# ТЕОРІЯ І ПРАКТИКА КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНОЇ ДІЯЛЬНОСТІ ТА КРИМІНАЛІСТИКИ. ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

*УДК 343.9.01*
DOI 10.32755/sjlaw.2020.03.089

**Гарига М. М.,**
судовий експерт, провідний фахівець
з організації наукової роботи відділу забезпечення діяльності
Чернігівського науково-дослідного експертно-криміналістичного
центру МВС України, м. Чернігів, Україна;
**Вергун Л. О.,**
засновник і керівник IT агентства WellDigital,
м. Київ, Україна;
**Кузнєцов О. О.,**
старший викладач кафедри тактико-спеціальної підготовки,
Академія Державної пенітенціарної служби, м. Чернігів, Україна
ORCID: 0000-0002-1064-9116

## ДЕЯКІ АСПЕКТИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

*У статті проведено аналіз динаміки здійснення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за 2019-2020 роки, акцентовано увагу на необхідності вдосконалення наявних та створення нових дієвих механізмів протидії відповідним злочинним виявам. Описано основні підходи та наведено коротку криміналістичну характеристику кіберзлочинів. Запропоновано приміpний перелік завдань, що можуть ставитись перед експертами-криміналістами у випадку їх участі в розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.*

***Ключові слова:*** *кіберзлочинність, кіберзлочини, статистика злочинності, комп'ютерні злочини.*

**Постановка проблеми.** В усьому світі спостерігається швидке зростання використання інтернету поряд з безпрецедентним зростанням кіберзлочинності.

За даними Генеральної прокуратури України (табл.) [1], станом на кінець червня 2020 року органами Національної по-

ліції обліковується 1 283 злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Хоча відсоткова частка від загальної кількості облікованих злочинів і становить трохи менше 1 відсотка, але чисельна стабільність цього показника на тлі 20 % зменшення загальної кількості правопорушень у порівнянні з 2019 роком свідчить про високу пристосувальну здатність вказаного злочинного сегмента з одного боку, а також про необхідність удосконалення наявних та створення нових дієвих механізмів протидії відповідним злочинним виявам.

Таблиця

**Порівняльна таблиця чисельності кримінальних правопорушень, досудове розслідування в яких здійснюється органами Національної поліції**

| **Розподіл злочинів за родовим об'єктом** | **Обліковано кримінальних правопорушень у звітному періоді** | |
|---|---|---|
| | Січень – червень 2019 | Січень – червень 2020 |
| 1 | 2 | 3 |
| Злочини проти основ національної безпеки | 214 | 214 |
| Злочини проти життя та здоров'я особи | 26 248 | 23 625 |
| Злочини проти волі, честі та гідності особи | 571 | 387 |
| Злочини проти статевої свободи та статевої недоторканості особи, що виявлені органами внутрішніх справ | 413 | 398 |
| Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина | 4 277 | 3 341 |
| Злочини проти власності | 148 943 | 110 968 |
| Злочини у сфері господарської діяльності | 1 959 | 1 716 |
| Злочини проти довкілля | 1 506 | 2 988 |
| Злочини проти громадської безпеки | 6 202 | 4 599 |
| Злочини проти безпеки виробництва | 791 | 724 |
| Злочини проти безпеки руху та експлуатації транспорту | 8 386 | 7 691 |
| Злочини проти громадського порядку та моральності | 3 988 | 3 524 |
| Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення | 15 650 | 17 191 |
| Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації | 679 | 262 |
| Злочини проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та злочини проти журналістів | 13 574 | 12 628 |

Закінчення табл.

| 1 | 2 | 3 |
|---|---|---|
| Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку | 1 271 | 1 283 |
| Злочини у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг | 7 104 | 7 344 |
| Злочини проти правосуддя та інші злочини, розслідувані органами Національної поліції | 4 762 | 3 897 |
| Всього | 24 8343 | 202 566 |

**Аналіз останніх досліджень і публікацій.** Дослідженню питань протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж присвятили свої роботи вітчизняні та зарубіжні науковці, зокрема: В. Г. Хахановський, Н. Г. Шурухнов, О. Ю. Довженко, В. Б. Вєхов, Ю. М. Батурин, В. М. Бутузов, В. Д. Гавловський, В. О. Голубєв, М. В. Гуцалюк, Р. А. Калюжний та ін.

