DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

УДК 343.973

Близнюк Ігор Леонідович,
кандидат юридичних наук, старший науковий співробітник,
головний науковий співробітник ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0003-3882-5790

ХАРАКТЕРИСТИКА ТИПОВИХ СПОСОБІВ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ В УМОВАХ ВОЄННОГО СТАНУ

У статті надається характеристика типових способів вчинення кіберзлочинів. Розкрито особливості причинного комплексу кіберзлочинності. Детально розглядаються причини, чому кіберзагрози еволюціонують у прискореному темпі, а кіберзлочини стають досконалішими, краще організованими і транснаціональними.

Наведені типи кіберзлочинів, які становлять найбільшу загрозу на сьогодні в умовах воєнного стану. Розглянуті також зміни кримінального та кримінально-процесуального законодавства, які відбулись під час війни, з удосконаленням підстав та процесуальних механізмів притягнення до кримінальної відповідальності кіберзлочинців.

Ключові слова: *кіберзлочини, кіберзлочинність, воєнний стан, кримінальне та кримінально-процесуальне законодавство, кібершахрайство, фішинг, кібертероризм, кібершпигунство, DDoS-атаки або DoS-атаки, дефейс, скімінг, дистанційне банківське обслуговування.*

Сьогодні кіберзлочинність є однією з найгостріших проблем інформаційної безпеки держави. Ризики кібербезпеки постійно зростають, як у їх поширеності, так і у руйнівному потенціалі. Наприклад, кількість кібератак на підприємства у світі подвоїлася протягом останніх років, а кіберінциденти, які колись розглядалися як надзвичайні, сьогодні стають все більш розповсюдженими [2, с. 42]. Відповідно до офіційної статистики Офісу Генерального прокурора України, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже в 7,5 рази (і це не враховуючи класичні правопорушення з використанням комп'ютерної техніки, а також рівня латентності такої злочинності) [1].

Наслідком зростаючого використання інформаційних технологій стало одночасне зростання та поширення кіберзагроз, зокрема, і у формі кіберзлочинів [3, с. 9]. Крадіжки даних платіжних карток (банківських рахунків) або даних доступу до системи Інтернет-банкінгу з метою заволодіння коштами клієнтів банку, несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, викрадення персональних даних та комерційної інформації з приватних комп'ютерів або серверів, умисне пошкодження роботи інформаційних систем або засобів комунікацій з метою створення збитків компаніям, розповсюдження комп'ютерних вірусів, DDoS-атаки на Інтернет-ресурси, шахрайство в інформаційних мережах – це далеко не повний перелік кіберзагроз, які несе з собою бурхливий

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).9

розвиток сучасних інформаційних технологій, та відповідно, визначається таким поняттям як кіберзлочинність. Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, здійснення незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет [4, с. 37]. При цьому дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій [5, с. 116].

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують у прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними [6, с. 150]. Це зумовлено тим, що Інтернет, цифрові послуги, інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, Інтернет-магазинів та онлайн-банкінгу до систем штучного інтелекту та інтелектуальних систем управління компаніями. Зі зростанням залежності від використання ІКТ у бізнесі і підприємництві, відповідно, зростають кіберризики і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення [6, с. 150].

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційно-психологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки [7].

Масового характеру набули електронні розкрадання грошових коштів у великих та особливо великих розмірах, заподіяння майнової шкоди в сфері інформаційно-телекомунікаційних технологій, неправомірний (несанкціонований) доступ до охоронюваної законом комп'ютерної інформації (інформаційних ресурсів), підробка електронних документів, порушення авторських прав тощо. Зокрема, серйозне занепокоєння викликає поширення фактів протизаконного збору та використання інформації, у тому числі як незаконної, так і шкідливої, протиправного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку [9, с. 221].

На сьогодні існує багато типів кіберзлочинів, серед яких найбільшу загрозу, на думку експертів, становлять: онлайн шахрайство, DDoS-атаки або DoS-атаки[1], дефейс (тип хакерської атаки, при якій сторінка вебсайту замінюється на іншу), розповсюдження шкідливих програм (вірусів), кардерство (вид шахрайства, при якому проводиться операція з використанням платіжних карток або їх реквізитів,

[1] Різниця між DoS і DDoS-атаками полягає в тому, що під час DDoS-атаки багато шкідливих машин спрямовані на один ресурс. Атака розподіленої відмови в обслуговуванні (DDoS) набагато успішніша у руйнуванні цілі, ніж атака DoS, що виходить з одного джерела.

