технічних засобів виступає способом вчинення іншого злочину, тому кваліфікація повинна проводитися за сукупністю з іншими злочинами, які вчиняються разом із зазначеним. Такі факультативні ознаки суб'єктивної сторони злочину, як мотив, мета і особливий емоційний стан на кваліфікацію неправомірного поводження зі шкідливими програмами не впливають, проте їх наявність може лише пом'якшувати або обтяжувати вирок суду.

Суб’єктивна сторона злочину, передбаченого статтею 361-2 КК України характеризується виною у формі прямого умислу, коли особа усвідомлює, що комп’ютерна інформація, яку вона збуває або розповсюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій. До того ж, диспозиція даної норми містить у якості необхідної ознаки суб'єктивної сторони мету: використання, збут чи розповсюдження предметів злочину.

Суб’єктивна сторона злочину, передбаченого ст. 362 КК України може характеризуватися виною, як у вигляді прямого, так і у вигляді непрямого умислу, при цьому особа має усвідомлювати, що вчиняє несанкціоновані дії щодо інформації в системі – дії, що проводяться з порушенням порядку доступу до інформації, установленого відповідно до законодавства.

Психічне ставлення до діяння, відповідальність за яке передбачена ст. 363 КК, виражається у формі умислу, тобто особа усвідомлює суспільну небезпечність свого діяння, передбачає можливість чи неминучість настання суспільно небезпечних наслідків і бажає, свідомо допускає або ставиться до них байдуже, з чого слідує, що цей злочин може бути вчинено як з прямим, так і з непрямим умислом. Склад даного злочину вимагає настання суспільно небезпечних наслідків, а отже є матеріальним. Однак його наслідки можна розділити на первинні і вторинні. До первинних наслідків відноситься: знищення, блокування і модифікація комп'ютерної

інформації; до вторинних — спричинення істотної шкоди. Як до первинних, так і до вторинних наслідків психічне ставлення особи виражається у формі умислу, проте необхідно провести градацію за видами умислу по відношенню до первинних і вторинних наслідків. Як по відношенню до первинних так і до вторинних наслідків при порушенні правил експлуатації ЕОМ, системи ЕОМ або їх мережі, психологічне ставлення особи характеризується непрямим умислом. Тобто, якщо винний передбачає лише можливість настання первинних наслідків і не передбачає неминучість їх настання (непрямий умисел), він не може бажати настання вторинних наслідків, а може лише свідомо допускати їх або ставиться до їх настання байдуже. Якщо ж по відношенню до первинних наслідків констатується прямий умисел, то по відношенню до вторинних наслідків, умисел може бути як прямим, так і непрямим. Наприклад, якщо особа передбачає можливість або неминучість настання первинних наслідків і бажає їх настання, то вважаємо, що особа передбачає можливість або неминучість настання вторинних наслідків і бажає, свідомо допускає, або ставиться до них байдуже. Кваліфікований склад передбачає наявність двох форм провини, що обумовлено особливостями конструкції, яка передбачає умисел по відношенню до діяння і необережність по відношенню до настання наслідків.

При порушенні правил експлуатації ЕОМ з необережності, що призвело до тяжкої шкоди, співвідношення первинних і вторинних наслідків може полягати як в послідовному настанні наслідків (один за одним), так і в паралельному. Загалом психічне ставлення до заподіяння тяжкої шкоди характеризується виною у формі необережності, яка може виражатися як у легковажності, так і у недбалості.

Факультативні ознаки суб'єктивної сторони складу злочину (мотив, мета, особливий емоційний стан) на кваліфікацію аналізованого виду комп'ютерних злочинів не впливають.

Суб’єктивна сторона складу злочину, передбаченого статтею 363-1 КК України характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням до наслідків.

При оцінці суб’єктивної сторони злочину у сфері використання ЕОМ (комп’ютерів), систем, комп’ютерних мереж і мереж електрозв’язку у більшості випадках (статті 361, 361-1, 361-2, 362, 363-1 КК України) необхідно встановити ознаки умислу в діях чи бездіяльності осіб. Однак, при цьому слід обмежуватися лише вказаною частиною об’єктивної сторони, адже щодо наслідків у цих складах злочинів може бути і необережна форма вини (змішана форма вини), це стосується тільки тих злочинів, склади яких визнаються матеріальними (ст. 361, 363-1 КК України).

У процесі оцінки суб’єктивної сторони складу злочинів, передбачених ст. 361 та ст. 362 КК України, слід приділяти окрему увагу завідомості – 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.

Мотиви та цілі вчинення різного роду комп'ютерних злочинів можуть бути різними — помста, прагнення до заволодіння інформацією та ін., наприклад, якщо викрадення інформації вчиняється з корисливих мотивів і містить ознаки шахрайства, вчинене слід кваліфікувати за сукупністю злочинів — за статтями 362 і 190 Кримінального кодексу Україїни.

Таким чином, проаналізував розділ XVI КК України, нам вдалося прослідкувати наступну картину суб'єктивної сторони комп'ютерних злочинів:

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. 2 ст. 361, 361-1, 361-2, 363 КК України).

3.5 Окремі спеціальні питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку

Розширення інформаційного простору створює нові можливості для розвитку організованої злочинності, яка поступово наближається до домінування над електронними мережами, що є приводом як до вчинення правопорушень так і до створення злочинних угрупувань, що може втілитися у перехід існуючих груп хакерів і кракерів, які координують свої операції [22, с. 79] до формування кримінальних організацій. До того ж, членам таких організацій не потрібно буде зустрічатися та навіть перебувати у одній державі, тобто відбувається об'єднання організованої злочинної діяльності з елементами неорганізованої злочинності — правопорушення, які заподіюють значну шкоду, що пов'язані з використанням комп'ютерних технологій чи проти них.

Кваліфікуючими ознаками (ч.2 ст. 361, ч.2 ст. 361-1 КК, ч. 2 ст. 361-2 КК, ч. 2 ст. 362 КК України) злочинів є вчинення їх:

1) повторно;

2) за попередньою змовою групою осіб;

3) заподіяння ним істотної шкоди.

Однією з найбільш розповсюджених кваліфікуючих ознак даних складів злочину є вчинення злочину групою осіб за попередньо змовою.

Відповідно до норми статті 28 КК України злочин вважається таким, що вчинений групою осіб, якщо у ньому брали участь декілька (два або більше) виконавців без попередньої змови між собою. Злочин визначається вчиненим за попередньою змовою групою осіб, якщо його вчинили декілька осіб (два або більше), які заздалегідь, тобто до початку злочину, домовилися про спільне його вчинення [78].

Науковці О.Ф. Ковітіді та А.М. Мельников, визначили наступні ознаки, притаманні злочинним групам:

1. Взаємна погодженість дій всіх учасників групи;

2. Наявність змови про спільне вчинення злочину;

3. Взаємна усвідомленість вчинення злочину спільними зусиллями;

4. Наявність суб'єктивного зв'язку між членами групи;

5. Участь у вчиненні злочину декількох суб'єктів.

Діяння, які не мають таких характеристик, наприклад, як взаємоузгодженість і завідомість, якщо, наприклад, обізнана лише одна діюча особа і не усвідомлюється іншими діючими особами, не може визнаватися вчиненими злочинною групою, адже найважливішою ознакою вчинення злочину групою осіб (співучасть) є змова — взаємне узгодження дій між усіма членами групи. Група завжди діє за внутрішньою узгодженістю, яка виникає внаслідок явної змови або навіть вираженої мовчанням. До того ж, діяння не може визнаватися вчиненим групою осіб, якщо дії однієї особи лише об'єктивно сприяли вчиненню злочину іншою особою [170, с. 101].

Існують випадки, коли один із співвиконавців обізнаний про вчинення злочину — створює шкідливі програми, а інший — ні, проте надає інформацію з приводу створення шкідливих програм, не думаючи про злочинність намірів), у тому числі враховуючи прогалини у правовій обізнаності. На перший погляд такі дії доцільно кваліфікувати як пособництво у вчиненні злочину (ч.5 ст. 27 КК), проте з огляду на п.6 ст. 27 КК, не є співучастю не обіцяне заздалегідь переховування злочинця, знарядь і засобів вчинення злочину, слідів злочину чи предметів, здобутих злочинним шляхом, або придбання чи збут таких предметів. У випадку одночасного, але не запланованого вчинення злочинних дій, наприклад вчинення Dos-атаки кількома особами, внаслідок чого система може вийти з ладу, наявний склад злочину, передбачений статтею 361 КК України, при цьому кожен з учасників може навіть ніколи не бачити інших виконавців, жодним чином не контактувати та навіть не здогадуватися про їх існування, у такому випадку, необхідно кваліфікувати дії кожного з осіб окремо за статтею 361 КК, не застосовуючи при цьому співучасті у вчиненні злочину.

З огляду на вищезазначене, доцільно розглядати вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку групою осіб за попередньою змовою.

Це означає, що в кожного з виконавців злочину повинен бути умисел на попередньо обговорені узгоджені дії, які необхідні для досягнення злочинного результату, до того ж, проміжок часу між змовою і початком здійснення суспільно небезпечних дій не відіграє ключову роль.

У кримінальному кодексі акцентується увага саме на виконавцях, проте на нашу думку, розподіл ролей у виконанні злочину можливий і серед них. Розглядаючи ж роль, наприклад, організатора, пособника або ж підбурювача доцільно проводити кваліфікацію за ст. 27 КК та відповідною статтею КК України при цьому без визнання його кваліфікуючою ознакою комп'ютерного злочину. Що ж стосується визнання учасником групи осіб, необхідно враховувати загальні ознаки визнання особи суб'єктом комп'ютерних злочинів: вік - 16 років та осудність. Скоєння комп'ютерного злочину за попередньою змовою, наприклад, знищення важливої інформації, що зберігалася на комп'ютері за допомогою малолітньої дитини (13 років) або ж за змовою з неосудною особою (наприклад, з розладами психічної діяльності) є опосередкованим виконавством, а отже не є співучастю, тому що один із учасників злочину не є повноцінним суб'єктом злочину, передбаченого чинним законодавством.

Проведення наукового аналізу кримінально-правової відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, скоєних у складі організованих груп та злочинних організацій є передумовою ефективної боротьби з організованою комп'ютерною злочинністю.

Під організованою комп'ютерною злочинністю мається на увазі сукупність комп'ютерних злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань [126, ст. 1]. Відповідно до статті 28 КК України злочин визнається вчиненим організованою групою, якщо у його готуванні або вчиненні приймали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення певного комп'ютерного злочину та інших злочинів у подальшому, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягненні плану, який відомий усім учасникам

такої групи [78]. Зазначені дії включають пошук співучасників, об'єднання їх зусиль, детальний розподіл між ними обов'язків, складання плану та визначення способів його виконання.

До ознак притаманних злочинним організаціям науковець М.Й. Коржанський відносить:

1) наявність статуту — розробленого і схваленого учасниками групи плану злочинної діяльності та визначення мети групи;

2) наявність організатора (керівника);

3) конспірація (приховування) своєї діяльності;

4) вербування нових членів;

5) наявність загальних правил поведінки, ієрархія стосунків між учасниками групи;

6) наявність матеріальної бази [72, с. 92].

Організовані співтовариства у даному випадку доцільно називати кібер-угрупуваннями, адже вони мають свою ієрархію, статут і розподіл ролей між учасниками. Деякі вчені застосовують термін «кібер-банда», проте на нашу думку це недоцільно, адже бандою визнається озброєна група/злочинна організація, яка попередньо створена з метою вчинення кількох нападів на підприємства, установи, організації чи на окремих осіб або для одного такого нападу, який потребує ретельної довготривалої підготовки. Вбачаючи віртуальність явною ознакою комп'ютерних злочинів наявність зброї практично виключається [148, с. 127].

Співучасниками комп'ютерних злочинів є організатор, виконавець, підбурювач та пособник. Організатором є особа, яка організувала вчинення злочину (злочинів) або керувала його (їх) підготовкою чи вчиненням; створила організовану групу/злочинну організацію або керувала нею; особа, яка забезпечувала фінансування чи організовувала приховування злочинної діяльності організованої групи або злочинної організації [78]. Саме організатор створює групу, здійснює підбір співучасників, розподіляє ролі між ними, встановлює дисципліну, а керівник забезпечує цілеспрямовану, спланована і злагоджену діяльність як групи в цілому, так і кожного з її учасників. Організатори злочинних груп у більшості випадках виступають у ролі координаторів проектів, під керівництвом яких розробляються

плани атак, створюється шкідливе програмне забезпечення, збирається конфіденційна інформація про осіб, яка потім реалізується на «чорному ринку» [62; 95, с. 190] не вчиняючи злочинів самотужки. При цьому основною метою організатора такої групи (організації) є утворення стійкого об'єднання осіб для заняття злочинною діяльністю, у даному разі для вчинення комп'ютерних злочинів, забезпечення взаємозв'язку між діями всіх учасників, упорядкування взаємодії його структурних частин.

Дії організатора злочину (злочинів) при простій формі співучасті належить кваліфікувати за статтею Особливої частини КК, якою передбачена відповідальність за вчинений злочин, із посиланням на ч. 3 ст. 27 КК, а якщо він був одним із виконавців діянь, що становлять об'єктивну сторону складу цього злочину, - без посилання на зазначену норму. Якщо ж особа приймала участь у вчиненні одного злочину як організатор, а іншого у якості виконавця, посібника чи підбурювача, його дії підлягають окремій кваліфікації у кожному випадку [135].

Особливістю організованої групи є виконання дій кожним зі співучасників для усієї групи. До складу організованої групи можуть входити особи, які виконують управлінські функції в організаціях, посадові особи та інші службовці. Участь такого роду суб'єктів може істотно полегшити підготовку і вчинення неправомірного доступу до комп'ютерної інформації, та здійснювати приховання таких злочинів. Особливістю організованої кібер злочинності є обов’язкова наявність специфічного учасника злочинної групи — хакера (фрікера, крекера тощо). Саме так називають особу, яка володіє знаннями й навичками несанкціонованого проникнення до комп’ютерних систем, він і є основним виконавцем злочинного діяння [168, с. 199; 169, с. 32-33].

На сьогоднішній день існує чимало кібер угрупувань та хакерських злочинних рухів, однією з таких є — Infroud. Зловмисники створили розгалужену й добре організовану мережу, яка протизаконним шляхом отримувала особисті дані інтернет-користувачів, які надавали доступ до банківських та електронних рахунків. За час існування угруповання злочинці завдали своїми діями збитків на понад $530 млн. Наразі слідчі вважають причетними до злочинного угруповання загалом 36

осіб. 13 членів кібербанди вже заарештували. Арешти проводилися в США, Австралії, Британії, Франції, Італії, Косові, Сербії та Албанії. Після чого співробітники правоохоронних органів США припинили діяльність злочинного угруповання [166; 148, с. 127].

Несанкціонований доступ до інформації в автоматизованих (комп'ютерних) системах є одним з найпоширеніших злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. Розповсюдження сучасних електронних засобів та простота їх використання може призвести до загроз усунення існуючого захисту інформації в автоматизованих системах, у тому числі таких, що становлять мережі телекомунікацій. До того ж, виникають обставини, які зумовлюють ланцюгову реакцію щодо несанкціонованого витоку інформації, її блокування, спотворення чи знищення у комп'ютерній формі [114, с. 89; 169, с. 34].

Банківська система держави пов'язана з накопиченням, розподілом і використанням державних та приватних коштів, отже є однією з найбільш привабливих для злочинців та особливо організованих злочинних груп. Злочини, що вчиняються у банківській системі або з її використанням, можна віднести до одних із найбільш небезпечних економічних злочинів, оскільки їх негативний вплив відображається не лише на окремих банках, а й чималій кількості суб'єктів економічної діяльності та фінансовій системі держави загалом. Способи вчинення таких злочинів різноманітні, найбільш розповсюдженими з них є такі, що вчиняються з використанням сучасних інформаційних технологій: підробка та використання пластикових платіжних карток та комп'ютерної банківської інформації. Відомою нині є діяльність міжнародної кібер мережі Avalanche, яка спеціалізувалася на кібер атаках з метою крадіжки пін-кодів, даних кредиток, розсилки спаму, DDoS-атак та ін. Збитки від діяльності цієї мережі сягають сотень мільйонів євро. Цікаво й те, що незважаючи на наявні докази, керівника злочинної організації, попередньо затриманого, — відпустили [148, с. 127-128; 162].