**Метою статті** є розгляд деяких аспектів криміналістичної характеристики кіберзлочинів.

**Виклад основного матеріалу**. Для науки криміналістики кіберзлочинність є порівняно новою категорією дослідження, а тому потребує достатньо фундаментальних досліджень для формування системи відомостей про вказаний вид злочинів, ознаки особи злочинця, його можливі мотиви, предмет посягання, злочинні способи, обстановку, інші обставини, що мають значення для виявлення, розслідування та розкриття таких діянь криміналістичними прийомами, методами та засобами.

Як зазначає В. Ю. Шепітько, структурну основу цієї системи становлять кримінально-правова та кримінально-процесуальна характеристики: система елементів складу злочину й обставин, що підлягають доказуванню, визначають тією чи іншою мірою структуру кримінологічної та криміналістичної характеристик злочину. Залежно від особливостей того чи іншого виду злочинів структура елементів кримінально-правової характеристики конкретизується включенням відповідних факультативних елементів, наприклад, предмет безпосереднього злочинного посягання, особа потерпілого [2].

Аналізуючи Закон України «Про основні засади забезпечення кібербезпеки України» [3], розширене визначення кіберз-

лочинності можна сформулювати як сукупність суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Для позначення цього виду суспільно небезпечних діянь також застосовують такі терміни, як: «злочинність у віртуальному просторі», «локальні та транснаціональні комп'ютерні злочини», «злочини, що вчиняються за допомогою мережі Internet».

Хахановський В. Г. стверджує, що стосовно кіберзлочинів найбільший інтерес становлять сліди, що вказують на те, як злочинець потрапив і зник з місця події, подолав перешкоди, використав своє службове становище, виконав поставлену злочинну мету, які знання та навички використав, чи спробував приховати сліди своїх дій. Важливі також сліди, що свідчать про характер зв'язку злочинця з предметом злочинного посягання тощо. Спосіб учинення злочину в низці складів є необхідним елементом об'єктивної сторони злочину та входить до його кримінально-правової характеристики, а іноді слугує навіть кваліфікувальною обставиною. Однак у кримінально-правовій характеристиці спосіб учинення злочину подано в загальному вигляді, для неї байдужі конкретні способи проникнення, засоби, що використовують при цьому, джерела їх отримання і т. ін. Якщо ж ці обставини суттєві, застосовують криміналістичну характеристику способу вчинення злочину [4].

Шурухнов Н. Г. структурує способи неправомірного доступу до комп'ютерної системи на такі групи:

– способи безпосереднього доступу;

– способи віддаленого доступу;

– комплексні способи [5, с. 103–110].

Довженко О. Ю., посилаючись на Конвенцію Ради Європи про кіберзлочинність, описує класифікацію з п'яти елементів. Перша група кіберзлочинів містить протиправні діяння, що посягають на конфіденційність, цілісність та недоступність комп'ютерних даних і систем, таких як несанкціонований доступ, незаконне перехоплення, втручання в бази даних і в систему. Другу групу становлять злочини, пов'язані з використанням

комп'ютерів як засобу здійснення протизаконних дій, тобто засобу маніпуляції з інформацією. До них можна віднести комп'ютерне шахрайство та комп'ютерне підроблення. Третя група – кіберзлочини, пов'язані зі змістом даних, що розміщені в комп'ютерних мережах. Найбільш розповсюдженим та найбільш суворо переслідуваним з таких злочинів є діяння, пов'язані з дитячою порнографією. Четверту групу злочинів становлять злочини, пов'язані з порушенням авторського права та суміжних прав, при чому встановлення таких правопорушень Конвенцією віднесено до компетенції національних держав. Нарешті, п'ята група, що була запроваджена Додатковим протоколом, складається з актів расизму та ксенофобії, що скоєні за допомогою комп'ютерних мереж [6].

До завдань, що вирішуються фахівцями Департаменту кіберполіції Національної поліції України, описаних Міністром внутрішніх справ на своїй сторінці однієї з соцмереж [7], належить, зокрема, протидія кіберзлочинам.

1. У сфері використання платіжних систем:

– скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;

– кеш-трепінг – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

– кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;

– несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

2. У сфері електронної комерції та господарської діяльності:

– фішинг – виманювання в користувачів інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування або обміну валюти тощо;

– онлайн-шахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

У сфері інтелектуальної власності:

– піратство – незаконне розповсюдження інтелектуальної власності в інтернеті;

- кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.

