ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ

НАУКОВИЙ ЖУРНАЛ

ЄВРОПЕЙСЬКИЙ ПРАВНИЧИЙ ЧАСОПИС

Випуск 4

Київ
2024

ISSN 3041-1149 (Print)
УДК 340

Засновник та видавець: Приватний вищий навчальний заклад «Європейський університет».
Заснований 2023 року.
Витяг з реєстру суб'єктів у сфері медіа-реєстрантів: ідентифікатор медіа R30-01886,
рішення Національної ради України з питань телебачення і радіомовлення
№ 1387 від 16 листопада 2023 року.
Журнал включено до Переліку наукових фахових видань категорії «Б»
наказом Міністерства освіти і науки України від 02.10.2024 № 1415
зі спеціальностей 081 «Право», 293 «Міжнародне право».

Періодичність виходу примірників – у міру накопичення.
Мови видання: українська, англійська.

Рекомендовано до друку рішенням Вченої ради
Приватного вищого навчального закладу «Європейський університет»
(протокол № 7 від 20 листопада 2024 року)

Європейський правничий часопис : науковий журнал / редкол. : П. В. Цимбал (голов. ред.) та ін. – Київ : Приватний вищий навчальний заклад «Європейський університет», 2024. – Випуск 4. – 166 с.

У виданні вміщені наукові статті, присвячені актуальним проблемам юридичної науки й практики. Науковий журнал започатковано з метою опублікування результатів наукових досліджень проблем правової науки, вдосконалення законодавства та правозастосування. Видання розраховане на науковців, викладачів, аспірантів, докторантів, практичних працівників судової та правоохоронної сфери й усіх, хто цікавиться проблемами теорії права та правозастосування.

Науковий журнал індексується в Google Scholar.

Національною бібліотекою України імені В. І. Вернадського.

Інституційний Репозитарій Європейського університету.

DOI (digital object identifier) – цифровий індикатор об'єкта привласнюється науковим статтям видання.

Редакція журналу веде систематичну роботу із включення наукового видання до міжнародних електронних бібліотек, каталогів і наукометричних баз із метою входження у світовий науковий інформаційний простір, підвищення рейтингу журналу й індексів цитування його авторів.

За достовірність фактичних даних, цитат, власних імен, географічних назв тощо відповідають автори публікацій.
Статті українською та англійською мовами друкуються в авторській редакції та рекомендовані рецензентами.
Думки авторів можуть не збігатися з позицією редколегії.

Адреса, за якою здійснюється редакційний контроль:
бульвар Академіка Вернадського, 16-в, м. Київ, 03115, Україна
email: legal.journal@e-u.edu.ua

EUROPEAN UNIVERSITY

Scientific Journal

EUROPEAN LEGAL JOURNAL

Issue 4

Kyiv
2024

ISSN 3041-1149 (Print)
УДК 340

Founder and Publisher: Private Higher Educational Establishment «European University»
Was founded in 2023.
Extract from the register of media entities: Media Identifier R30-01886,
decision of the National Council of Ukraine on Television and Radio Broadcasting
№ 1387 dated November 16, 2023.
The journal is included in the List of Scientific Professional Publications of category "B"
by the order of the Ministry of Education and Science of Ukraine dated 02.10.2024 No. 1415
for specialties 081 "Law"; 293 "International Law".

Publication frequency: As materials accumulate.
Languages of publication: Ukrainian, English.

Recommended for printing by the decision of the Academic Council
of the Private Higher Educational Establishment «European University»
(protocol No. 7 dated November 20, 2024).

European Legal Journal : The Scientific Journal / Editorial Board : P. V. Tsimbal (Editor-in-chief) and others. – Kyiv : Private Higher Educational Establishment «European University», 2024. – Issue 4. – 166 p.

The publication contains scientific articles dedicated to current issues in legal science and practice. The scientific journal was initiated with the aim of publishing the results of scientific research on problems of legal science, improving legislation, and law enforcement. The publication is intended for researchers, teachers, postgraduates, doctoral students, practical workers in the judicial and law enforcement fields, and all those interested in the problems of legal theory and application.