Особливістю злочинів у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж, мереж електрозв'язку є використанням

засобів комунікацій віддаленого доступу, тобто не потребується присутності правопорушників на безпосередньому місці вчинення злочину, адже особливість глобальної мережі — відсутність кордонів. Дедалі частіше хакери об'єднуються у групи, мають ознаки організованих злочинних угруповань. Хакерська субкультура за своєю суттю є унікальним явищем, яке не має аналогів, адже використання комунікаційних можливостей сучасних глобальних мереж для обміну кримінальним досвідом та координації своєї діяльності якісно відрізняє організовану комп'ютерну злочинність від інших злочинів. У мережах створюються спеціальні місця для спілкування: форуми, конференції з хакерською тематикою, спеціалізовані сайти. Нерідко відвідування таких місць може бути обмежено та захищено паролями, це свого роду «комп'ютерне підпілля», що означає особливе соціальне середовище у якому хакери підтримують один одного за рахунок спільного використання інформаційних ресурсів. З цією ж метою розповсюджено й використання псевдонімів. Зв'язки у злочинних угрупованнях можуть мати як тимчасовий, так і постійний характер з чіткою ієрархією та розподілом ролей у виконанні протиправного посягання [95, с. 190; 106, с. 136].

Розподіл ролей у комп'ютерній організованій злочинності та дослідження ролі організатора попередньо було окреслено, тож перейдемо до інших ймовірних учасників організованої комп'ютерної злочинності. Виконавцем (співвиконавцем) є особа, яка у співучасті з іншими суб'єктами злочину безпосередньо чи шляхом використання інших осіб, що відповідно до закону не підлягають кримінальній відповідальності за скоєне, вчинила злочин, передбачений КК України [78]. Наприклад, у березні 2018 року працівниками кіберполіції було виявлено причетність 30-річного мешканця Києва до розробки вірусів, кібершпигунства та продажу персональних даних громадян з усього світу. Також хакер збував шкідливе програмне забезпечення та створював віруси, які використовувалися для отримання віддаленого доступу до комп'ютерів жертв та подальшого всебічного контролю над ними. Поліцейськими було встановлено, що чоловік є учасником хакерського угрупування «Cobalt», члени якого причетні до масових атак на різноманітні світові банки. До його обов'язків входили розробка та підтримання належної роботи

експлойтів, які використовували вразливості у найбільш розповсюджених серед користувачів програмних продуктах. Тобто ми спостерігаємо чіткий розподіл ролей учасників. У межах кримінального провадження розпочатого за ст. 361 КК України встановлюються особи, яким зловмисник продавав шкідливе програмне забезпечення та допомагав в отриманні повного контролю над комп'ютерною технікою жертв [64]. У даному випадку описане злочинне діяння підпадає під вчинення злочину виконавцем, попередню кваліфікацію за якою доцільно проводити за статтею 361-1 Кримінального кодексу України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» [148, с. 128].

Підбурювачем є особа, яка умовлянням, підкупом, погрозою, примусом або іншим чином схилила іншого співучасника до вчинення злочину [78]. Ймовірно організовані злочинні угруповання мають у своїх "штатах" спеціалістів, які займаються розвідкою з використанням найсучасніших технічних засобів для збору необхідної інформації про діяльність конкурентів, засобів масової інформації, підприємств та фірм, які перебувають у межах їх інтересів, і правоохоронних органів. Серед комп'ютерних злочинів, які вчиняються у світі, все більше стає "міжнародних", таких, які у якості засобів або жертв використовують інформаційні системи різних держав світу, з можливістю доступу до національних, у тому числі й спеціально захищених інформаційних ресурсів, що створює нові умови для організованої злочинності — використання мережі Інтернет не тільки для здійснення правопорушень, а й для організації віртуальних банд. Таких учасників доцільно називати пособниками.

Пособником визнається особа, яка порадами, вказівками, наданням засобів чи знарядь або усуненням перешкод сприяла вчиненню злочину іншими співучасниками, а також особа, яка заздалегідь обіцяла переховувати злочинця, знаряддя чи засоби вчинення злочину, сліди злочину чи предмети, здобуті злочинним шляхом, придбати чи збути такі предмети, або іншим чином сприяти приховуванню злочину.

Злочин визнається вчиненим злочинною організацією, якщо його було скоєно стійким ієрархічним об'єднанням декількох осіб (п'яти і більше), члени або структурні частини якого за попередньою змовою зорганізувалися для спільної діяльності з метою безпосереднього вчинення тяжких або особливо тяжких злочинів учасниками цієї організації, або керівництва чи координації злочинної діяльності інших осіб, або забезпечення функціонування як самої злочинної організації, так і інших злочинних груп. Відповідно до статті 255 КК — створення злочинної організації з метою вчинення тяжкого чи особливо тяжкого злочину, а також керівництво такою організацією або участь у ній; участь у злочинах, вчинюваних такою організацією, а також організація, керівництво чи сприяння зустрічі (сходці) представників злочинних організацій або організованих груп для розроблення планів і умов спільного вчинення злочинів, матеріального забезпечення злочинної діяльності чи координації дій об'єднань злочинних організацій або організованих груп є злочином та караються позбавленням волі на строк від п'яти до дванадцяти років [78].

Стійкість організованої групи та злочинної організації полягає у здатності забезпечити стабільність та безпеку функціонування — ефективно протидіяти факторам, що можуть їх дезорганізувати, як внутрішнім (наприклад, невизнання авторитету або наказів керівника, намагання окремих членів об'єднання відокремитись чи вийти з нього), так і зовнішнім (недотримання правил безпеки щодо дій правоохоронних органів, діяльність конкурентів по злочинному середовищу тощо). На здатність об'єднання протидіяти внутрішнім дезорганізуючим факторам вказують, зокрема, такі ознаки: стабільний склад, тісні стосунки між його учасниками, їх централізоване підпорядкування, єдині для всіх правила поведінки, а також наявність плану злочинної діяльності і чіткий розподіл функцій учасників щодо його досягнення. Ознаками зовнішньої стійкості злочинних організацій можуть бути встановлення корупційних зв'язків в органах влади, наявність каналів обміну інформацією щодо діяльності конкурентів у злочинному середовищі, створення нелегальних (тіньових) страхових фондів та визначення порядку їх наповнення й використання тощо [148, с. 129]. У складі злочинів у сфері

використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку найбільшу небезпеку для суспільства, осіб та держави становлять злочини, що мають ознаки організованої злочинності: комп’ютерний тероризм; диверсія, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з баз даних та комп’ютерних програм; шахрайства з використанням комп’ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) тощо [55, с. 56]. Однією з таких кібер-угрупувань визнано — Sofacy Group, його відносять до типу розвиненої сталої загрози. Злочинне угрупування спеціалізується на кібер-шпигунстві за військовими та політичними установами, викраденні інформації, що становить інтерес зі сторони оборони та геополітики. Серед відомих жертв угрупування: Національний комітет Демократичної партії США, Німецький парламент, французька компанія TV5Monde, міжнародна антидопінгова асоціація WADA та ін. [193].

Організована комп'ютерна злочинність є серйозною загрозою державного рівня. На тлі віртуальності комп'ютерної злочинності виникає можливість організовувати свою діяльність на досить великих відстанях [148, с. 129]. Має сенс доповнити розділ XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» кваліфікуючими складами за вчинення комп'ютерних злочинів організованими групами та злочинними організаціями, підсилюючи кримінальну відповідальність за умови використання службового становища, не тільки до статті 362 КК, а й до інших норм розділу. Доцільно проводити кваліфікацію за сукупністю норм КК за статтею розділу XVI КК та статтею 255 КК України на тлі підвищеної суспільної небезпеки.

При кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку виникають питання, що стосуються розмежування комп'ютерних злочинів один від

одного та відмежування їх від інших злочинів, предмети яких тотожні з комп'ютерними.

Несанкціоноване втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку (ст. 361 КК), як і створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, їх розповсюдження, збут (ст. 361-1 КК) можуть призводити до несанкціонованого витоку, втрати, підробки, блокування інформації, спотворення процесу її обробки або до порушення встановленого порядку її маршрутизації, однак ці злочини мають ряд принципових відмінностей.

Створення програм або внесення до існуючих програм змін, призводять до вказаних в диспозиції статті 361-1 КК України наслідків, та може поєднуватися з неправомірним доступом до комп'ютерної інформації, що передбачено статтею 361 КК України. Наприклад, можливі випадки, коли винний з метою створення шкідливої програми несанкціоновано отримує доступ і копіює існуючу програму з подальшим внесенням у неї відповідних змін, які роблять цю програму шкідливою, у такому випадку виникає сукупність злочинів, відповідальність за які передбачена відповідно до ст. 361 та ст. 361-1 Кримінального кодексу України.

У якості замаху на внесення шкідливих змін до вже існуючих програм поєднаний з закінченим неправомірним доступом до комп'ютерної інформації слід кваліфікувати діяння особи, яка неправомірно скопіювавши існуючу програму і внісши в неї зміни, не змогла в силу незалежних від неї обставин довести таку програму до якості «шкідливої». У такому разі кваліфікація повинна проводитися за ч. 1 ст. 361, ч. 1 ст. 361-1 з посиланням на ч. 3 ст. 15 Кримінального кодексу України.

Також необхідно відрізняти несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку (ст. 361 КК) від порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, або порушення порядку чи правил захисту інформації, яка в них обробляється (ст. 363 КК). У деяких випадках неправомірний доступ може бути здійснено спільно з

порушенням правил експлуатації ЕОМ, системи ЕОМ або їх мережі, однак, сукупність даних злочинів повністю виключена у зв'язку з наявністю спеціального суб'єкта в складі злочину, передбаченого ст. 363 КК. Об’єктивна сторона незаконного втручання (ст. 361 КК України) полягає у діях, результатом яких комп’ютерна інформація (предмет злочину), перестає існувати або стає повністю/частково непридатною для задоволення інформаційної потреби, у той час як при вчиненні викрадення, привласнення, вимагання комп’ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем комп’ютерна інформація не знищується і не перекручується — нею заволодіває суб’єкт злочину, до того ж, як правило така інформація залишається у власника. Наступноа відмінність між складами цих злочину полягає видах умислу. Незаконне втручання може вчинятися як з прямим, так і з непрямим умислом, у той час як вчинення несанкціонованих дій з інформацією, особою, яка має право доступу до неї вчиняється з прямим умислом та корисливим мотивом.

Що стосується відмежування досліджуваного складу злочину від злочину, передбаченого ст. 363 КК «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем», різниця очевидна, адже відрізняються усі елементи складу злочину. Безпосереднім об’єктом несанкціонованого втручання є право власності на комп’ютерну інформацію; порушення правил експлуатації завдає шкоди відносинам щодо забезпечення встановленого порядку експлуатації електронно-обчислювальних машин, їх систем та комп’ютерних мереж. Об’єктивна сторона злочину передбаченого статтею 361 КК, полягає у незаконному втручанні, що спричинило знищення чи перекручення комп’ютерної інформації, або в розповсюдженні шкідливих програмних або технічних засобів; об’єктивна сторона злочину, передбаченого ст. 363 КК України полягає в порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж. Суб’єкт незаконного втручання є загальним; суб'єктом порушення правил

експлуатації автоматизованих електронно-обчислювальних машин є особа, яка відповідає за їх експлуатацію. За ознаками суб'єктивної сторони — психічне ставлення особи до вчинення незаконного втручання характеризується умислом; порушення правил експлуатації ЕОМ, систем або комп'ютерних мереж характеризується змішаною формою вини: стосовно порушення правил експлуатації можливий як умисел, так і необережність, а відносно наслідків (викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, незаконне копіювання комп'ютерної інформації, істотне порушення роботи ЕОМ, їх систем чи комп'ютерних мереж) – тільки необережність. Якщо особа умисно порушує правила експлуатації і її умислом (прямим або непрямим) охоплюється настання зазначених наслідків, то такі дії слід розцінювати як несанкціоноване втручання (ст. 361 КК України) або як викрадення, привласнення, вимагання комп'ютерної інформації або (відповідно за метою) заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362 КК України) [61, с. 10].

Таким чином, комп'ютерні злочини хоча й захищають охоронюваний законом інтерес у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, проте дослідивши елементи даних складів злочинів, на наш погляд, між ними існують суттєві відмінності, що й передбачено існуванням шести статей, а не однією. У окремо взятих випадках такі склади злочинів можливо кваліфікувати за сукупністю.

Останнім часом, з приводу кваліфікації діянь за нормами Розділу XVI КК України та за суміжними складами злочинів у кримінальній практиці виникає чимало проблем. Це обумовлено стрімким розвитком інформаційних технологій, різноманітністю злочинної активності у цій сфері, елементи якої проникають у все більшу частину охоронюваних кримінальним законом відносин. Усе частіше вчиняються злочини, які не тільки пов'язані із заподіянням шкоди відносинам в сфері використання комп'ютерних систем, але й суспільно небезпечні посягання на інші, традиційні об'єкти: національну безпеку, власність, громадську безпеку, громадський порядок та моральність, інші не менш важливі суспільні відносини і навіть життя та здоров'я осіб використовуючи інформаційно телекомунікаційні

системи. Аналіз даних «Єдиного звіту про кримінальні правопорушення» (форма 1), дозволив дійти до висновку, що кваліфікація кіберзлочинів за статтями, які не містяться у Розділі XVI КК України, призводить до викривлення статистичної звітності та є однією з причин неможливості встановлення реального уявлення про злочинність, як наслідок, частка злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в загальній структурі злочинності є незначною й становить менше 1% [53].

Крім комп'ютерних злочинів кримінальний кодекс України передбачає відповідальність за ряд інших злочинів, предметом яких також може бути комп'ютерна інформація або які вчинені за допомогою електронно-обчислювальних мереж, систем та комп'ютерних мереж чи мереж електрозв'язку. До числа таких злочинів можливо віднести: посягання на територіальну цілісність і недоторканність України (ст. 110 КК), державна зрада (ст. 111 КК), шпигунство (ст. 114 КК), незаконна лікувальна діяльність (ст. 137 КК); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК), порушення авторського права і суміжних прав (ст. 176 КК); порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію (ст. 177 КК), шахрайство (ст. 190 КК), незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків електронними грошима, обладнанням для їх виготовлення (ст. 200 КК); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК); створення злочинної організації (ст. 255 КК), сприяння учасникам злочинних організацій та укриття їх злочинної діяльності (ст. 256 КК), хуліганство (ст. 296 КК); розголошення державної таємниці (ст. 328 КК), передача або збирання відомостей. що становлять конфіденційну інформацію, яка знаходиться у володінні держави (ст. 330 КК) та ін.

Застосовуючи кримінально-правові норми, кваліфікуючій особі необхідно визначити, яку з кількох норм КК України слід застосувати. Коли достатньо

інкримінувати порушення однієї норми та, у яких випадках необхідно оцінювати скоєне у якості злочину, передбаченого двома чи більше статтями Особливої частини КК. За дослідженням вченого Д.В. Пашнєва найчастіше помилки зустрічаються при кваліфікації одного діяння, яке, на перший погляд, містить ознаки декількох складів злочинів. Отже, основною проблемою, вирішення якої впливає на правильність кваліфікації злочинів є визначення наявності або відсутності у вчиненому ідеальної сукупності злочинів [108, с. 258] або ж, якщо трактувати інакше, — необхідно подолати існуючу конкуренцію правових норм злочинів передбачених Розділом XVI КК України та іншими розділами КК України.

Сукупністю злочинів у кримінальному праві називається вчинення особою двох або більше злочинів, передбачених різними кримінально-правовими нормами, за жоден з яких її не було засуджено.

Згідно зі ст. 33 КК України сукупність злочинів характеризується такими ознаками:

1) вчинення однією особою двох або більше злочинів, передбачених різними статтями кримінального закону (різними кримінально-правовими нормами); скоєне не охоплюється одним складом злочину;

2) діяння вчинені однією особою мають різні юридичні ознаки, підпадають під ознаки різних статей або різних частин однієї статті кримінального закону;

3) за вчинені злочини особа ще не притягалася до кримінальної відповідальності і не була за них засудженою [78].