3. У сфері інформаційної безпеки:

- соціальна інженерія – технологія управління людьми в інтернет-просторі;

- мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

- протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства;

- рефайлінг – незаконна підміна телефонного трафіку.

Цей перелік свідчить про значний відсоток злочинів, пов'язаний зі зломом вебсайтів.

Існують такі основні методи злому вебсайтів.

SQL-ін'єкція – вставка SQL-запиту в текст, що відправляється через інтерактивні форми. Таким способом можна отримати несанкціонований доступ до бази даних сайту.

Міжсайтове виконання сценаріїв (XSS) – запуск спеціалізованого скрипту на сайті чи окремій сторінці для його подальшої взаємодії з вебсервером зловмисника та подальшого отримання конфіденційних даних користувачів.

Вразливості в ядрі сайту або системі управління контентом (CMS). Знаючи версію програмного забезпечення сайту, зловмисник може знайти уразливості для нього і експлойти до цих вразливостей.

Фішинг. За допомогою фішингу зловмисник може дізнатися пароль від панелі адміністрування або FTP-сервера.

Загальний (shared) хостинг. Якщо на такому хостингу неправильно налаштовані права доступу, то є можливість зламати сайт через вразливих «сусідів».

Після вдалого злому перед зловмисником відкриваються великі можливості: вкрасти базу, кошти і ресурси, розпочати заражати комп'ютери відвідувачів шкідливими програмами, розміщувати несанкціоновану рекламу на зламаному сайті, продати доступ до панелі управління, влаштувати фішинг-розсилку і т. ін. Далі розглянемо методи злому детально [8].

Про SQL-ін'єкції можна не говорити, оскільки це вразливість застаріла. Сьогодні трапляється досить рідко, особливо з появою підготовлених запитів і різних фреймворків, які теж стають дуже популярними, але чомусь не всі знають що це таке. Особливо ті програмісти, хто пише тільки на фреймворках. SQL-ін'єкція – це коли через user input прописують шматок SQL шкідливого запиту і вебсайт цей input ніяк не фільтрує. Таким чином зловмисник може просто стерти всю вашу базу даних за допомогою цієї уразливості або злити йому потрібні дані. І перше, що рекомендується робити для захисту, це серйозно фільтрувати user input або використовувати підготовлені запити. Тобто принцип підготовленого запиту полягає в тому, що створюється незмінний запит, в якому просто вставляються значення під час виконання.

Cross-Site Scripting – цей вид атаки працює приблизно так само як і SQL-ін'єкції, але його метою є не база даних, але відвідувачі і користувачі вебсайту. Всі також через якийсь input на сайті, зловмисники намагаються пробити, як правило, шматок javascript коду. Зазвичай таким чином зливають кукіси, після чого можуть авторизуватися на сайті без пароля і логіна. Особливо небезпечною ця вразливість буває для сайтів комерційних проєктів. Оскільки отримавши доступ до акаунту, зловмисники зможуть робити все, що захочуть. Особливо буде погано, якщо вони отримають доступ до акаунту адміністратора з повним доступом.

Cross-Site Request Forgery. Форма злому, коли абсолютно інший сайт людина підробляє форму, наприклад, пост запиту на сайт жертви і змушує кожного відвідувача перейти за цією формою і часто за допомогою методу clickjacking, тому жертва нічого за фактом взагалі не натискає. Підробляється http запит і на сайті жертви відбувається шкідливий вплив. Наприклад, можна відправити вашому другу листа в Telegram, а ви цього можете навіть не бачити [9].

Cookie Faking. Тут все просто і сесії, і кукіси зберігаються, а це значить, що їх можна запозичити з комп'ютера жертви. Той же PHP зберігає сесії у себе, а в користувача в кукіс зберігає мітку PHP ssid, який можна скачати. Але тут важливіше не се-

сії, а кукіси. І якщо їх можна скачати, значить їх можна підставити у свій браузер. А значить можна зайти на потрібний сайт від імені жертви. Зазвичай зливом кукісів займаються віруси, яких користувач навіть не помічає.

Man-In-The-Middle. MITM – це коли хакер перехоплює ваші пакети та змінює їх. Тобто ви зі свого комп'ютера пишете повідомлення, а хакер змінює цей пакет і повідомлення, яке надходить, змінює зміст.