The Scientific Journal is indexed in Google Scholar.

V. I. Vernadsky National Library of Ukraine.

Institutional Repository of the European University.

DOI (Digital Object Identifier) is assigned to the scientific articles of the edition.

The editorial board of the journal systematically works on including the scientific publication in international electronic libraries, catalogs, and scientometric databases with the aim of entering the global scientific information space, increasing the journal's rating, and the citation indexes of its authors.

Address for editorial control:
16-v Academician Vernadsky Boulevard, Kyiv, 03115, Ukraine
email: legal.journal@e-u.edu.ua

ЗМІСТ

КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

МІЖНАРОДНЕ ПРАВО

КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.985
DOI 36919/3041-1149(Print).4.2024.78-84

А. Ю. Нашинець-Наумова,
доктор юридичних наук, професор,
заступник декана з науково-методичної
та навчальної роботи факультету права
та міжнародних відносин,
Київський столичний університет імені Бориса Грінченка
email: a.nashynets-naumova@kubg.edu.ua
ORCID ID 0000-0002-5811-7733;
В. В. Удовенко,
аспірант кафедри права,
ПВНЗ «Європейський університет»
email: law.kafedra@e-u.edu.ua
ORCID ID 0000-0003-3163-982X

СПОСОБИ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У КРИМІНАЛЬНІЙ ПРОТИПРАВНІЙ ДІЯЛЬНОСТІ

У статті комплексно досліджуються питання способів використання комп'ютерних технологій у кримінальній протиправній діяльності взагалі та способів вчинення кримінальних правопорушень у сфері комп'ютерної інформації зокрема. Метою статті є висвітлення сучасних наукових підходів до визначення способів кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації. Визначені наразі найтиповіші та найпоширеніші способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій. Зазначено, що способи приховування аналізованої категорії кримінальних правопорушень значною мірою обумовлені способами їхнього вчинення.

Ключові слова: *кримінальні правопорушення, які вчиняють у сфері комп'ютерної інформації, кіберзлочин, спосіб вчинення, класифікація, криміналістична характеристика, несанкціонований доступ, сліди.*

Постановка проблеми та її актуальність. Наразі кримінальні правопорушення, які вчиняють у сфері комп'ютерної інформації, є однією з найбільш динамічних груп суспільно небезпечних посягань. Швидко збільшуються показники поширеності цих кримінальних правопорушень, а також постійно зростає їхня суспільна небезпечність і змінюються способи їхнього вчинення [1, с. 332]. Для ефективного їхнього розслідування правоохоронним органам потрібно знати й правильно розуміти їхню криміналістичну характеристику, зокрема способи їхнього вчинення.

Не існує єдиної позиції серед науковців не лише щодо поняття та класифікації кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації, а й щодо визначення та класифікації способів їхнього вчинення. Спосіб вчинення кримінального правопорушення є комплексним феноменом, який існує на кількох наукових дисциплінах. Його вивчають як у кримінальному праві (юридична кваліфікація), так і в кримінальному процесі (збирання доказів) і криміналістиці (встановлення механізму злочину). На нашу думку, він охоплює дії з готування до кримінального правопорушення, його безпосереднє вчинення та спроби приховування слідів кримінального правопорушення.

Аналіз останніх досліджень і публікацій. Питаннями кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації, та, зокрема, способів їхнього вчинення займалися такі вчені, як Н. М. Ахтирська, І. В. Гора, О. Є. Користін, М. Ю. Літвінов, Р. В. Лук'янчук, В. В. Марков, О. І. Мотлях, Я. В. Неділько, Ю. М. Онищенко, О. В. Орлов, Л. П. Паламарчук, П. І. Пушкаренко, К. М. Рудой, Є. Д. Скулиш, В. Г. Хахановський та інші.

Термін «спосіб» є багатогранним і може бути виражений залежно від контексту. Зокрема, його тлумачать як певну дію, прийом чи систему прийомів, що дає змогу зробити, виконати щось, досягти потрібного результату [2, с. 1179]. Як зазначає Є. М. Рожик, посилаючись на І. В. Гору, спосіб вчинення злочину є центральним моментом у генезисі злочинної поведінки. Саме спосіб вчинення злочину є тією основною якісною характеристикою діяльності злочинця, яка найтісніше взаємопов'язана з властивостями інших елементів злочинної події [3, с. 200].