Зазначені у ст. 33 КК України ознаки сукупності злочинів мають важливе значення для кваліфікації злочинів, які утворюють сукупність. При кваліфікації сукупності злочинів необхідно враховувати, що сукупність утворюють різні злочини, передбачені різними кримінально-правовими нормами, які мають власні санкції. **Не буде сукупності злочинів у тих випадках, коли вчинені діяння передбачені різними пунктами однієї статті, якщо ці пункти не мають власних санкцій.** Таке діяння кваліфікується як один злочин, але до вини додаються всі ті пункти, які є у діях винної особи.

Криміналісти XIX століття сукупність злочинів називали «збігом злочинів», що на їх думку більш повно і точно розкривало сутність такого юридичного явища. Однією з нпйголовніших ознак сукупності злочинів є вчинення двох або більше злочинів до засудження хоча б за один із них [72, с. 40-41].

У науці кримінального права сукупність злочинів поділяється на **два види**: ідеальну та реальну. **Ідеальна сукупність** наявна там, де одним діянням особа вчиняє два або більше злочинів [163].

За Д.В. Пашнєвим та О.О. Авдєєвим у процесі вчинення кіберзлочину шкода може завдаватися суспільним відносинам у трьох **варіантах:**

1) суспільним відносинам, які виникають в ході забезпечення за допомогою інформаційно телекомунікаційних систем (ІТС) життєдіяльності людини, суспільства, держави;

2) традиційним суспільним відносинам, охоронюваним кримінальним законом, які забезпечуються за допомогою ІТС, цілеспрямований шкідливий вплив на які використовується для завдання шкоди цим відносинам;

3) традиційним суспільним відносинам, охоронюваним кримінальним законом, для нанесення шкоди яким використовуються ІТС, які, в свою чергу, не зазнають при цьому шкоди.

Перша група відносин охороняється Розділом XVI Особливої Частини КК (злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку). Ці відносини є частиною другої та третьої групи відносин, але в другій групі вони зазнають шкоди разом із традиційними відносинами кримінально-правової охорони, а в третій — ні [108, с. 259].

Ідеальною сукупністю злочинів вважається два або більше злочинів вчинених одним діянням. Відповідно до вказаних груп відносин, що зазнають шкоди при вчиненні такого діяння у випадку вчинення кіберзлочину, можна виділити три групи цих злочинів, що будуть мати свої особливості кваліфікації відповідно до діючого КК:

1) злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку (Розділ XVI Особливої Частини КК);

2) злочини, що кваліфікуються за статтями КК відповідно до об’єкту посягання з додатковим посиланням на статті Розділу XVI Особливої Частини КК;
3) злочини, що кваліфікуються за статтями КК відповідно до об’єкту посягання без додаткового посилання на статті Розділу XVI Особливої Частини КК.

Тобто, діяння з першої та третьої групи є одиничними злочинами, а з другої — ідеальною сукупністю злочинів. На практиці застосування норм КК з протидії кіберзлочинам, діяння що відносяться до різних із вказаних груп, часто плутаються. Найчастіше, злочини другої групи кваліфікуються тільки за однією статтею, і навпаки, злочини першої чи третьої групи кваліфікуються за декількома статтями, хоча не потребують додаткової кваліфікації. При цьому стаття, яка застосовується при кваліфікації другої групи злочинів, або із Розділу XVI Особливої Частини КК, або інша — відповідно до безпосереднього об’єкту посягання. Очевидно, що в обох випадках частина злочину кваліфікацією не охоплюється, що порушує принципи повноти та точності кваліфікації, а у разі кваліфікації одного діяння, яке містить один склад злочину, за двома статтями порушується ще й принцип заборони подвійного інкримінування.

Раніше нами було висвітлено особливості неправомірного доступу до комп'ютерної інформації (об'єктивна сторона ст. 361 КК). Дедалі частіше зустрічаються випадки неправомірного доступу до інформації приватного характеру як комерційних, так і державних структур які займаються збором інформації про громадян. Втручання у приватне життя людини (цікавить саме інформація), — заборонено, проте існують певні випадки коли ця заборона зникає у зв'язку з необхідністю розкриття злочинів. Відповідно до кримінально-процесуального кодексу України одним з різновидів слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених КПК є негласні слідчі (розшукові) дії (ст. 246 КПК). Аудіо-, відеоконтроль особи (ст. 260 КПК), накладення арешту на кореспонденцію (ст. 261 КПК), огляд і виїмка кореспонденції (ст. 262 КПК), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК), зняття інформації з електронних інформаційних систем (ст. 264 КПК) — проводяться на підставі ухвали

слідчого судді; моніторинг банківських рахунків (ст. 269-1 КПК) — проводиться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. Рішення про проведення негласних слідчих (розшукових) дій приймає слідчий, прокурор, у певних випадках, — слідчий суддя за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором. Проводити негласні слідчі (розшукові) дії має право слідчий, який здійснює досудове розслідування злочину, або за його дорученням — уповноважені оперативні підрозділи Національної поліції, органів безпеки, Національного антикорупційного бюро України, Державного бюро розслідувань, органів, що здійснюють контроль за додержанням податкового і митного законодавства, органів Державної кримінально-виконавчої служби України, органів Державної прикордонної служби України. За рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій можуть залучатися також інші особи [79, ст. 246, 260, 262, 263, 264, 269-1].

Тобто ми бачимо, що кримінально-процесуальним кодексом визначено процедуру доступу до приватної інформації, яка необхідна у певних випадках, проте виникає питання — чи завжди дотримується процедура доступу до особистої інформації та є необхідність її проведення? На наш погляд, немає жодної гарантії, що нашу пошту/смс — не читають та не копіюють; дзвінки — не прослуховують, або ж записують; не проглядають банківські рахунки, як співробітники правоохоронних, так і банківських органів; або ж ще краще — не слідкують через камеру телефону або ж комп'ютеру, ноутбуку і т.д. Таким чином, несанкціонований доступ до комп'ютерної інформації (ст. 361 КК України) і порушення таємниці приватного життя (ст . 182 КК України) є суміжними злочинами, хоча і мають ряд принципових відмінностей.

Цікаво й те, що суміжність цих злочинів не є перешкодою для їх кваліфікації за сукупністю. Особа, здійснюючи неправомірний доступ до інформації, що містить таємницю приватного життя, копіює її на носій комп'ютерної інформації, то кваліфікувати це діяння слід за правилами ідеальної сукупності злочинів, а саме за ч. 1 ст. 182 КК і ч. 1 ст. 361 КК України. Нерідко подібні злочини скоюються

особами, які використовують своє службе становище (наприклад, співробітниками правоохоронних органів), у таких випадках кваліфікація скоєного повинна проводитися за сукупністю ч. 1 ст. 182 КК і ч. 1, ч.2 ст. 362 КК. Аналогічна ситуація складається при порушенні таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції (ст. 163 КК).

Велика частка кіберзлочинів припадає на випадки, коли посягання у сфері використання ІТС здійснюється з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням потерпілим матеріальної шкоди і є способом вчинення таких злочинів проти власності, як шахрайство (ст.190 КК) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК). У більшості випадках суди кваліфікують такі дії за сукупністю злочинів: за статтею Розділу XVI особливої частини КК і тією статтею, якою передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС [108, с. 259-260]. Наприклад, Красногвардійський районний суд м. Дніпропетровська визнав Є. винним за ч.1 ст.361 КК і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ «ПриватБанк» надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв'язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ «Приват-Банк» [164]. Автор узагальнення з якого взятий цей приклад, вважає, що оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст.190 КК (шахрайство). Вважаємо, що тут дійсно наявна сукупність злочинів, але вона вже врахована в КК у ч.3 ст.190, отже достатньо кваліфікації за цією нормою без додаткових посилань на інші норми КК [108, с. 260].

Поглибимось трохи у випадки комп'ютерного шахрайства. Раніше повідомлялося, що інтернет-шахраї почали виманювати гроші українських інтернет-користувачів за допомогою трояна з повідомленням про блокування системи за нелегальну діяльність від імені Служби безпеки України (СБУ). Починаючи з квітня 2013 року стало відомо, що злочинці озброїлись Skype для розповсюдження шкідливих програм. Експерти Лабораторії Касперського (ЛК) виявили дві шкідливі кампанії в Skype, які набирали оберти. Як стало відомо Корреспондент.biz, в обох випадках зловмисники заманювали користувачів перейти за шкідливим посиланням методами соціальної інженерії, обіцяючи цікавий фото- або відео- контент. За даними ЛК, для поширення шкідливих посилань використовуються викрадені або спеціально створені Skype-акаунти, а кінцевою метою однієї з кампаній ймовірно є шахрайська генерація віртуальної валюти Bitcoin. Користувачі отримували повідомлення з закликом перейти за посиланням, однак, як з'ясували фахівці ЛК, на цей раз разом зі шкідливою програмою на комп'ютер користувача встановлювалася спеціальна програма для генерації віртуальної валюти Bitcoin. Ця валюта дозволяє заробляти гроші за рахунок надання обчислювальних ресурсів комп'ютера, на якому встановлено спеціалізований додаток. Учасник системи надає свій комп'ютер для проведення обчислень, а натомість отримує монети Bitcoin, які згодом можна конвертувати в іншу валюту або використовувати для оплати товарів і послуг у деяких інтернет-магазинах. «В силу анонімності і неконтрольованості такі угоди дуже важко відстежити, тому злочинці почуваються дуже комфортно», — підкреслив експерт ЛК Сергій Ложкін [63].

Злочин вчинявся за допомогою шкідливих програм, що вживлювались у ПК інших користувачів комп'ютерних мереж. Окреслене не підпадає під кваліфікацію жодної зі статей розділу XVI КК України, а скоріш нагадує шахрайство. До того ж, з розвитком комп'ютерних технологій вчинення злочинів стало зручнішим та доступнішим, адже комп'ютерні програми відкривають нові можливості для розвитку злочинності, наприклад, за допомогою різноманітних фото-редакторів у процесі створення зображень, складених з частин різних фотографій (фотомонтаж), можливо у короткі строки без особливих знань та надмірних навантажень підробити

підпис, або й створити новий документ скомбінувавши певні елементи існуючих документів — довіреність, договір і т.д., що можна кваліфікувати за ч.1 ст. 358 КК України «Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів». Що стосується документів, вони напевне не будуть мати чинності, адже ні печатка, ні штамп не будуть справжніми, тим паче, якщо певним документам присвоюється реєстровий номер [116, п. 6] (договори, заповіти, довіреності, свідоцтва про право на спадщину і т.д. [125, ст. 34]), добре коли їх перевіряють; що ж стосується документів, яким не присвоюється реєстровий номер, або ж якщо вони потрапили до рук людини не обізнаної про особливості діловодства, то їх ввести у оману досить легко, особливо, коли документи не мають рівня державного значення і не спричиняють великої шкоди, відповідно з'являється питання: чи доцільно розглядати їх з кримінально-правової точки зору у якості злочину? Зовсім інша справа, якщо шахрайство вчиняється банками і фірмами, коли справа йде про великі гроші. Що заважає, наприклад, фірмі Z підробити певні документи, щодо клієнта? Впевнені, що такі випадки шахрайства не рідкість.

Кваліфікація за ознаками шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки також є проблемним і остаточно не вирішеною для науки кримінального права, але більшість його аспектів потребують окремого дослідження, а тому зупинимося у цьому дослідженні лише на наявності в цьому випадку ідеальної сукупності, яка вже врахована законодавцем. На відсутність необхідності додаткової кваліфікації у таких випадках чітко вказував Пленум Верховного Суду України в часи свого існування: «...шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, має кваліфікуватися за ч.3 ст. 190 КК і додаткової кваліфікації не потребує». Але перед цим Пленум чітко вказує: «Якщо обман чи зловживання довірою при шахрайстві полягають у вчиненні іншого злочину, дії винної особи належить кваліфікувати за відповідною частиною статті 190 КК і статтею, що передбачає відповідальність за цей злочин» [138].

Таким чином, перед нами постає одна з основних проблем кримінально-правової кваліфікації — поглинання одного злочину іншим, який був його частиною. У деяких випадках, умисне заподіяння істотної шкоди в результаті комп'ютерного злочину може фактично представляти собою склад іншого злочину. Наприклад, цілком очевидно, що знищення надзвичайно важливої для обороноздатності країни комп'ютерної інформації з метою ослаблення держави не представляє собою несанкціоноване втручання, яке спричинило істотну шкоду (ч.2 ст.361 КК), а є нічим іншим як диверсія (ст.113 КК) [73, с. 146].

Науковець М.Й. Коржанський, виводячи правила кваліфікації за сукупністю на підставі досягнутих ним висновків, вивів загальне правило: **якщо вчинене є посяганням на різні безпосередні об'єкти кримінально-правової охорони, то його належить кваліфікувати як сукупність злочинів** [72, с. 60]. В наведеному ж вище випадку безпосередні об'єкти різні, отже підстав кваліфікувати описаний злочин як одиничний бути не повинно. У той же час М.Й. Коржанський уточнює своє правило стосовно злочинів, які мають додаткові об'єкти посягання: діяння, при якому заподіяння шкоди додатковому безпосередньому об'єктові посягання є способом, складовою частиною заподіяння шкоди головному безпосередньому об'єктові, слід кваліфікувати як одиничний злочин; діяння, при вчиненні якого шкода заподіюється додатковому об'єкту, слід кваліфікувати за сукупністю злочинів [108, с. 260-261].

Дослідженням кваліфікації злочинів за сукупністю займався й науковець Т.І. Созанський, за його словами: «Якщо об'єкти злочинів співвідносяться як основний і додатковий, то діяння необхідно кваліфікувати як одиничний злочин, якщо ж обидва (чи більше) об'єктів є основними, то діяння утворює ідеальну сукупність злочинів». Але далі він вказує, що визначити, коли об'єкт є додатковим, а коли він переходить у основний, буває складно. Це набуває критичного значення при оцінці кіберзлочину, адже з точки зору отримання шкоди відділити відносини в сфері використання ІТС від відносин, автоматизацію яких вони забезпечують, в більшості випадків дуже складно. Т.І. Созанський пропонує, одним із варіантів вирішення цього питання, визначати суспільну небезпечність посягань на

відносини, які охороняються цими об'єктами. **Якщо суспільна небезпечність відносин, що охороняються додатковим об'єктом, є більшою, ніж основного об'єкта, то діяння утворює ідеальну сукупність** [156, с. 133]. У практичну площину цю рекомендацію перевів Пленум Верховного Суду України у постанові, яка стосується судової практики застосування норм про множинність злочинів [134]. У п.11 цієї постанови вказано: «Якщо у складі злочину передбачене діяння, яке у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання про його кримінально-правову оцінку необхідно вирішувати з урахуванням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей (частин статей) Особливої частини КК. У випадках, коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діяння і санкцією статті (частини статті) Особливої частини КК встановлене за цей злочин більш суворе максимальне основне покарання, ніж за відповідне діяння, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує». В даному випадку Пленум Верховного Суду України фактично суперечить своїм же рекомендаціям щодо кваліфікації за ст.190, наведеним вище, але при цьому, він підтримав висловлену вище думку науковців, яка, на наш погляд, є найбільш вірним виходом із цієї складної ситуації.

Відповідно до узагальнення судової практики з питань кваліфікації повторності та сукупності злочинів призначаючи покарання за сукупністю злочинів, суди призначають таке покарання за кожний злочин окремо, а остаточне покарання призначається за правилами, передбаченими ст. 70 КК. Зокрема, за наявності сукупності злочинів суди, призначивши покарання (основне і додаткове) за кожний злочин окремо, визначають остаточне покарання шляхом поглинення менш суворого покарання більш суворим або шляхом повного чи часткового складання призначених покарань. При складанні покарань остаточне з них за сукупністю злочинів суди визначають в межах, встановлених санкцією статті Особливої частини КК, яка передбачає більш суворе покарання. Суди призначають покарання за сукупністю злочинів, якщо після постановлення вироку в справі було

встановлено, що засуджений винен ще й в іншому злочині, вчиненому ним до постановлення попереднього вироку [171].