Clickjacking на сайті шахрая він відкриває iFrame з юрл-адресою сайту жертви, вішає його координати миші і дає йому тотальну прозорість. Людина бачить напис натисни на мене. І сам того не розуміючи, клікає на iFrame, який точно стоїть біля нього під мишею. Ну і рухає він його за допомогою javascript.

Brute-Force – це коли зловмисник запускає скрипт перебору паролів до певної email адреси або логіну, щоб дістати доступ до акаунту.

Zero Day – це вразливість першого дня. Це коли після релізу була допущена діра в програмному забезпеченні, за допомогою якої хакер може пробити ваш захист. Взагалі до таких проблем належить не тільки Zero Day, а й взагалі будь-які діри у старому ПО. Щоб захиститися від такої атаки, ви постійно повинні оновлювати своє програмне забезпечення [10].

Backdoor. Найчастіше з цим видом стикаються програмісти під WordPress і всі інші CMS системи або просто користувачі цих сіемесок. Вони також стикаються з BlackSeo, але це не можна назвати явною уразливістю або якою-небудь там атакою, тому про BlackSeo ми говорити не будемо. Що ж стосується бекдор, так це просто зашифровані скрипти. Які або окремими файлами, або хвостами знаходяться на вашому сервері і завдяки ним хакер отримує до вашого сервера доступ і, як правило, нерідко експлуатує його як Botnet. Найчастіше бекдор зливають бази, сайти або навіть можуть видалити проєкти та просити грошей за нього.

Перед експертами-криміналістами в такому випадку можна ставити такі завдання:

– з'ясувати, як була реалізована атака;

– побудувати сценарій злому;

– відтворити хронологію (таймлайн) атаки;

– виявити та зафіксувати сліди, залишені в результаті атаки;

– запропонувати превентивні заходи щодо запобігання таких атак.

Щодо характеристики особи злочинця та потерпілого, то В. Б. Вєхов виділяє такі три групи комп'ютерних злочинців: особи, особливістю яких є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості; особи, які страждають на новий вид психічних захворювань – інформаційні хвороби (комп'ютерні фобії); професійні комп'ютерні злочинці з яскраво вираженою корисливою метою (за В.Г. Хахановським).

Потерпілими від кіберзлочинів найчастіше є юридичні особи. Це зумовлено тим, що процес комп'ютеризації широко охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб.

Виокремлюють три головні групи потерпілих від таких злочинів: власники комп'ютерної системи; клієнти, які користуються їх послугами; інші особи. Слід зазначити, що потерпіла сторона першої групи, як правило, неохоче звертається (якщо робить це взагалі) до правоохоронних органів за фактом учинення злочину, що, зокрема, є одним з головних факторів, який спричиняє високий рівень латентності такого виду злочинів [4].

**Висновки.** Таким чином, сучасна динаміка інформатизації в усіх сферах суспільних відносин вимагає від України забезпечити ефективний механізм боротьби із кіберзлочинами як однією із серйозних загроз національній безпеці. Однією з умов існування таких механізмів є наявність ґрунтовної криміналістичної характеристики вказаної групи злочинів, що дозволяє виявити та зрозуміти закономірності підготовки, вчинення та приховування цієї групи протиправних діянь.

**Список використаних джерел**

1. Статистична інформація за 2011–2020 роки. *Генеральна прокуратура:* офіційний вебсайт. URL: https://old.gp.gov.ua/ua/statinfo.html (дата звернення: 01.07.2020).

2. Криміналістика / за ред. В. Ю. Шепітька. 2-ге вид., переробл. і доповн. Київ: Ін Юре, 2004. 728 с. URL: https://buklib.net/books/21972/ (дата звернення: 01.07.2020).

3. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017. *База даних «Законодавство України»* / Верховна Рада України. Дата оновлення: 03.07.2020. URL: https://zakon.rada.gov.ua /laws/show/2163-19#Text (дата звернення: 10.07.2020).

4. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів. *Юридичний часопис Національної академії внутрішніх справ*. 2011. № 1 (1). С. 89–93. URL: http://nbuv.gov.ua/UJRN /aymvs_2011_1(1)__13 (дата звернення: 06.07.2020).

5. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. Москва: Щит-М, 1999. 254 с.

6. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019 (1). URL: http://www.sulj.oduvs.od.ua/archive/2019/1/7.pdf (дата звернення: 01.07.2020).

7. Аваков А. Кіберполіція (крок реформі). Дата оновлення: 11.10.2015. URL: https://www.facebook.com/arsen.avakov.1/posts/ 916452195111554 (дата звернення: 01.07.2020).