З огляду на зазначене спосіб вчинення кримінальних кіберправопорушень визначають як сукупність послідовних дій суб'єкта (суб'єктів), що охоплюють дії з підготування, вчинення та приховування, спрямовані на досягнення певного злочинного результату з використанням інформаційних комп'ютерних технологій [4, с. 121].

Водночас існують розбіжності між місцем вчинення кримінального правопорушення, яке вчиняють у сфері комп'ютерної інформації, та місцем підготовки й приховування, оскільки останні дії можуть відбуватися як в онлайн-, так і в офлайн-середовищі. Способи використання комп'ютерних технологій у кримінально протиправній діяльності охоплюють весь спектр того, як зловмисники використовують комп'ютери та мережі для вчинення різних видів кримінальних правопорушень. Це може охоплювати не лише кримінальні правопорушення, які вчиняють у сфері комп'ютерної інформації (ті, що відбуваються повністю в цифровому середовищі), але й традиційні загальнокримінальні злочини, в яких комп'ютери використовують як інструмент досягнення злочинного результату (наприклад, для підробки документів, шахрайства з банківськими картками тощо).

Щодо способів вчинення кримінальних правопорушень, які вчиняють у сфері інформаційних комп'ютерних технологій, О. І. Мотлях виділяє такі їхні три види:

1) способи безпосереднього доступу до комп'ютерних технологій (операційної системи) та комп'ютерної інформації;

2) способи віддаленого (опосередкованого) доступу;

3) способи виготовлення, розповсюдження на технічних носіях шкідливих програм для електронно-обчислювальної машини [5, с. 44].

Метою статті з огляду на наявність різних позицій, висвітлених науковцями, є висвітлення сучасних наукових підходів до визначення способу кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації.

Виклад основного матеріалу дослідження. Криміналістична характеристика містить у собі сукупність типових ознак, властивих певному виду кримінальних правопорушень, що дає змогу слідчим обрати найбільш ефективні методи збирання доказів, охопити всі аспекти кримінального правопорушення – від мотиву до способу приховування слідів.

Криміналістична характеристика кримінальних правопорушень у сфері комп'ютерної інформації має певну специфіку. Насамперед до неї повинні входити відомості про особу правопорушника, мотиви та цілі її злочинної поведінки, типові способи, предмет і місце посягань, а також відомості про особу потерпілого. На особливу увагу заслуговують способи, якими злочинці здійснюють свої протиправні дії під час вчинення цього виду кримінальних правопорушень. Їхня різноманітність і постійна еволюція ускладнюють процес розслідування.

Способи вчинення кримінальних правопорушень у сфері комп'ютерної інформації є способами використання комп'ютерних технологій у кримінальній протиправній діяльності. Але не всі способи використання комп'ютерних технологій у кримінально протиправній діяльності є способами вчинення кримінальних кіберправопорушень.

На думку Н. М. Ахтирської, способи вчинення кіберзлочинів варто класифікувати на підставі правової регламентації, тобто в межах статей КК України [6, с. 108–110].

З огляду на диспозиції статей 361–363[1] КК України можна вказати такі способи вчинення кримінальних правопорушень, в яких комп'ютерні технології є безпосереднім засобом вчинення кримінального правопорушення, а об'єктом – відносини у сфері використання комп'ютерних систем, обробки та зберігання комп'ютерної інформації, а саме:

1. Несанкціоноване втручання в роботу комп'ютерної системи (стаття 361).

2. Створення, розповсюдження, збут шкідливих програмних чи технічних засобів (стаття 361[1]).

3. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом (стаття 361[2]).

4. Несанкціоновані зміна, знищення, блокування, перехоплення, копіювання комп'ютерної інформації (стаття 362).

5. Порушення правил експлуатації комп'ютерних систем або порядку чи правил захисту комп'ютерної інформації в них (стаття 363).