яка не ініційована або не підтверджена її власником), фішинг (вид шахрайства, відповідно до якого, наприклад, клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі), комп'ютерне шпигунство, екстремізм у мережі (який все частіше кваліфікується як кібертероризм), особиста образа або наклеп тощо.

Значною є й небезпека використання підроблених платіжних систем зі сторінкою 3-D Secure, яка полягає в тому, що ці кіберзлочини досить складно виявити, ці підроблені платіжні системи часто містять логотипи міжнародних платіжних систем Visa, MasterCard та не викликають підозри у покупців, які прагнуть швидко оформити покупку онлайн. При цьому для банку-емітента платіж його клієнта виглядає легально, і в разі вчинення кіберзлочину – клієнту дуже складно повернути свої гроші, які він відправив кібершахраям через нібито справжню сторінку платіжної системи 3-D Secure, підтвердивши транзакцію перевірним кодом із СМС.

В умовах війни кіберзлочинець стає бойовою одиницею, а його основний інструмент – кібератаки і злами. Крім того, під час воєнного стану кібератаки можливі не лише з боку ворога, який використовує кіберпростір для завдання шкоди обороноздатності України, а й з боку тих, хто вирішив скористатися ситуацією, коли правоохоронні органи перевантажені, та поживитися коштами наших громадян [1]. Протягом війни кіберзлочинність в Україні стабільно зростає.

Війна у кіберпросторі може завдати не меншої шкоди, аніж війна на полі бою. Розуміючи це, ще у перший місяць війни Верховна Рада України оптимізувала кримінальне та кримінально-процесуальне законодавство, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Зміни зосереджено у двох законах [1]: "Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам" № 2137-IX від 15.03.2022;

• "Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану" № 2149-IX від 24.03.2022.

Зокрема, метою закону № 2149-IX є посилення спроможностей та оптимізація національної системи кібербезпеки для протидії кіберзагрозам, впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності, забезпечення надійності та безпеки використання цифрових послуг.

Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу

державних інституцій, техніки, завдання іншої матеріальної шкоди. Під прицілом знаходяться також об'єкти критичної інфраструктури. Приміром,

23 березня 2022 р. ворог намагався здійснити кібератаку на державні установи України з використанням шкідливої програми Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття [1].

Хоча *зазвичай кіберзлочини мають корисливе спрямування*, їм властиве постійне збільшення розмірів завданих збитків. Ідеться про різні прояви фінансового шахрайства, зокрема фішинг, використання номерів чужих кредитних карток, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж фінансових установ, порушення авторських і суміжних прав, виготовлення й розповсюдження шкідливих програм, кібервимагання, поширення в мережі забороненого контенту [8, с. 5].

У науці і практиці міжнародного права відсутня єдність у визначенні та застосуванні поняття "кіберзлочинність". У науковій літературі для характеристики злочинів, які вчиняються у кіберпросторі, використовуються різні поняття: "кіберзлочинність", "комп'ютерна злочинність", "злочинність у сфері використання електронно-обчислювальних машин", "злочинність у сфері високих технологій", "злочинність у сфері інформаційних технологій", "злочини у сфері IT-технологій", "інформаційна злочинність", "hi-tech злочини" тощо [3, с. 158]. На окрему увагу заслуговує терміносполучення "злочини у сфері комп'ютерної інформації". Цей вислів зумовлений важливістю та значенням об'єкта посягання – комп'ютерної інформації [10, с. 51]. До таких відносять злочини, передбачені Розділом XVI КК України, а також ч. 3 ст. 190 КК (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки) та ст. 200 КК (використання підроблених електронних засобів доступу до банківських рахунків). У цьому аспекті деякі вчені уживають поняття "інформаційні злочини", розуміючи їх як суспільно небезпечні діяння, заборонені кримінальним законом під погрозою покарання, вчинені в галузі інформаційних правовідносин.

Складність у формулюванні цього поняття існує як внаслідок неможливості виділення єдиного об'єкта злочинного посягання, так і у зв'язку з множинністю предметів злочинного посягання з погляду їх кримінально-правового значення.

Водночас термін "кіберзлочинність" також не отримав загального універсального визначення й на конвенціональному рівні чи в інших міжнародних правових документах. Так, Конвенція Ради Європи "Про кіберзлочинність" не містить визначення кіберзлочинності. Однак слід зазначити, що термін "кіберзлочинність" є універсальним та найбільш вдалим для використання. Пояснюється це тим, що саме термін "кіберзлочинність" (cybercrime) законодавчо закріплений на міжнародному та вітчизняному рівнях. Це Конвенція Ради Європи "Про кіберзлочинність", Закон України "Про основні засади забезпечення кібербезпеки України".