8. Тюрин А. В поисках лазеек: гид по DOM Based XSS. *Хакер*. 2013. № 172. С. 80–85.

9. Seth Fogie, Jeremiah Grossman, Robert Hansen, Anton Rager, Petko D. Petkov. XSS атаки: эксплуатация и защита. XSS Attacks: Cross Site Scripting Exploits and Defense. Syngress, 2007. 464 p.

10. Stewart, James Michael. CISSP®: Certified Information Systems Security Professional Study Guide / Mike Chapple, Darril Gibson. Seventh Edition., Canada: John Wiley & Sons, Inc., 2015. 1023 p.

**Haryha M., Verhun L., Kuznetsov O.**

## SOME ASPECTS OF CRIMINAL CHARACTERISTICS OF CYBER CRIMES

*The article analyzes the dynamics of crimes in the use of computers, systems, computer networks and telecommunications networks for 2019-2020, and focuses on the high "adaptive" ability of this criminal segment as well as the need to improve existing and create new effective mechanisms to combat relevant criminal acts. One of the conditions for the existence of such mechanisms is the presence of thorough forensic characteristics of this group of crimes, which allows identifying and understanding the training, commission and concealment of the group of illegal acts. The research describes the main approaches to determining the mandatory and optional features of the crime in the use of computers, systems and computer networks. The article also provides a brief forensic description of cybercrime in accordance with the generally accepted system, which contains the following elements: the identity of the offender, methods of preparation for the crime; the victim, the subject of the offense; the circumstances of the crime, the*

*consequences of any changes caused by the crime in the physical material damage reflected in the material situation of the crime. To determine the scope of the investigated illegal actions, a list is given to be solved by specialists of the Cyber Police Department of the National Police of Ukraine. Additionally, the main methods of hacking websites are described, including: SQL injection, Cross-site scripting, Phishing, Shared hosting, Cross-Site Scripting, Cross-Site Request, ForgeryCookie Faking, Man-In-The-Middle , Clickjacking, Brute-Force, Zero Day, Backdoor. An approximate list of tasks that may be assigned to forensic experts in the case of their participation in the investigation of crimes in the use of electronic computers, systems and computer networks.*

***Key words:*** *cybercrime, cyber crime actions, crime statistics, computer crimes.*

## References

1. Statistical information for 2011–2020, *Office of the Prosecutor General:* official web-site, available at: https://old.gp.gov.ua/ua/statinfo.html (last accessed at: 01.07.2020).

2. Criminalistics (2004) / in Shepitka, V. Yu. (Ed.), Vol. 2, Concern Publishing House "In Jure", Kyiv, available at: https://buklib.net/books/21972/ (last accessed at: 01.07.2020).

3. Ukraine (2017), *On the Basic Principles of Cybersecurity in Ukraine*: Law of Ukraine dated 05.10.2017: The Verkhovna Rada of Ukraine, available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (last accessed at: 10.07.2020).

4. Khahanovskyi, V. G. (2011), "Features of forensic characteristics of cybercrimes", *Legal Journal of the National Academy of Internal Affairs*, № 1 (1), pp. 89–93, available at: http://nbuv.gov.ua/UJRN/aymvs_2011_1(1)__13 (last accessed at: 06.07.2020).

5. Investigation of illegal access to computer information (1999) / in Shurukhnova, N.G. (Ed.), Shchit-M, Moscow.

6. Dovzhenko, O. Yu. (2019), "Classification of cybercrimes in criminology", *South Ukrainian Law Journal*, (1), available at: http://www.sulj.oduvs.od.ua/archive/2019/1/7.pdf (last accessed at: 01.07.2020).

7. Avakov, A. (2015), Cyberpolice (reform step), available at: https://www.facebook.com/arsen.avakov.1/posts/916452195111554 (last accessed at: 01.07.2020).

8. Tiurin, A. (2013), "In search of loopholes: guide to DOM Based XSS // Hacker", *Magazine*, № 172, pp. 80–85.

9. Fogie, S., Grossman, J., Hansen, R., Rager, A., Petkov, D. (2007), XSS Attacks: Cross Site Scripting Exploits and Defense, *Syngress*.

10. Stewart, J. M. (2015), *CISSP: Certified Information Systems Security Professional Study Guide*, John Wiley & Sons, Inc., Canada.