6. Масове розповсюдження повідомлень електрозв'язку (стаття 363[1]).

Вважаємо, існують й інші способи, які можуть бути пов'язані з цими статтями, тобто способи використання комп'ютерних технологій у кримінальній протиправній діяльності, як-от: використання комп'ютерних систем для вчинення інших злочинів, наприклад шахрайство, вимагання, відмивання коштів тощо; створення ботнетів, тобто мережі заражених комп'ютерів, які використовують для здійснення DDoS-атак або розсилки спаму; маніпуляція людьми з метою отримання доступу до їхніх облікових даних чи конфіденційної інформації за допомогою створення фальшивих вебсайтів або відправка електронних листів, які імітують відомі компанії чи установи; перенаправлення користувачів на підроблені вебсайти для крадіжки даних тощо.

Якщо за основу класифікації покласти метод, який використовувався злочинцем для отримання доступу до засобів обчислювальної техніки, можна виділити такі п'ять основних груп:

1) вилучення засобів комп'ютерної техніки;

2) перехоплення інформації;

3) несанкціонований доступ;

4) маніпулювання даними та керуючими командами;

5) комплексні методи [7].

Авторський колектив медійного посібника «Особливості розслідування окремих видів злочинів» способи вчинення цього виду кримінальних правопорушень поділяє на три групи.

Перша група – це способи безпосереднього доступу. Під час їхньої реалізації інформація знищується, блокується, модифікується або копіюється. Також може порушуватися робота ЕОМ, системи ЕОМ або їхні мережі через видачу відповідних команд з комп'ютера, на якому інформація міститься.

Друга група охоплює способи опосередкованого (віддаленого) доступу до комп'ютерної інформації. До них можна віднести:

1) підключення до лінії зв'язку законного користувача (наприклад, до телефонної лінії) та одержання тим самим доступу до його системи;

2) проникнення до чужої інформаційної мережі через автоматичний перебір абонентських номерів із наступним з'єднанням з певним комп'ютером. Перебір здійснюється, допоки на іншому кінці лінії не «озветься» чужий комп'ютер (комп'ютерний «абордаж»);

3) проникнення до комп'ютерної системи з використанням чужих паролів, коли незаконний користувач видає себе за законного користувача. Щодо подібного способу, який одержав назву «повільний вибір», незаконний користувач здійснює підбір пароля для доступу до чужого комп'ютера, використовуючи для цього спеціально розроблені програми. Підібравши потрібний пароль (на думку спеціалістів, для підбору восьмизначного пароля потрібно не більше доби), незаконний користувач одержує доступ до комп'ютерної інформації та може проводити з нею будь-які дії під виглядом законного користувача: копіювати, модифікувати, видаляти, змушувати програми виконувати потрібні операції, наприклад перераховувати кошти на свої рахунки, фальсифікувати платіжні документи, викрадати конфіденційну інформацію тощо.

Третю групу становлять змішані способи, які можуть здійснюватися за допомогою як безпосереднього, так і опосередкованого (віддаленого) доступу. До таких способів належать:

1) підміна даних – заміна або введення нових даних, які здійснюються зазвичай, коли інформація вводиться або виводиться з ЕОМ;

2) таємне введення до чужої програми таких команд, які допомагають їй здійснити нові, незапланові функції в процесі одночасного зберігання її працездатності («троянський кінь»);

3) модифікація програм за допомогою таємного впровадження до програми набору команд, що повинні спрацювати за певних умов через деякий час («логічна бомба»);

4) здійснення доступу до баз даних і файлів законного користувача за рахунок знаходження слабких місць у системах захисту («маскарад» або «самозванство» – хтось проникає до комп'ютерної системи, видаючи себе за законного користувача). Системи, які не мають засобів автентичної ідентифікації (наприклад, за фізіологічними характеристиками: за відбитками пальців, сітківкою ока, голосом тощо), залишаються без захисту проти цього прийому. Найпростішим способом його здійснення є одержання ідентифікаційних кодів законних користувачів. Виявивши їх, з'являється можливість читати й аналізувати наявну в системі інформацію, копіювати її, повертатися до неї в разі потреби;