Таким чином, слід визнати за правило кваліфікації кіберзлочинів, які через посягання на відносини в сфері використання ІТС посягають на інші «традиційні» відносини, які забезпечуються цими ІТС, наступне: у разі, коли складом певного злочину охоплюється вчинене одночасно з цим злочином діяння, передбачене статтею Розділу 16 Особливої Частини КК, і санкцією статті (частини статті) Особливої частини КК встановлене за цей злочин більш суворе максимальне основне покарання, ніж за діяння, передбачене статтею Розділу 16 Особливої Частини КК, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує [108, с. 261-262]. Не буде сукупності злочинів у тих випадках, коли вчинені діяння передбачені різними пунктами однієї статті, якщо ці пункти не мають власних санкцій. Якщо ж вчинене є посяганням на різні безпосередні об’єкти кримінально-правової охорони, то його належить кваліфікувати як сукупність злочинів. Якщо суспільна небезпечність відносин, що охороняються додатковим об’єктом, є більшою, ніж основного об’єкта, то діяння утворює ідеальну сукупність.

Подолання конкуренції і колізії правових норм під час кримінально-правової кваліфікації злочинів у сфері інформаційних технологій допоможе здійснити вірну кваліфікацію вчинених злочинів та призначити справедливе покарання.

Висновки до розділу 3

1. Об'єктом кібернетичних злочинів виступають суспільні відносини, яким завдається шкода, внаслідок впливу на інформацію, що обертається у кібернетичних системах.

2. Предмети комп'ютерних злочинів багатогранні та визначаються в залежності від норми статті, що підпадає під вчинюване діяння, однак об'єднує їх одне — ними виступає інформація, яка маючи різні форми, обертається у електронно-обчислювальних мережах, системах та комп'ютерних мережах, мережах мелектрозв'язку.

Пропонуємо доповнити Розділ XVI Кримінального кодексу України, а саме статті 361, 362 та 363 такими поняттями, як: банкомати та термінали, з метою розтлумачення певних видів злочинної діяльності, та вважати комп'ютерне шахрайство кібернетичним злочином.

3. З огляду на існування кримінального покарання за порушення авторського права (стаття 176 Кримінального кодексу України), заборону вторгнення до особистого простору людини (стаття 163, 182 Кримінального кодексу України), пропонуємо ввести кримінальну відповідальність за копіювання особистих даних осіб у разі використання таких зі злочинними намірами, наприклад, злам баз даних, внаслідок чого з дійсними копіювання особистої інформації клієнтів банку, адже наслідками використання даних можуть стати поява великої кількості нових злочинів.

Пропонуємо доповнити статтю 361 Кримінального кодексу 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 її розпорядження».

Відповідно до норми статті 361-1 Кримінального кодексу України, кримінальна відповідальність передбачена за виготовлення шкідливих програм, вбачаючи високий ступінь суспільної небезпеки та формальність його складу, пропонуємо ввести кримінальну відповідальність за підготовчі дії до вчинення злочину та посилити відповідальність за замах на створення з метою використання, розповсюдження або збуту шкідливих програмних, технічних засобів, їх розповсюдження або збут за умови настання суспільно-небезпечних наслідків від підготовчих дій.

Виходячи зі змісту частини 2 статті 362 Кримінального кодексу України, пропонуємо виключити поняття «перехоплення», адже у такому випадку відсутній доступ суб'єкта до охоронюваної законом інформації. Пропонуємо ввести нову статтю до Розділу XVI, яка передбачатиме відповідальність саме за перехоплення інформації, яка оброблюється в ЕОМ, АС, комп'ютерних мережах або зберігається

на носіях такої інформації, вчинені особами, які не мають на це права доступу, або ж доповнити статтю 361-2 Кримінального кодексу України.

Статтею 363 Кримінального кодексу України прямо не встановлено за настання яких саме наслідків у розмірі значної шкоди передбачається покарання, пропонуємо доповнити статтю таким 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».

У зв'язку з відсутністю законодавчих актів, які б прямо визначали правила експлуатації ЕОМ, систем та мереж. пропонуємо здійснити судове або ж правозастосовне тлумачення у вигляді роз'яснень, наприклад на рівні Постанов Пленуму Верховного Суду.

Враховуючи контингент користувачів комп'ютерних технологій пропонуємо понизити вік настання кримінальної відповідальності з 16 років на 14 років.

Дослідив норму статті 362 Кримінального кодексу України вважаємо, за потрібне доповнити норму таким чином: «... наявність в особи права доступу до інформації та реалізації такої можливості зі злочинним наміром».

Пропонуємо доповнити існуючі форми вини — злочинною необачністю, яка б включала у себе ознаки непрямого умислу і злочинної самовпевненості (легковажності), саме така форма вини притаманна ст. 361-1 Кримінального кодексу України.

Має сенс доповнити розділ XVI Кримінального кодексу України кваліфікуючими складами за вчинення комп'ютерних злочинів організованими групами та злочинними організаціями, підсилюючи кримінальну відповідальність за умови використання службового становища, не тільки до статті 362 КК, а й до інших норм розділу. Доцільно проводити кваліфікацію за сукупністю норм КК за статтею розділу XVI КК та статтею 255 КК України та тлі підвищеної суспільної небезпеки.

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 кваліфікція» 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 аппарату у національному законодавстві України ускладює 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. Грунтуючись 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 сорони 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). Звернуто увагу на тому, 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) злочинів є їх вчинення: 1) повторно; 2) за попередньою змовою групою осіб; 3) заподіяння ними істотної шкоди.

Відмічено, що застосування статті 361-1 КК можливе лише за умови встановлення, що винний знав про шкідливість програм. Враховуючи, що у «формальних» складах, де є характеристика інтелектуального моменту умислу, – завідомість, 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 з 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'ютеру (ЕОМ) у мережі «Інтернет». Проблему становить невизначеність застосування законодачого регулювання, подекуди місцем скоєння злочину і місцем настання суспільно-небезпечних наслідків є різні країни. Обгрунтовано надання правовому режиму мережі Інтернет статус, подібний до статусу територій загального користування.

– при здійсненні кримінально-правової кваліфікації необхідное подолати конкуренціїю 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 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 жерті 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 перелічуватимуться на рахунок потерпілих.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д.С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. 304 с.

2. Александров Ю.В., Дудоров О.О., Клименко В.А. та ін. Кримінальне право України. Особлива частина: підр. авт. кол.: За ред. М. І. Мельника, В. А. Клименка. Київ: Юридична думка, 2004. 656 с.

3. Амелін О.Ю. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. Вип. № 3. С. 1–10.

4. Аналіз розділу XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». URL: http://adhdportal.com/book_1704_chapter_12_2.3._Analz_rozdlu_XVIKK_Ukrani_"Zlochini__sfer_vikoristannja_elektronnoobchisljuvalnikh_mashin(komp'juterv),_sistem_ta_komp'juternikh_merezh&qu.html.

5. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. Москва: «Юрлитинформ», 2001. 152 с.

6. Андрушко П.П. Об'єкти кримінально-правової кваліфікації: поняття, види. Тези міжн. наук. конф.: *«Проблеми юридичної кваліфікації (теорія і практика)»*. Вісник Академії адвокатури України. Число 1 (17) 2010. С. 150-157. URL: http://nbuv.gov.ua/UJRN/vaau_2010_1_29.

7. Анісімов Г.М., Володіна О.О., Зінченко І.О. та ін. Кваліфікація злочинів : навч. посіб.; за ред. М. І. Панова. Харків. : Право, 2016. 356 с.

8. Батурин Ю.М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. Москва: Юрид. лит., 1991. 160 с.

9. Батурин Ю.М. Проблемы компьютерного права. Москва: Юрид. лит., 1991. 268 с.

10. Баулін Ю.В. Борисов В.І., Кривоченко Л.М., Ломако В.А., Панов М.І., Сташис В.В., Тацій В.Я., Тихий В.П., Тютюгін В.І. Кримінальне право України:

Загальна частина: підр. за ред. проф. В. В. Сташиса, В. Я. Тація. 4-те вид., переробл. і допов. Харків: Право, 2010. 608с. URL: https://coollib.com/b/322718/read.

11. Баулін Ю.В. Проблеми застосування кримінально-правових норм органами досудового слідства. Правова система України: історія, стан та перспективи: у 5т.: Т. 5: Кримінально-правові науки: «Актуальні проблеми боротьби зі злочинністю в Україні». за заг. ред. В.В. Сташиса. Харків: Право, 2008. 840 с.

12. Беккариа Ч.О преступлениях и наказаниях: пер. с итал. Киев.: Ин Юре, 2014. 240 с.

13. Бельський Ю.А. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. Вип. № 6, 2014. С. 414 - 418.

14. Бернська конвенція про охорону літературних і художніх творів: Паризький Акт від 24.07.1971 змінений 2.11.1979 № 995_051 (приєднання 31.05.1995). URL: http://zakon3.rada.gov.ua/laws/show/995_051.

15. Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: дис. ..канд. юрид. наук. Н. Новгород, 2000. 249 с.

16. Бєлєнький В.П. Сучасна історія злочинів у сфері комп'ютерної безпеки. *Правова держава*. Вип. №1 (3), 2011.С. 96-101.

17. Бидашко Е.А., Волкова Н.Л. Компьютерные преступления: миф или реальность?. Науковий вісник Дніпропетровського юридичного інституту Міністерства внутрішніх справ України. 2001. Вип. №1 (14). С. 160-168.

18. Битяк Ю.П., Богуцький В.В., Гаращук В.М. та ін. Адміністративне право України: підр. для юрид. вузів і ф-тів. Харків: Право, 2000. 520 с.

19. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соцально-правові та кримінолого-криміналістичні аспекти : навч. пос. Київ : українська академія внутрішніх справ, 1994. 128 с.

20. Біленчук П.Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.

21. Болгов В.М., Гадіон Н.М., Гладун О.З. та ін. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з

використанням інформаційних технологій: наук.-практ. посіб. Київ: Національна академія прокуратури України, 2015. 202 с.

22. Борисова Л.В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права*. 2008. Вип. № 44. С. 76-81.

23. Брайнин Я.М. Уголовная ответственность в советском уголовном праве. Москва, 1963. 275 с.

24. Бусел В.Т. Великий тлумачний словник сучасної української мови. Київ; Ірпінь : ВТФ «Перун», 2003. 1728 с.

25. Бутузов В.М., Кузьмін С.А., Шеломенцев В.П. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: наук.-практ. ком. Київ: ПАЛИВОДА А.В., 2010. 152 с.

26. Бутузов В.М., Остапець С.Л., Шеломцев В.П. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. ком. Київ : Друкарня МВС України, 2005. 86с.

27. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 148 с.

28. Васильєв А.А., Пашнєв Д.В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України*. Вип. № 5. 2013., С. 34-42.

29. Вереша Р.В. Кримінальне право України. Загальна частина: навч. посіб. 2-ге вид. перероб. та доп. станом на вересень 2011 р. Київ: Центр учбової літератури, 2012. 320 с.

30. Вехов В.Б. Компьютерные преступления: Способы совершения, методики расследования. Москва: Право и закон, 1996. 179 с.

31. Виды компьютерных вирусов, и способы борьбы с ними // Web 3.0. URL: http://comp.web-3.ru/virus/?act=full&id_article=1411.

32. Відповідальність у міжнародному праві та мирні засоби розв'язання міжнародних спорів. Національна академія Внутрішніх справ. Мультимедійний посібник з навчальної дисципліни «Міжнародне право». URL: http://www.naiau.kiev.ua/books/mg/lectures/lecture_8.html.

33. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества Москва: ООО Издательство «Юрлитинформ», 2002. 496 с.

34. Воробьев В.В. Преступления в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 Москва: РГБ, 2003. 201 с.

35. В Україні на початок 2017 року нараховано 21,6 млн користувачів інтернету // Semantrum.URL: https://promo.semantrum.net/ uk/2017/04/21/v-ukrayini-na-pochatok-2017-roku-narahovano-21-6-mln-koristuvachiv-internetu.

36. Гаврилов О.А. Основы правовой информатики: учеб. пос.. Москва: Институт государства и права РАН, 1998.42 с.

37. Гавриш С.Б. Кримінально-правова охорона довкілля в Україні. Київ: Інст. Законод. Верховної Ради України, 2002. 636 с.

38. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. Москва: АО «Центр ЮрИнфоР», 2003. 448 с.

39. Голубєв В.О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту*. 1997. Вип. № 2. С. 39 - 40.

40. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.

41. Голубев В.О. Суб'єкт злочинної діяльності у сфері використання електронно-обчислювальних машин. *Підприємництво, господарство і право*. 2004. Вип. № 6. С. 105-111.

42. Гринберг М.С. Преступления против общественной безопасности: учеб. пос. Свердловск: Свердловский юрид. ин-т, 1974. 351 с.

43. Гринчак І.В. Кіберзлочинність як злочин міжнародного характеру. *Науково-інформаційний вісник Івано-Франківського університету права імені*

Короля Данила Галицького. 2015. Вип. № 12. С. 93-98. URL: http://nbuv.gov.ua/UJRN/Nivif_2015_12_15.

44. Гуцалюк М. І Україна та Internet: перспективи розвитку . Електронна стаття «Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet». Центр информационной безопасности. URL: http://www.bezpeka.com/ru/lib/spec/law/legal-protection-information-systems-Internet.html.

45. Директива 97/7/ЄС Європейського парламенту та Ради «Про захист прав споживачів в дистанційних контрактах» від 20.05.1997 № 994_245 (у ред. 23.09.2002). URL: http://zakon2.rada.gov.ua/laws/show/994_245.

46. Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 року та положення Бернської конвенції (1971 р.), на які містяться посилання у Договорі (Договір ВОІВ про авторське право) (1996) від 20.12.1996 № 995_770 (приєднання 20.09.2001). URL*:* http://zakon2.rada.gov.ua/laws/show/995_770.

47. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21.07.2006 № 23-V (ратифікація 21.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_687.

48. Дуда Х.І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2014. Вип. № 197. Ч. 1. С. 262 - 267.

49. Дудоров О.О., Письменський Є. О. Кримінальне право (Особлива частина): підр. 2-ге вид. Київ: "ВД "Дакор", 2013. 786 с. URL: http://pidruchniki.com/1726062160070/pravo/zlochini_sferi_vikoristannya_elektronnoobchislyuvalnih_mashin_kompyuteriv_sistem_kompyuternih_merezh_merezh_elektrozvyazku.

50. Європейська конвенція про видачу правопорушників від 13.12.1957 № 995_033 (у ред. 20.09.2012). URL: http://zakon3.rada.gov.ua/laws/show/995_033.

51. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. Число 3. С. 129-136.

52. Єдиний звіт про кримінальні правопорушення по державі. Офіційний сайт Генеральної прокуратури України URL : https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402.

53. Звіт судів першої інстанції про розгляд матеріалів кримінального провадження за 2017 рік . Офіційний сайт Судова влада України. *URL:* https://court.gov.ua/inshe/sudova_statystyka/rik_2017.

54. Здравомыслов Б.В. Уголовное право РФ. Особенная часть: учебник. Москва: Юрист, 1996. 559 с.

55. Злобін Д.Л. Взаємодія операторів мобільного зв'язку з ОВС при розслідуванні комп'ютерних злочинів. Матеріали регіонального наук.-практ. сем., м. Донецьк, 12 грудня 2008 р. Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк : ДЮІ ЛДУВС, 2009. С. 56–61.

56. Игошев К.Е. Типология личности преступника и мотивация преступного поведения. Горький, 1974. 167 с.

57. Иксар В. Компьютерные преступления. URL: http://www.comprice.ru/articles/detail.php?ID=42319.

58. Как создать, написать компьютерный вирус? . Сайт немного про Windows. URL: http://about-windows.ru/virusy-i-xakery/pishem-virusy/sozdaem-virus.

59. Карпец И.И. Преступления международного характера. Москва : Юрид. лит., 1979. 111 с.

60. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки: навч. пос. Київ: Атіка, 2010. 168 с.

61. Карчевський М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину): автореф. дис. канд. юрид. наук., Харків, 2003. 15 с.

62. Киберпреступность становится более организованной . Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/news/17.07.2008/4632/.

63. Кіберзлочинці озброїлися Skype для розповсюдження шкідливих програм - експерти . Корреспондент. URL: https://ua.korrespondent.net/business/web/1541304-kiberzlochinci-ozbroyilisya-skype-dlya-rozpovsyudzhennya-shkidlivih-program-eksperti.

64. Кіберполіція викрила українського хакера у взламі комп'ютерів світових банків та готелів . Офіційний сайт Національної поліції. URL: https://www.npu.gov.ua/news/ kiberzlochini/ kiberpolicziya-vikrila-ukrajinskogo-xakera-u-vzlami-komp-yuteriv-svitovix-bankiv-ta-goteliv/.

65. Кіберполіція (крок реформі) . Українська правда. URL: http://blogs.pravda.com.ua/authors/avakov/ 561a92c183c27/ view_print/.

66. Козак Н.С. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Збірник наукових праць Ірпінської фінансово-юридичної академії (економіка, право*). Вип. № 2. 2013. 159 с.

67. Коментар до кримінально-процесуального кодексу України . Законодавство України. URL: https://zakon.osmark.com.ua/кримінальний-кодекс-україни-комента-15/.

68. Коментар до статті 363-1 КК . Юрисконсульт. Народний правовий журнал. URL: http://legalexpert.in.ua/komkodeks/uk/81-uky/2075-363-1.html.

69. Конвенція «Про кіберзлочинність» від 23.11.2001 № 994_575 (ратифікація 07.09.2005). URL: http://zakon2.rada.gov.ua/laws/show/994_575/.

70. Конституція України від 28.06.1996 № 254к/96-ВР (у ред. 21.02.2019). URL: http://zakon2.rada.gov.ua/laws/show/254к/96-вр.

71. Копатін О., Скулишин Є. Словник термінів з кібербезпеки. Київ: ВБ «Аванпост-Прим», 2012. 214 с.

72. Коржанський М.Й. Кваліфікація злочинів: навч. посіб. Вид. № 2. Київ: Атіка, 2002. 640 с.

73. Користін О.Є., Бутузов В.М., Василевич В.В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб.Київ: Видавничий дім «Скіф», 2012. 728 с.

74. Корнякова Т.В., Соколенко О.Л., Юзіков Г.С. Віктимологічне моделювання у системі заходів забезпечення кримінологічної безпеки суспільства : моногр. Дніпропетровськ : ЛІРА, 2016. 220 с.

75. Кривогін М.С. Міжнародно-правові аспекти боротьби з кібернетичними злочинами. «*Держава і право : теорія і практика»*: матеріали II міжнар. науч. конф. (м. Чита, березень 2013 р.). Чита : «Молодий вчений», 2013. С. 77-79.

76. Кримінальне право України. Загальна частина: навч.-метод. посіб. для самост. вивч. дисц. Київ: КНЕУ, 2003. 354 с. URL: http://ubooks.com.ua/books/000157/inx20.php.

77. Кримінальне право України: Загальна частина: підручник. *URL:* https://law.wikireading.ru/8493.

78. Кримінальний кодекс України від 05.04.2001 № 2341-III (у ред. 26.02.2019). *URL*: http://zakon3.rada.gov.ua/laws/show/2341-14.

79. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (у ред. 11.01.2019). URL: http://zakon5.rada.gov.ua/laws/show/4651-17.

80. Крылов В.В. Информационные компьютерные преступления: учеб. и практ. пособие. Москва: ИНФРА-М: Норма, 1997. 276 с.

81. Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. Уголовное право. 1998. Вып. № 3. С. 81-89.

82. Кругликов Л.Л., Спиридонов О.Е. Юридические конструкции и символы в уголовном праве. Санкт-Петербург: Юрид. центр Пресс, 2005. 336 с.

83. Кудрявцев В.Н. Общая теория квалификации преступлений. Москва: Юрид. лит., 1972. 352 с.

84. Кузнецова Н.Ф. Проблемы квалификации преступлений: лекции по спецкурсу «Основы квалификации преступлений». Москва: Изд. дом «Городец», 2007. 336 с.

85. Куліш, А.М., Тютюнник В.В. Комп'ютерна злочинність: нормативно-правове врегулювання. *«Сучасні інформаційні системи і технології»*: матеріали Першої міжнародної науково-практ. конфер., м. Суми, 15-18 травня 2012 р. Суми: СумДУ, 2012. С. 229-231.

86. Куринов Б.А. Научные основы квалификации преступлений. Москва: Изд-во Моск. ун-та, 1984. 184 с.

87. Лише 58% українців користуються інтернетом. Дослідження . Еспресо. URL:https://espreso.tv/news/2018/01/31/lyshe_58_ukrayinciv_korystuyutsya_internetom_doslidzhennya.

88. Лісовий В.В. «Комп'ютерні» злочини: питання кваліфікації. Право України. 2002. Вип. № 2. С. 86-88.

89. Ляпунов Ю.И. Общественная опасность деяния как универсальная категория советского уголовного права. Москва, 1989. 119 с.

90. Ляпунов Ю.И. Ответственность за компьютерные преступления. *Законность*. 1997.Вып. №1. С. 8-13.

91. Мазолина О.В. Вопросы международно-правового регулирования Интернета. *Московский журнал международного права*. 2004. Вып. № 4. С. 152-164.

92. Митрофанов І.І. Загальна частина кримінального права України : навч. посіб. Одеса : Фенікс, 2015. 576 с.

93. Міжнародна конвенція про охорону інтересів виконавців, виробників фонограм і організацій мовлення 26.10.1961 № 995_763 (приєднання 20.09.2001). URL: http://zakon2.rada.gov.ua/laws/ show/995_763.

94. Мірошниченко С.С. Злочини проти правосуддя : теоретичні і прикладні проблеми запобігання та протидії : дис. … д-ра юрид. наук : 12.00.08. Київ, 2012. 492 с.

95. Міхайліна Т.В. Особливості кваліфікації злочинів із використанням засобів комп’ютерної техніки, що вчиняються групою осіб. *Публічне право*. Вип. № 3. 2011. С. 183-193.

96. Мішин А.В. Поняття комп'ютерної вірусу. Шляхи проникнення вірусів: лекційне заняття. URL: http://om.net.ua/5/5_13/5_ 131653_ponyatie-kompyuternogo-virusa-puti-proniknoveniya-virusov.html.

97. Музика А.А. Азаров Д.С. Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практ. ком. і шляхи вдосконалення. Київ: Вид-во Паливода, 2005. 120 с.

98. Навроцький В.О. Основи кримінально-правової кваліфікації: навч. пос. Київ: Юрінком Інтер, 2006. 704 с.

99. Навроцький В.О. Теоретичні проблеми кримінально-правової кваліфікації. Київ : Атіка, 1999. 464 с.

100. Навроцький В.О. Українське кримінальне право. Загальна частина: підр. Київ: Юрінком Інтер, 2013. 712 с. URL: http://pidruchniki.com/1019091256215/pravo/mistse_vchinennya_zlochinu.

101. Населення України . Мінфін. URL: https://index.minfin.com.ua/ua/reference/people/2017.

102. Науково-практичний коментар до кримінального кодексу . Радник. Український юридичний портал. *URL*: http://radnuk.info/komentar/kruminal/osobluva/302-rozd16/4662--361----------.html.

103. Наумов А.В., Новиченко А.С. Законы логики при квалификации преступлений. Москва: Юрид. лит., 1978. 104 с.

104. Новая эпидемия шифровальщика Petya. NotPetya. ExPetr . Kaspersky. *URL*: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855.

105. Ортинський В.Л., Грищук В. К., Мацько М. А. Основи держави і права України: підр. Київ: Знання, 2008. 583 с. URL: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,170/task,view.annotation/.

106. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях : международный опыт. Москва, 2004. С. 135–138.

107. Панфилова Е.И., Попов А.С. Компьютерные преступления: серия «*Современные стандарты в уголовном праве и уголовном процессе*». под ред. Б.В. Волженкина. Санкт-Петербург.: СПб. юрид. ин-т ген. Прокуратуры, 1998. 203 с.

108. Пашнєв Д.В. Авдєєв О.О. Кваліфікація кіберзлочинів у випадках ідеальної сукупності злочинів. *Форум права*. 2016. Вип. № 4. С. 258–263.

109. Пашнєв Д.В. Властивості комп'ютерної інформації як предмету злочину. *Вісник Кримінологічної асоціації України : збірник наукових праць*. Вип. № 1. Харків : ХНУВС, 2012.С. 115-125.

110. Першиков В.И., Савинков В.М. Толковый словарь по информатике. Москва: Финансы и статистика, 1991. 543 с.

111. Плугатир М.В. Особа, що має право доступу до комп'ютерної інформації як суб'єкт злочину, передбаченого ст. 362 КК України. *Юридична Україна*. *Кримінально-правові науки*. Вип. №1, 2010. С. 113-116.

112. Погорецький М.А., Шеломенцев В.П. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. Вип. № 8. С. 89–96.

113. Полевой Н.С. и др. Правовая информатика и кибернетика: учебник. Москва: Юридическая литература, 1993. 528 с.

114. Поливода О.Ю. Боротьба з комп'ютерною злочинністю в Україні: проблемні питання. «*Взаємодія правоохоронних органів з провайдерами та операторами зв'язку в боротьбі з комп'ютерними злочинами»* : матеріали регіонального наук.-практ. сем., м. Донецьк, 12 грудня 2008 р. Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк : ДЮІ ЛДУВС, 2009. С. 88–91.

115. Потебенько М.О., Гончаренко В.Г. Науково-практичний коментар до Кримінального Кодексу України. Київ: ФОРУМ, 2001., у 2-х ч. Особлива частина. 721 с.

116. Правила ведення нотаріального діловодства: Наказ Міністерства юстиції України від 22.12.2010 № 3253/5 (у ред. 03.04.2015). URL: http://zakon3.rada.gov.ua/laws/show/z1318-10.

117. Про авторське право і суміжні права: Закон України від 23.12.1993 № 3792-XII (у ред. 04.11.2018). URL: http://zakon5.rada.gov.ua/laws/show/3792-12.

118. Про державне регулювання діяльності у сфері трансферу технологій: Закон України від 14.09.2006 № 143-V (у ред. 09.12.2015).URL: http://zakon3.rada.gov.ua/laws/show/143-16.

119. Про Доктрину інформаційної безпеки України: Указ Президента України від 8.07.2009 № 514/2009. *Офіційний вісник України*. 2009. № 52. С. 7.

120. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI (у ред. 01.05.2015). URL: http://zakon5.rada.gov.ua/laws/show/2939-17.

121. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР (у ред. 19.04.2014). URL: https://zakon2.rada.gov.ua/laws/show/80/94-вр/.

122. Про інформацію: Закон України від 02.10.1992 № 2657-XII (у ред. 01.01.2017). URL: http://zakon2.rada.gov.ua/laws/show/2657-12.

123. Про міжнародне приватне право: Закон України від 23.06.2005 № 2709-IV (у ред. 22.08.2018). URL: https://zakon.rada.gov.ua/ laws/show/2709-15.

124. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР (у ред. 01.08.2016). URL: http:// https://zakon2.rada.gov.ua/laws/show/74/98-вр.

125. Про нотаріат: Закон України від 02.09.1993 № 3425-XII (у ред. 04.02.2019). URL: http://zakon2.rada.gov.ua/laws/show/ 3425-12/page.

126. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 № 3341-XII (у ред. 05.01.2017). URL: http://zakon2.rada. gov.ua/laws/show/3341-12.

127. Про основи національної безпеки України: Закон України від 19.06. 2003 № 964-IV (втрата чинності 08.07.2018). URL: http://zakon5.rada.gov.ua/laws/show/964-15.

128. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163- VIII (у ред. 08.07.2018). URL: https://zakon.rada.gov.ua/laws/show/2163-19.

129. Про платіжні системи та переказ коштів в Україні: Закон України від 05.04.2001 № 2346-III (у ред. 07.02.2019). URL: http://zakon3.rada.gov.ua/laws/show/2346-14.

130. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98 (у ред. 12.09.2009). URL: http://zakon0.rada.gov.ua/laws/show/505/98.

131. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 № 1229/99 (у ред. 04.05.2008).URL: http://zakon5.rada.gov.ua/laws/show/1229/99.

132. Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України: Закон України від 22.02.2000 № 1479-III (у ред. 28.06.2015). URL: http://zakon5.rada.gov.ua/laws/show/1479-14.

133. Про порядок направлення підрозділів Збройних Сил України до інших держав: Закон України від 02.03.2000 № 1518-III (у ред. 04.11.2018). URL: https://zakon.rada.gov.ua/laws/show/1518-14.

134. Про практику застосування судами законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки: Постанова Пленуму Верховного Суду України від 04.06.2010 №7 (прийняття 04.06.2010). URL: https://zakon.rada.gov.ua/laws/show/v0007700-10.

135. Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями: Постанова Пленуму ВСУ України від 23.12.2005 № 13 (прийняття 23.12.2005). URL: http://zakon2.rada.gov.ua/laws/show/v0013700-05.

136. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV (у ред. 14.10.2010. URL: //zakon.rada.gov.ua/laws/show/2824-15.

137. Про ратифікацію Третього додаткового протоколу та Четвертого додаткового протоколу до Європейської конвенції про видачу правопорушників: Закон України від 07.06.2017 № 2090-VIII (прийняття 07.06.2017). URL: http://zakon5.rada.gov.ua/laws/show/2090-19.

138. Про судову практику у справах про злочини проти власності: Постанова Пленуму Верховного Суду України від 06.11.2009 № 10 (прийняття 06.11.2009). URL: https://zakon.rada.gov.ua/laws/show/v0010700-09.

139. Про телекомунікації: Закон України у редакції від 18.11.2003 № 1280-IV (у ред. 04.11.2018). URL: http://zakon2.rada.gov.ua/laws/show/1280-15.

140. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування: Аналітична записка. Офіційне інтернет-преставництво Національного інституту стратегічних досліджень. URL: http:// www.niss.gov.ua/articles/454.

141. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю : автореф. дис. ... канд. юрид. наук. Харків, Національна юридична академія України ім. Ярослава Мудрого. 2002. 21 с.

142. Рарог А.И. Уголовное право. Особенная часть . Москва: Триада. ЛТД. 1996. 480 с.

143. Ричка Д.О. Історичні аспекти кіберзлочинності. Матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених *«Сучасний стан і перспективи розвитку держави і права»*. Дніпропетровськ, 2015. С. 293-295.

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

145. 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.

146. Ричка Д.О. Модель комп'ютерних злочинців. *«Науковий вісник Ужгородського національного університету. Серія : «Право».* Ужгород, 2018. С. 122-125.

147. 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»*. Дніпро, 2017. С. 267-268.

148. 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.

149. Ричка Д.О. Тенденції розвитку криптовалюти на території України. Матеріали ІІ Всеукраїнської науково-практичної конференції *«Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності»*. Хмельницький : Вид-во НАДПСУ, 2018. С. 520-522.

150. Ричка Д.О. Транснаціональна злочинність новітніх комп'ютерних технологій. Науково-виробничий журнал *«Держава та регіони. Серія : Право»*. Класичний приватний університет. Запоріжжя, 2018. С. 133-138.

151. Розенфельд Н.А. Суб'єкт злочину «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж» . Центр исследования проблем компьютерной преступности. URL: http://www.crime-research.org/library/Rozenf.htm.

152. Сень Р.Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. «*Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності»* : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014. С. 192–194.

153. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть Москва, 1996. 416 с.

154. Словник української мови. Академічний тлумачний словник (1970-1980). Том 4, 1973. 840 с. URL: http://sum.in.ua/p/4/36/1.

155. Снігерьов О.П., Сергач О.І. Деякі правові проблеми злочинності в сфері комп'ютерної інформації. «*Інформаційні технології та захист інформації*». Збірник наукових праць. Міністерство внутрішніх справ України. Запорізький юридичний інститут. Вип. № 1. 1998. С. 59-64.

156. Созанський Т.І. Кваліфікація злочинів, передбачених різними статтями КК України. *Європейські перспективи*. 2012. Вип. № 2 (Ч. 1). С. 131–136.

157. Сорока Л.В. Види правопорушень у сфері комп'ютерних та інформаційних технологій. *Наукові записки КДПУ*. Серія: Історичні науки. Кіровоград : КДПУ ім. В. Винниченка, 2005. Вип. 9. С. 262-270.

158. Спасович В.Д. Учебник уголовного права. Т. 1. Санкт-Петербург: Тип. И. Огризко, 1863. 442 с.

159. Сташис В.В. Передача на поруки и некоторые вопросы советского уголовного права. *Об усилении роли общественности в укреплении социалистического правопорядка*. Харьков: Харьк. юрид. ин-т, 1961. С. 27-30.

160. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016 (прийняття 15.03.2016). URL: http://zakon2.rada.gov.ua/laws/show/96/2016.

161. Стратегія національної безпеки України: Указ Президента України від 26.05.2015 № 287/2015 (прийняття 26.05.2015). *URL*: http://zakon5.rada.gov.ua/laws/show/287/2015.