5) використання помилок у логіці побудови програми й виявлення «прогалин». У літературі подібні способи одержали найменування «аварійний» і «склад без стін». Перший дає змогу здійснити несанкціонований доступ до інформації в момент спрацьовування спеціальних програм, які застосовують на випадок виникнення збоїв або інших відхилень у роботі ЕОМ; другий – у результаті системної поломки, коли деякі файли користувача залишаються відкритими й злочинець одержує можливість несанкціонованого доступу до цієї бази даних;

6) поширення комп'ютерними мережами або продаж програм, що призводить до знищення або блокування інформації, порушення працездатності ЕОМ, системи ЕОМ або їхньої мережі, охоплюючи переважну більшість комп'ютерних вірусів (на сьогодні спеціалістам відомо близько 15 тисяч видів вірусів) [8].

З огляду на реалії сьогодення Я. В. Неділько визначає найтиповіші та найпоширеніші нині способи вчинення кримінальних правопорушень з використанням інформаційних комп'ютерних технологій: 1) використання шкідливого програмного забезпечення; 2) вчинення DoS / DDoS-атак; 3) несанкціонований доступ до інформації; 4) шахрайство, вчинене з використанням інформаційних комп'ютерних технологій; 5) поширення шкідливого (протиправного) контенту (спам, погрози, створення, поширення та збут дитячої порнографії, заклики до вчинення насильства, домагання тощо); 6) порушення авторських чи суміжних прав з використанням інформаційних комп'ютерних технологій; 7) комплекс способів і використання інформаційних комп'ютерних технологій як засіб користування кіберпростором для вчинення інших кримінальних правопорушень [4, с. 123].

Відповідно до наведених підстав пропонуємо більш детальну класифікацію з урахуванням сучасних тенденцій.

1. За метою атаки:

- фінансова (вимагання викупу (*ransomware*), крадіжка банківських даних, шахрайство з криптовалютами, відмивання грошей);
- політична (кібератаки на державні установи, дестабілізація суспільства, кібершпигунство);
- ідеологічна (розповсюдження екстремістських матеріалів, кібертероризм);
- вандалізм (DDoS-атаки, руйнування даних, дефейсмент сайтів);
- конкурентна розвідка (викрадення комерційної таємниці);
- особиста помста (кібератаки на конкретних осіб або організації).

2. За засобами атаки:

- шкідливе програмне забезпечення (віруси, трояни, черви, ботнети, ransomware);
- соціальна інженерія (фішинг, виманювання паролів, претекстинг);
- експлойти (використання вразливостей у програмному забезпеченні);
- брутфорс (перебір усіх можливих комбінацій паролів);
- DDoS-атаки (відмова в обслуговуванні);

- ботнети (мережі заражених комп'ютерів для здійснення масованих атак);
- інструменти віддаленого доступу (RAT – *Remote Access Trojan*);
- атаки на бездротові мережі (Wi-Fi hacking, Bluetooth hacking);
- атаки на хмарні середовища (викрадення даних, DDoS-атаки на хмарні сервіси);
- атаки на блокчейн (маніпуляції з транзакціями, крадіжка криптовалют).

3. За етапами атаки:

- розвідка (збір інформації про ціль);
- проникнення (отримання несанкціонованого доступу);
- підтримання доступу (збереження контролю над системою);
- виконання злочинних дій (викрадення даних, руйнування системи тощо);
- приховування через видалення слідів злочинної діяльності.

Важливо зазначити, що ця класифікація не є вичерпною, оскільки постійно з'являються нові способи вчинення кримінальних правопорушень, пов'язаних з комп'ютерною інформацією. Проте вона охоплює широкий спектр сучасних кіберзагроз, різні критерії та враховує нові технології й тенденції в кіберзлочинності.

Одна з ключових проблем розслідування кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації, полягає в їхній надзвичайній швидкості й анонімності. Вони можуть бути вчинені практично миттєво через автоматизацію та використання мережевих технологій. Зловмисник може, зокрема, за лічені секунди отримати несанкціонований доступ до системи, викрасти конфіденційні дані або запустити шкідливу програму [9, с. 147].

Отже, підготовка до кримінального правопорушення, яке вчиняють у сфері комп'ютерної інформації, може зайняти від кількох хвилин до кількох місяців і більше, залежно від складності атаки, навичок та цілей зловмисника. Вона може охоплювати дії зі збору інформації про потенційні цілі, аналіз їхньої вразливості, пошук експлойтів, розробку детального плану атаки, вибір інструментів і методів, визначення ролей учасників (за наявності).

Швидкість поширення кіберзагроз, високий рівень анонімності й відсутність доказів роблять кримінальні правопорушення, які вчиняють у сфері комп'ютерної інформації, особливо складними для розслідування, вимагаючи від правоохоронних органів застосування спеціальних технологій і знань. Водночас нерідкісними є випадки, коли після вчинення кримінального правопорушення злочинці намагаються приховати сліди своєї протиправної діяльності. Вони можуть видаляти файли, змінювати налаштування системи, використовувати спеціальні програми для приховування своїх дій тощо.

Способи приховування аналізованої категорії кримінальних правопорушень значною мірою обумовлені способами їхнього вчинення. У разі безпосереднього доступу до комп'ютерної інформації приховування слідів кримінального правопорушення зводиться до відтворення обстановки, що передувала його вчиненню, тобто знищення залишених слідів (зокрема, слідів пальців рук на клавіатурі, кнопках дисководів та інших поверхнях, яких торкався злочинець; слідів взуття; мікрочасток тощо). Під час опосередкованого (віддаленого) доступу приховування полягає в самому способі вчинення кримінального правопорушення, що ускладнює виявлення неправомірного доступу. Зокрема, використання універсальних програм, призначених для застосування в аварійних ситуаціях, дає змогу не лише здійснити несанкціонований доступ до комп'ютера, оминаючи всі засоби захисту та контролю, а й довільно змінювати будь-які атрибути файлів, не залишаючи водночас ніяких слідів (робота цих програм не протоколюється) [8].

Зловмисники часто використовують проксі-сервери та VPN для маскування своєї IP-адреси та географічного розташування, ускладнюючи відстеження їхньої діяльності. Для обходу систем фільтрації та захисту мережі можуть створювати зашифровані тунелі, які дають змогу передавати дані непомітно. Для проведення фінансових операцій, пов'язаних з кримінальними правопорушеннями в сфері комп'ютерної інформації, часто використовують криптовалюти, що ускладнює відстеження руху коштів.

Висновки. Отже, розуміння способу вчинення кримінального правопорушення загалом і кримінальних правопорушень, які вчиняють у сфері комп'ютерної інформації, зокрема є фундаментальним аспектом криміналістичної характеристики цього виду злочинності. Він дає змогу не лише детально зрозуміти механізми вчинення таких кримінальних правопорушень,

але й розробити ефективні методики їхнього розслідування. Захист, заснований на розумінні загроз, в поєднанні з ефективним розслідуванням, що використовує сучасні технології та міждисциплінарний підхід, дасть змогу мінімізувати збитки від кіберзагроз і забезпечувати кібербезпеку в сучасному цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримський Т. С. Способи вчинення злочинів, пов'язаних з несанкціонованим доступом до комп'ютерних мереж та мереж електрозв'язку. *Юридична наука.* 2020. № 109. С. 33–338.

2. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2001. 1440 с.

3. Рожик Є. М. Співвідношення способу вчинення злочину та наслідків злочину. *Право і суспільство*. 2020. Ч. 2, № 6. С. 200–207.

4. Неділько Я. В. Криміналістичний аспект способів вчинення кримінальних правопорушень, що вчиняються з використанням інформаційних технологій. *Knowledge, Education, Law, Management.* 2021. № 8 (44), vol. 2. С. 119–124. DOI : https://doi.org/10.51647/kelm.2021.8.2.19

5. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 221 с.

6. Ахтирська Н. М. Актуальні питання розслідування кіберзлочинів : навч. посіб. Київ : Київ. ун-т, 2018. 229 с.