162. Суд Полтави відпустив хакера кібербанди Avalanche, розшукуваного 4 роки у 30 країнах світу - ЗМІ . Новое время. URL: https://nv.ua/ukr/ukraine/events/sud-poltavi-vidpustiv-hakera-kiberseti-avalanche rozshukuvanogo-4-roki-u-30-krajinah-svitu-zmi-303223.html.

163. Судова практика з питань кваліфікації повторності та сукупності злочинів (статті 32, 33, 35 Кримінального кодексу України) . Офіційний веб-сайт Верховний Суд України. URL: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/9998DC9C06A6F4342257B7C004712AE.

164. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. Вісник Верховного Суду України. 2010. Вип. № 2. С. 29-34. URL: http://nbuv.gov.ua/UJRN/vvsu_2010_2_7.

165. Сухонос В.В. Кримінальне право України. Загальна частина: підр. Суми : Університетська книга, 2016. 375 с.

166. США спіймали організовану українцем кібербанду, яка накрала $530 млн // Depo.ua. URL: https://www.depo.ua/ukr/life/ssha-spiymali-organizovanu-ukrayincem-kiberbandu-yaka-nakrala-530-mln-20180208723213.

167. Таций В.Я. Объект и предмет преступления в советском уголовном праве. Харьков: Вища школа, 1998. 196 с.

168. Телійчук В.Г. Протидія злочинам, що вчиняються організованими злочинними угрупованнями з використанням комп'ютерних технологій. *«Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку»* : матеріали всеукр. наук.-практ. конф., м. Донецьк, 4 грудня 2009 р. Донецький юрид. ін-т ЛДУВС ім. Е.О. Дідоренка. Донецьк: ДЮІ ЛДУВС, 2009. С. 198–202.

169. Телійчук В.Г. Способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії. *Держава та регіони*. Вип. № 2 (44), 2014р. С. 31-37.

170. Топчій В.В. Кваліфікація злочинів, вчинених групами осіб в місцях масового скупчення людей. *Науковий вісник Ужгородського національного університету*. Серія ПРАВО. Випуск 36. Том 2, 2016. С.100-103.

171. Узагальнення судової практики з питань кваліфікації повторності та сукупності злочинів (статті 32, 33, 35 Кримінального кодексу України) від 01.12.2008 № n0007700-08 . Вісник Верховного Суду України. URL: http://zakon3.rada.gov.ua/laws/show/ n0007700-08/page.

172. Фігель М.В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. 336 с.

173. Фролов Е.А. Спорные вопросы общего учения об объекте преступления. Вып. 10. Свердловск: Свердловский юрид. ин-т., 1969. С. 184-226.

174. Хакерская атака на Украину: подробности . РБК - Україна. URL: https://www.rbc.ua/rus/news/hakerskaya-ataka-ukrainu-podrobnosti1498566985.html.

175. Хряпінський П.В. Кримінальна правотворчість (теорія кваліфікації злочинів): навч. посіб. Дніпропетровськ. 2011, 302 с.

176. Целевые атаки . Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/targeted-attacks.

177. Цивільний кодекс України у редакції від 16.01.2003 № 435-IV (у ред. 31.03.2019). URL: http://zakon2.rada.gov.ua/laws/show/435-15/page.

178. Чисельність населення (за оцінкою) на 1 січня 2018 року та середня чисельність у 2017 році . Державна служба статистики України. URL: http://www.ukrstat.gov.ua/operativ/operativ2017/ds/kn/kn_u/kn1217_u.html

179. Шапченко С.Д. Кваліфікація злочинів як соціально-правове явище: основні юридичні аспекти. *Альманах кримінального права: збірник статей*. Вип. №1. Київ: Правова єдність, 2009. С. 415-422.

180. Шапченко С.Д. Юридична кваліфікація як соціально-правове явище та деякі її загальнотеоретичні аспекти. Тези міжнародної наукової конференції: *«Проблеми юридичної кваліфікації (теорія і практика)»*. Вісник Академії адвокатури України. Число 1 (17) 2010. С. 135-138.

181. Шевердін Д.О., Гаряєва Г.М. Порівняльно-правовий аналіз законодавства України та зарубіжних країн, що регламентує відповідальність за комп'ютерні злочини. «*Переяславская рада: её историческое значение и перспективы развития восточнославянской цивилизации»*: сб. науч. тр.: по матер. VII Междунар. науч.-практич. конференции, 19-20 декабря 2012 г., Ч. 2. Харьков: НТУ «ХПИ», 2013. С. 165-168.

182. Шеломенцев В.П. Боротьба з організованими злочинними угрупуваннями у сфері використання банківських платіжних карток. Боротьба з організованою злочинністю і корупцією (теорія і практика). Киев: МНДЦ, 2004. Вып. № 10. 185-194 с.

183. Школьний В.Б. Криміналістична характеристика основних видів кіберзлочинів. «Спеціальна техніка у правоохоронній діяльності»: Матеріали V міжнар. наук. -практ. конф., 25 листоп. 2011 р. м. Київ. Київ: Нац. акад. внутр. справ України, 2012. С. 199-201.

184. Юридичний словник-довідник. *URL:* http://subject.com.ua/pravo/dict/449.html.

185. Юртаєва К.В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права*. 2009. Вип. № 2. С. 434–441.

186. Яценко С.С. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. Київ: А.С.К., 2002. 936 с.

187. 10 относительно честных способов взломать почту . Хабрахабр. *URL:* https://habrahabr.ru/company/cybersafe/ blog/269829.

188. Brenner S.W. Toward a Criminal Law for Cyberspace A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J.1 (2004).

189. HUGE 'PETYA' CYBER ATTACK SPREADING ACROSS THE WORLD IN POTENTIAL REPEAT OF 'WANNACRY' HACK . Independent. URL*:* https://www.independent.co.uk/life-style/gadgets-and-tech/news/hack-cyber-attack-ukraine-russia-wannacry-petya-security-internet-broken-computer-not-working-a7810626.html.

190. Petya' ransomware attack: what is it and how can it be stopped? Cybercrime. *URL:* https://www.theguardian.com/technology/ 2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how.

191. Petya ransomware outbreak: Here's what you need to know. Symantec. *URL:* https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper.

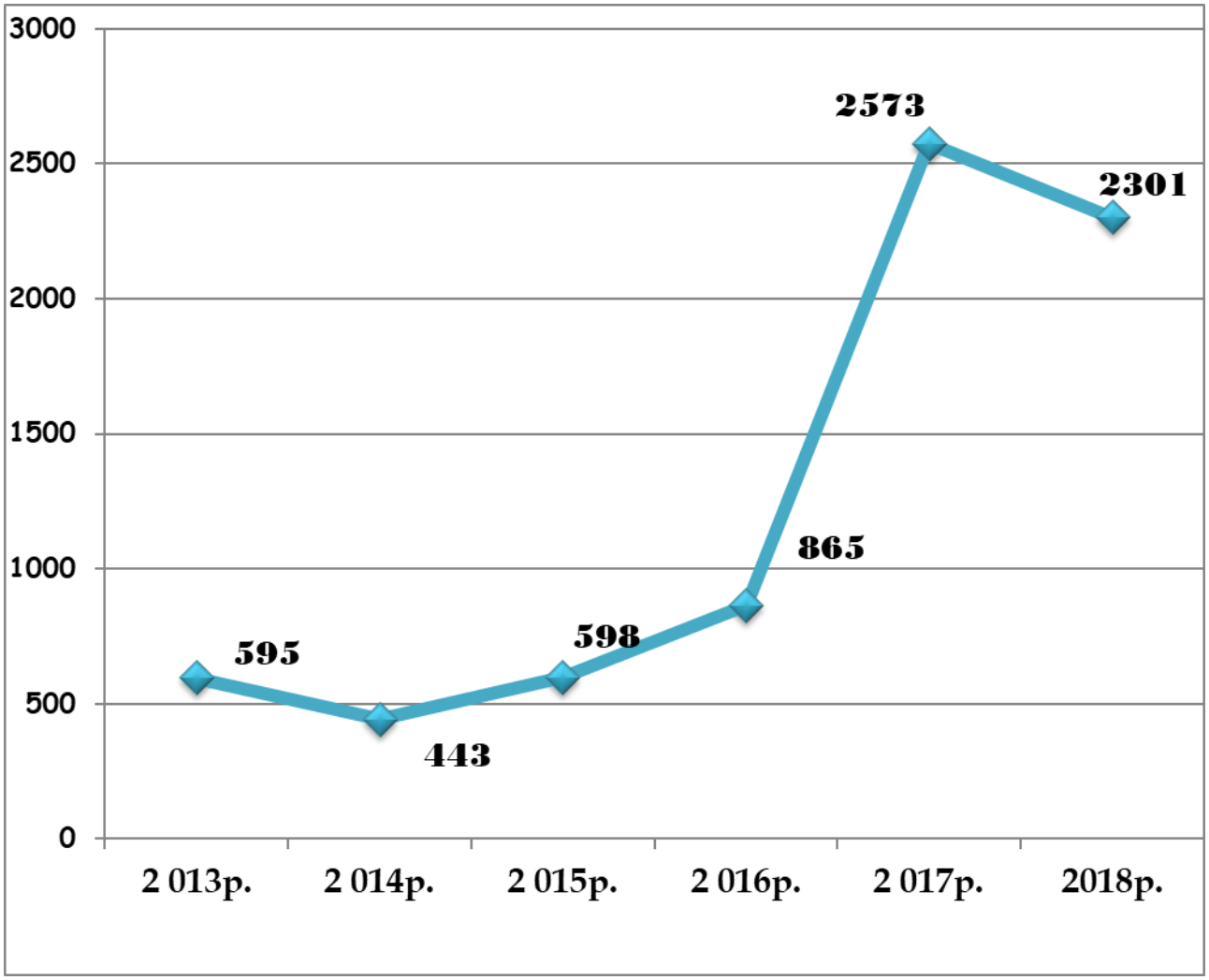
192. Rychka D.O. Types of crime in information and telecommunication systems. Cybersquatting (cybercrime). *Международный научно-практический журнал «Право и закон»*. 2018. № 3. С. 101–105.

193. Sofacy Group . Вікіпедія. URL*:* https://uk.wikipedia.org/wiki/Sofacy_Group.

194. Stein A.R. Simposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulator Precision. 98 Nw. U.L.Rev. 411 (2004).

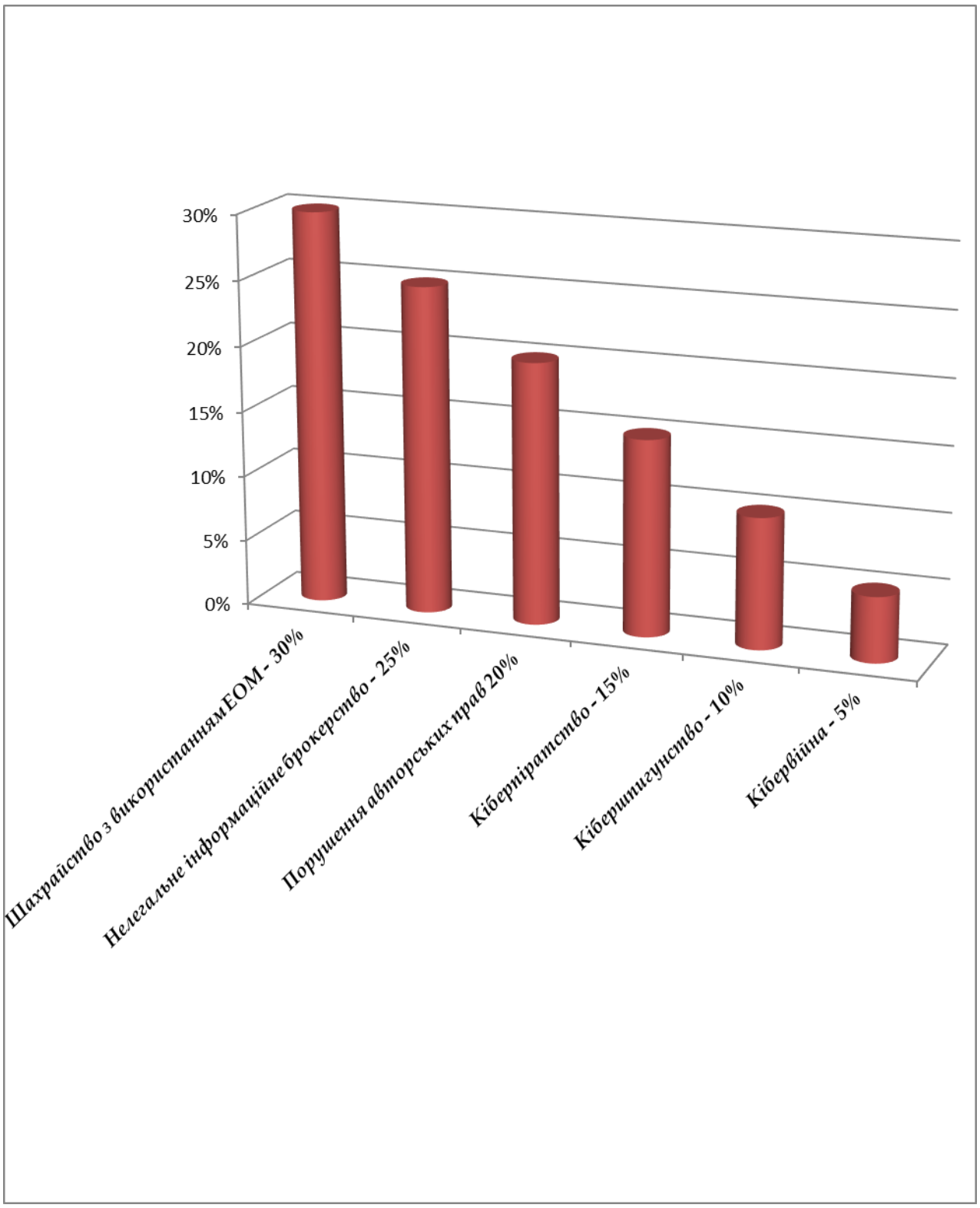
Додаток **А**

Обліковано кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку з 2013 по 2018 роки