7. Правопорушення в сфері високих інформаційних технологій. URL : https://arm.naiau.kiev.ua/ books/ kryminalist_inform/lection/lec6.html

8. Особливості розслідування окремих видів злочинів : медійн. навч. пос. URL : ttps://arm.naiau.kiev.ua/books/orovz/lections/lection8.html

9. Грищенко Д. О., Андрієнко І. А. Особливості розслідування кіберзлочинів у сфері високих технологій. *Проблеми сучасної поліцеїстики.* Вінниця, 2024. С. 146–148.

REFERENCES

1. Krimskij T. S. (2020). Sposobi vchinennya zlochiniv, pov'yazanih znesankcionovanim dostupom do komp'yuternih merezh ta merezh elektrozv'yazku [Methods of perpetrating cybercrimes involving unauthorized access to computer and communication networks]. *Yuridichna nauka.* № 109. Pp. 331–338 [in Ukrainian].

2. Velikij tlumachnij slovnik suchasnoyi ukrayinskoyi movi. (2001) [*Great Explanatory Dictionary of Modern Ukrainian*] / uklad. i golov. red. V. T. Busel. Kiyiv ; Irpin : Perun, 1440 p. [in Ukrainian].

3. Rozhik Ye. M. (2020). Spivvidnoshennya sposobu vchinennya zlochinu ta naslidkiv zlochinu [Relationship between the mode of committing a crime and the consequences of a crime]. *Pravo i suspilstvo.* Ch. 2, № 6. Pp. 200–207 [in Ukrainian].

4. Nedilko Ya. V. (2021). Kriminalistichnij aspekt sposobiv vchinennya kriminalnih pravoporushen, sho vchinyayutsya z vikoristannyam informacijnih tehnologij [Forensic aspects of crimes committed using information technology]. *Knowledge, Education, Law, Management.* № 8 (44), vol. 2. Pp. 119–124 [in Ukrainian].

5. Motlyah O. I. (2005). Pitannya metodiki rozsliduvannya zlochiniv u sferi informacijnih komp'yuternih tehnologij [Methods of investigating crimes in the field of information and computer technology] : dis. … kand. yurid. nauk : 12.00.09. Kiyiv, 221 p. [in Ukrainian].

6. Ahtirska N. M. (2018). Aktualni pitannya rozsliduvannya kiberzlochiniv [Current issues in cybercrime investigations] : navch. posib. Kiyiv : Kiyiv. un-t, 229 p. [in Ukrainian].

7. Pravoporushennya v cferi visokih informacijnih tehnologij [Information technology offenses]. URL : https://arm.naiau.kiev.ua/books/kryminalist_inform/lection/lec6.html [in Ukrainian].

8. Osoblivosti rozsliduvannya okremih vidiv zlochiniv [Specifics of investigating different types of crimes] : medijn. navch. pos. URL : ttps://arm.naiau.kiev.ua/books/orovz/lections/lection8.html [in Ukrainian].

9. Grishenko D. O., Andriyenko I. A. (2024). Osoblivosti rozsliduvannya kiberzlochiniv u sferi visokih tehnologij [Specifics of investigating cybercrimes in the field of high technology]. *Problemi suchasnoyi policeyistiki.* Vinnicya. Pp. 146–148 [in Ukrainian].

A. Yu. Nashynets-Naumova, V. V. Udovenko. METHODS OF USING COMPUTER TECHNOLOGIES IN CRIMINAL ACTIVITIES

The article comprehensively examines the issues of ways of using computer technologies in criminal illegal activities in general and ways of committing criminal offenses, in the field of computer information. The purpose of the article is to highlight modern scientific approaches to determining the methods of criminal offenses committed in the field of computer information. Currently, the most typical and common ways of committing criminal offenses with the use of computer information technologies have been determined. It is noted that the methods of hiding the analyzed category of criminal offenses are largely determined by the methods of their commission.

Keywords: *method, computer crime, cybercrime, classification, forensic characteristics, unauthorized access.*

Стаття надійшла до редколегії 24 вересня 2024 року