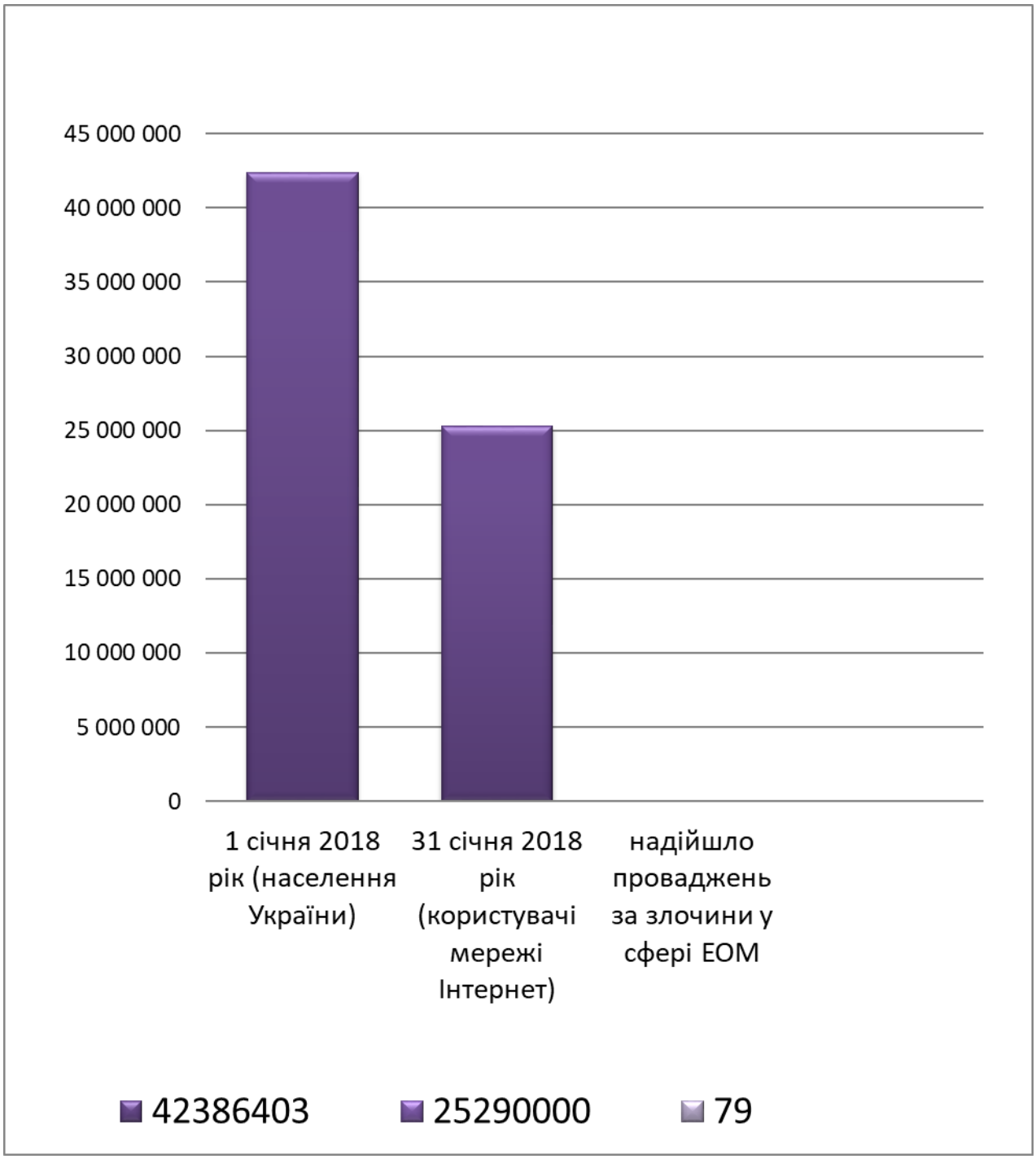
Додаток **Б**

Найбільш розповсюджені види міжнародних кібернетичних злочинів



Додаток **В**

Суб'єкти комп'ютерних злочинів



Додаток Д

Громадянство суб'єктів комп'ютерних злочинів

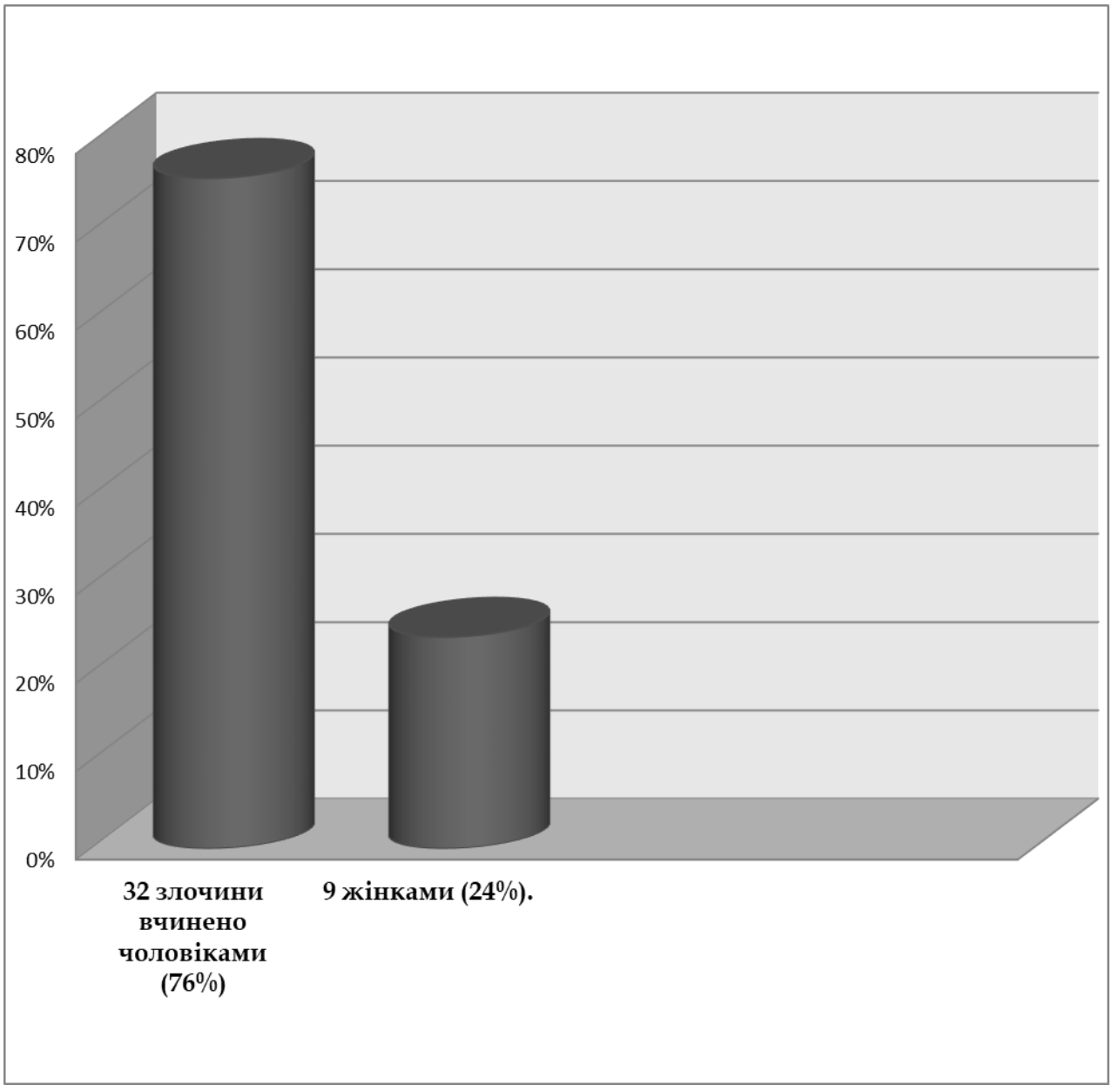
2017р.

2018р.

Додаток **Е**

Склад засуджених

Відповідно до звіту Державної судової адміністрації України про склад засуджених у 2017 році за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст. 361-363-1 КК) **було засуджено 42 особи**.

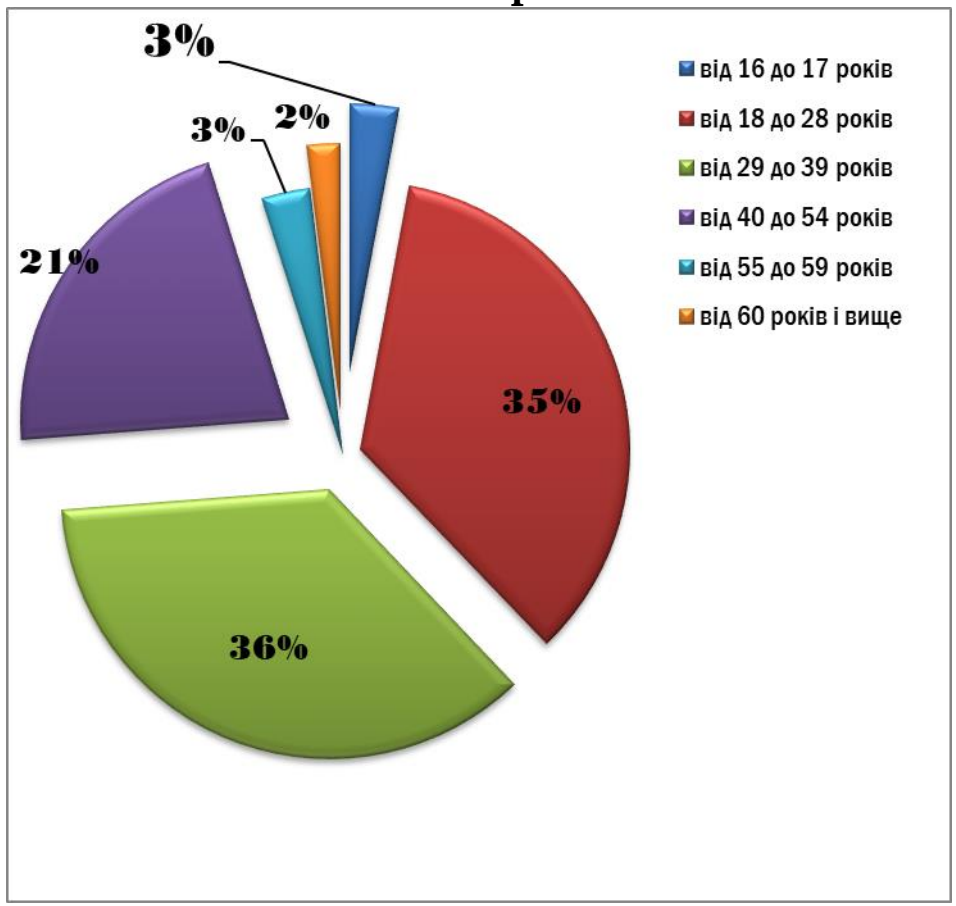


*інформація про склад засуджених у 2018 році за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст. 361-363-1 КК) відповідно до звіту Державної судової адміністрації України наявна за 9 місяців. У зв'язку з відсутністю інформації за 12 місяців 2018 року порівняння стану кіберзлочинності за 2017р. та 2018р. не проводиться.

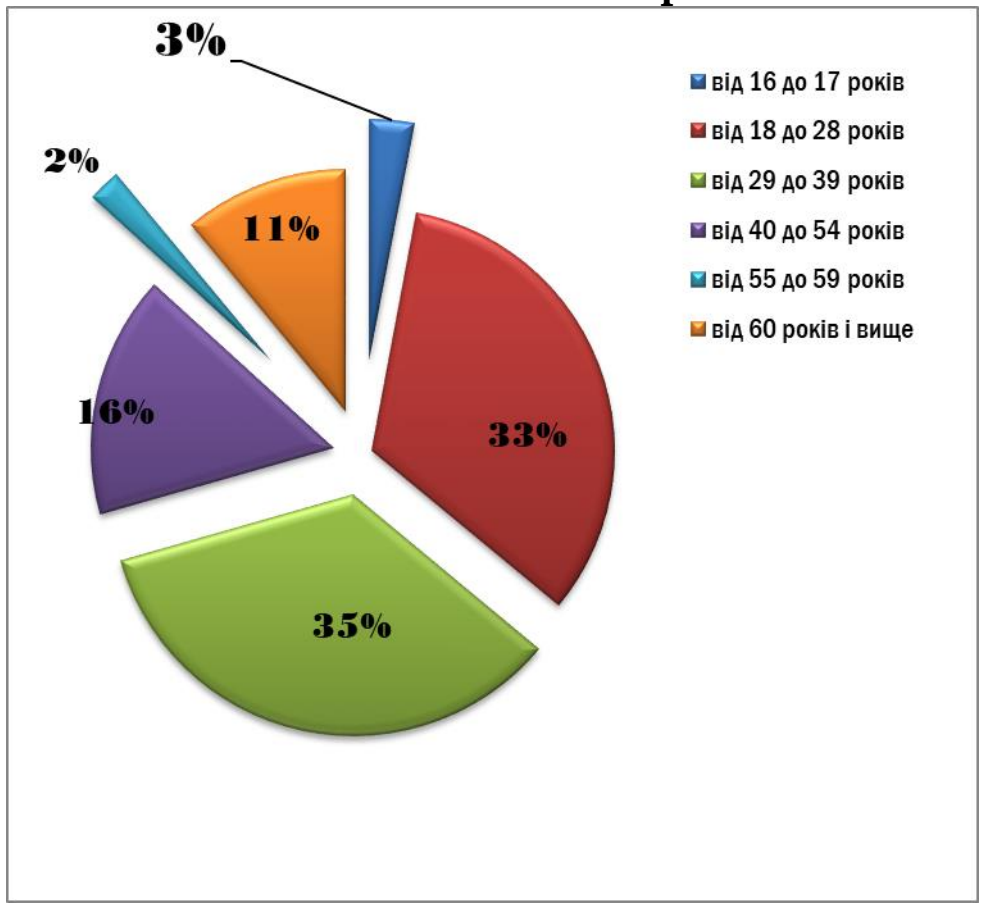
Додаток **Ж**

Віковий показник злочинців у сфері ЕОМ станом на 2017 рік

2017р.

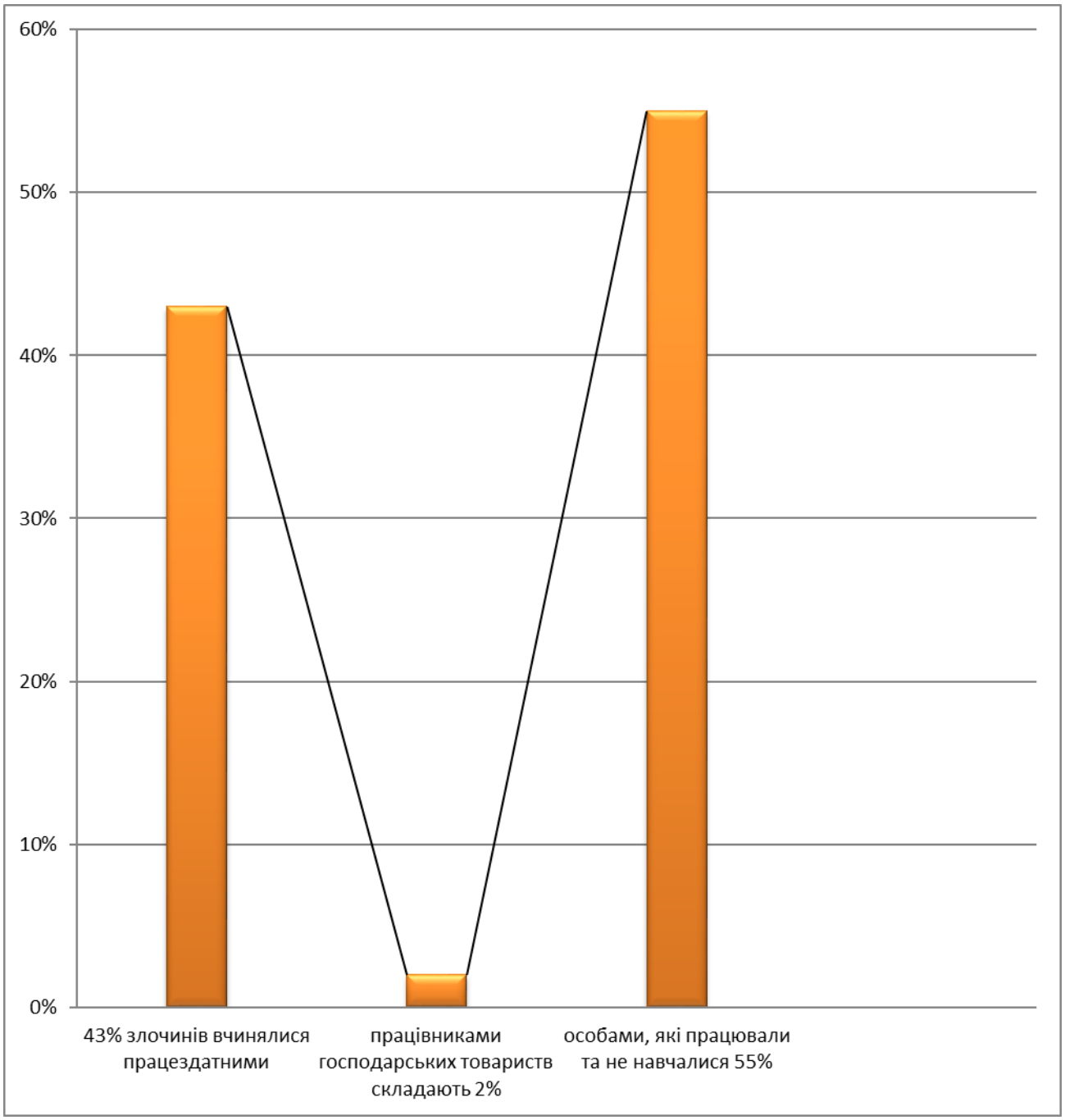


2018р.



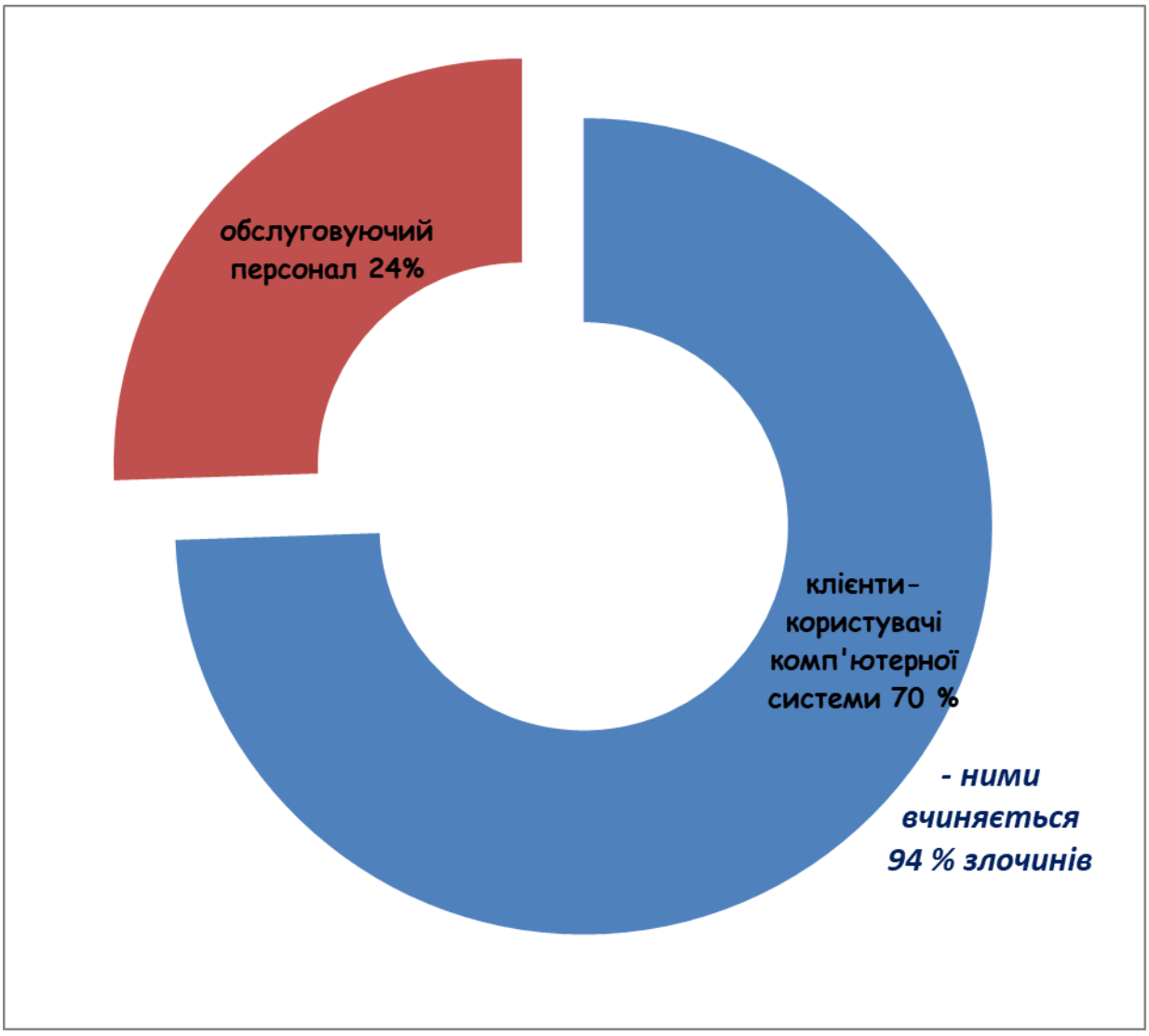
Додаток **3**

Класифікація суб'єктів вчинення комп'ютерних злочинів за сферами діяльності



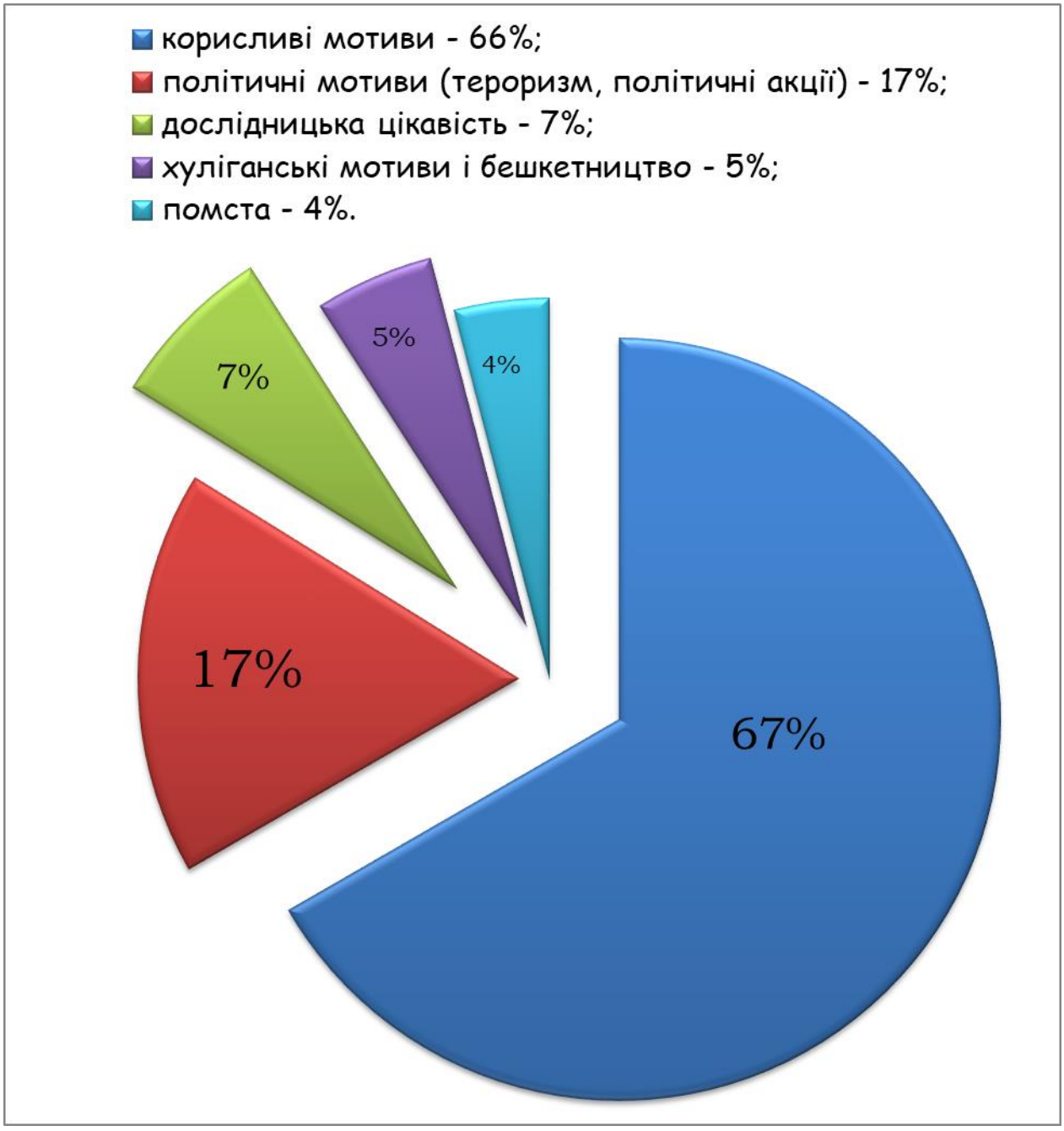
Додаток **К**

Класифікація суб'єктів вчинення комп'ютерних злочинів по відношенню до ЕОМ



Додаток **Л**

Мотиви вчинення комп'ютерних злочинів



Додаток **М**

Акти впровадження

ЗАТВЕРДЖУЮ

Проректор з наукової роботи Дніпровського національного університету імені Олеся Гончара, професор С.І. Оковитий

«09» 11 2018р.

АКТ

Про впровадження у навчальний процес Дніпровського національного університету імені Олеся Гончара основних результатів дисертації аспіранта Рички Дениса Олеговича за темою «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право.

Уклала комісія у складі:

Голови: професор кафедри адміністративного і кримінального права юридичного факультету Дніпровського національного університету імені Олеся Гончара, д.ю.н., доцент Н.С. Юзікова.

Членів комісії: голова методичної ради юридичного факультету Дніпровського національного університету імені Олеся Гончара, д.ю.н., доцент І.В.Патерило;

доцент кафедри адміністративного і кримінального права юридичного факультету Дніпровського національного університету імені Олеся Гончара, к.ю.н., доцент О.В. Лахова.

Комісія склала цей акт з приводу розгляду результатів дисертаційного дослідження аспіранта Рички Дениса Олеговича за темою «Особливості кримінально-правової кваліфікації злочинів у сфері використання

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право і використання у навчальному процесі з дисциплін «Кримінальне право», «Кримінологія» та «Кримінально-виконавче право» кафедри адміністративного і кримінального права юридичного факультету Дніпровського національного університету імені Олеся Гончара.

Комісія дійшла висновку, що подані Ричкою Д.О. на кафедру матеріали становлять цінність для навчального процесу у зв'язку з їх актуальністю. Зазначені матеріали зроблено на достатньому теоретичному та методичному рівні та ґрунтуються на результатах проведеного автором глибокого дослідження чинного законодавства, матеріалів практики та наукових джерел і можуть бути впроваджені у навчальний процес для викладання курсів «Кримінальне право», «Кримінологія» та «Кримінально-виконавче право», а також використані у науково-дослідній роботі студентів.

Зокрема наукові публікації Рички Д.О.:

1. Rychka D.O. Types of crime in information and telecommunication systems. Cybersquatting (cybercrime) / Rychka D.O. // Zbiór artykułów naukowych z Konferencji Miedzynarodowej Naukowo-Praktycznej (on-line) zorganizowanej dla pracowników naukowych uczelni, jednostek naukowo-badawczych oraz badawczych z państw obszaru byłego Związku Radzieckiego oraz byłej Jugosławii. - Warszawa, 2017. str. 53-57.
2. Ричка Д.О. Комп'ютерні віруси - шкідливі програмні засоби, рушійна сила модифікації / Ричка Д.О. // Науковий вісник Херсонського державного університету. Серія: «Юридичні науки». – Херсон, 2018. – Вип. 1. Том 2. – С. 89-93.
3. Ричка Д.О. Транснаціональна злочинність новітніх комп'ютерних технологій / Ричка Д.О. // Науково-виробничий журнал «Держава та регіони. Серія: Право», Класичний приватний університет. – Запоріжжя, 2018. – С. 133-138.
4. Ричка Д.О. Модель комп'ютерних злочинців / Ричка Д.О. // «Науковий вісник Ужгородського національного університету. Серія «Право». – Ужгород, 2018. – С. 122-125.
5. Ричка Д.О. Історичні аспекти кіберзлочинності / Ричка Д.О. // Матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених «Сучасний стан і перспективи розвитку держави і права». – Дніпропетровськ, 2015. – С. 293-295.
6. Ричка Д.О. Передумови виникнення злочинів у сфері використання електронно-обчислювальних машин / Ричка Д.О. // Матеріали IX Міжнародної наукової конференції студентів, аспірантів та молодих вчених

«Сучасний стан і перспективи розвитку держави і права». – Дніпро, 2017. – С. 267-268.
7. Ричка Д.О. Тенденції розвитку криптовалюти на території України / Ричка Д.О. // Матеріали II Всеукраїнської науково-практичної конференції «Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності». – Хмельницький : Вид-во НАДПСУ, 2018. – С. 520-522.
8. Ричка Д.О. Комп'ютерна фобія / Ричка Д.О. // Матеріали Всеукраїнської наукової інтернет - конференції «Вітчизняна наука на зламі епох: проблеми та перспективи розвитку». Переяслав-Хмельницький, 2018. – Вип.41. – С. 87-88.

внесені до списку літератури робочих навчальних програм дисциплін «Кримінальне право», «Кримінологія» та «Кримінально-виконавче право».

Зазначені наукові публікації Рички Д.О. рекомендуються для користування під час підготовки до семінарських занять з навчальних «Кримінальне право», «Кримінологія» та «Кримінально-виконавче право».

Голова комісії

Професор кафедри адміністративного і кримінального права юридичного факультету Дніпровського національного університету імені Олеся Гончара, д.ю.н., доцент Н.С. Юзікова

Члени комісії:

голова методичної ради юридичного факультету Дніпровського національного університету імені Олеся Гончара, д.ю.н., доцент І.В. Патерило

доцент кафедри адміністративного і кримінального права юридичного факультету Дніпровського національного університету імені Олеся Гончара, к.ю.н., доцент О.В. Лахова

ЗАТВЕРДЖУЮ
Заступник начальника – начальника
СУ ГУНП в
Дніпропетровській області
полковник поліції
Кураченко М.В.
„15" 10 2018 р.

АКТ

„15" 10 2018 р. м. Дніпро №_____

Про впровадження у практичну діяльність ГУНП в Дніпропетровської області основних результатів дисертаційного дослідження Рички Д.О. «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 «кримінальне право та кримінологія; кримінально-виконавче право»

Уклала комісія у складі:

Голови:

Заступник начальника-
начальник СВ СУ ГУНП
п/п-к поліції П.П. Мітенка

Члени комісії:

начальник відділу СУ ГУНП
майор поліції
Заворуєвська Н.М.

Заступник начальника відділу
СУ ГУНП
п/п-к поліції О.О. Єфіменко

Про те, що до Головного управління національної поліції Дніпропетровської області надійшли матеріали дисертаційного дослідження Рички Дениса Олеговича «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп`ютерів), систем та комп`ютерних мереж і мереж електрозв`язку», виконаного на кафедрі адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара. Актуальність обраної теми дослідження обґрунтована, оскільки необхідно вирішувати наукові і практичні проблеми, пов'язані з встановленням кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв`язку.

Впровадження науково-практичних рекомендацій Рички Д.О. сприятиме підвищенню якості діяльності працівників ГУНП в Дніпропетровської області щодо визначення вірної кваліфікації, враховуючи особливості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв`язку під час розслідування злочинів вказаної категорії.

Відповідно, теоретичні і практичні результати зазначеної науково-дослідної роботи свідчать про актуальність та практичну значимість виконаного дослідження.

Результати та пропозиції, отримані у ході дисертаційного дослідження, доведені до відома особового складу.

Акт обговорено і схвалено на спільному засіданні протокол № __ від „15" 10 2018 р.

Голова комісії

Члени комісії:

ЗАТВЕРДЖУЮ
Перший заступник прокурора
Дніпропетровської області
старший радник юстиції
Р.М. Сосков

„18" вересня 2018 р.

АКТ

„18" вересня 2018 р. м. Дніпро № 6/4

Про впровадження у практичну діяльність прокуратури Дніпропетровської області основних результатів дисертаційного дослідження Рички Д.О. «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 «кримінальне право та кримінологія; кримінально-виконавче право»

Уклала комісія у складі:

Голови: начальник управління представництва інтересів держави в суді прокуратури Дніпропетровської області [illegible]

Членів комісії: начальник відділу представництва при виконанні судових рішень прокуратури Дніпропетровської області [illegible] В.В.
прокурор відділу організації представництва інтересів держави прокуратури Дніпропетровської області [illegible]

Про те, що до прокуратури Дніпропетровської області надійшли матеріали дисертаційного дослідження Рички Дениса Олеговича «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», виконаного на кафедрі адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара. Актуальність обраної теми дослідження обґрунтована, оскільки необхідно вирішувати наукові і практичні проблеми, пов'язані з встановленням кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Впровадження науково-практичних рекомендацій Рички Д.О. сприятиме підвищенню якості діяльності працівників органів прокуратури щодо визначення вірної кваліфікації, враховуючи особливості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при здійсненні представництва інтересів громадян в суді та під час нагляду за додержанням законів органами, що проводять оперативно-розшукову діяльність, дізнання, досудове слідство

Відповідно, теоретичні і практичні результати зазначеної науково-дослідної роботи свідчать про актуальність та практичну значимість виконаного дослідження.

Результати та пропозиції, отримані у ході дисертаційного дослідження, доведені до відома особового складу.

Акт обговорено і схвалено на спільному засіданні протокол №6/4 від „18" вересня 2018 р.

Голова комісії

Члени комісії:

Додаток **Н**

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. С. 133-138.

3. Ричка Д.О. Модель комп'ютерних злочинців. *«Науковий вісник Ужгородського національного університету.* Серія : «Право». Ужгород, 2018. 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. 101–105.

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»*. 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»*. 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». 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»*. Переяслав-Хмельницький, 2018. Вип.41. С. 87-88.