Зазвичай кіберзлочин розглядається як протиправне суспільно небезпечне діяння, вчинене за допомогою інформаційно-комунікаційних технологій (ІКТ) проти прав і законних інтересів учасників кіберпростору (фізичних, юридичних осіб, держав), що охороняються нормами кримінального та міжнародного права [11, с. 93].

Можна надати й інші вдалі визначення цього поняття.

Під кіберзлочинністю розуміються кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [12, с. 46].

Кіберзлочинність може бути визначена і як сукупність злочинів, учинених у кіберпросторі за допомогою комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [13, с. 119].

Термін "кіберзлочин" визначено й Законом України "Про основні засади забезпечення кібербезпеки України". Цим законом кіберзлочин (комп'ютерний злочин) визначається як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У свою чергу, у Кримінальному кодексі України, який містить окремий розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку", використовується термін "комп'ютерний злочин".

Термін з префіксом "кібер" дає однозначну відповідь на обстановку вчинення конкретного злочинного явища – це кіберпростір як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій [10, с. 54].

На сьогодні у Кримінальному кодексі України поки що не визначено чіткого переліку статей, які слід відносити до кіберзлочинів. *Дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів.*

Кримінальна відповідальність за кіберзлочини передбачена різними розділами та статтями КК України. Передусім кримінально-правовий обсяг поняття "кіберзлочинність" складають злочини, передбачені статтями 361 ("Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку"), 361-1 ("Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут"), 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"), 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"), 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"), 363-1 ("Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).9

шляхом масового розповсюдження повідомлень електрозв'язку") КК України, що містяться у Розділі XVI "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Отже, основною, системоутворюючою групою кіберзлочинів є злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Також кримінальна відповідальність за кіберзлочини передбачена ч. 3 ст. 190 "Шахрайство", тобто за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки; ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення" КК України.

Про комп'ютерне обладнання, комп'ютерні програми та інші спеціальні пристрої як засоби вчинення злочинів зазначається у ст. 163 "Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер", ст. 176 "Порушення авторського права і суміжних прав" КК України.

Загалом у структурі кіберзлочинності в Україні переважає несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України).

Отже, згідно з класифікацією кримінальних злочинів, упроваджених КК України, поняття кіберзлочинності охоплює кримінальні правопорушення у сфері:

• використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем);

• обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

• господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж.

До кіберзлочинів за способами вчинення можна віднести такі типи злочинних посягань [14, с. 20]:

1. Неправомірне підключення до мережі Інтернет, а саме:

• неправомірне отримання та використання чужих даних для доступу до мережі Інтернет (логіну та паролю);

• неправомірне отримання й використання облікових власних даних на чужих електронних приладах чи з використанням чужої MAC та IP-адреси з метою неправомірного доступу до мережі Інтернет;

• неправомірне підключення до мережі оператора електронного зв'язку з метою ухилення від сплати послуг, отриманих в мережі Інтернет.

2. Створення, використання та розповсюдження мережевих шкідливих комп'ютерних програм.

3. Незаконне виготовлення, зберігання, розповсюдження, рекламування чи публічна демонстрація інформації, що заборонена до вільного обігу, за допомогою мережі Інтернет:

• незаконне виготовлення, зберігання, розповсюдження, рекламування та публічна демонстрація порнографічних матеріалів, вчинені з використанням мережі Інтернет;

• незаконне отримання та розголошення відомостей, які становлять комерційну, податкову чи банківську таємницю, вчинені з використанням мережі Інтернет;

• порушення таємниці переписки, телефонних розмов, поштових чи інших повідомлень, що здійснюється за допомогою мережі Інтернет;

• образа, нанесена шляхом розповсюдження неправдивих відомостей на інформаційних ресурсах у мережі Інтернет;

• збудження ненависті чи ворожнечі, а також приниження людської гідності, вчинені за допомогою мережі Інтернет.

4. Порушення авторських та суміжних прав, а також незаконне використання товарних знаків за допомогою мережі Інтернет.

5. Шахрайство, вчинене у сфері надання послуг у мережі Інтернеті:

• продаж неіснуючих товарів, фіктивних послуг та пропозиція фіктивної роботи, вчинені за допомогою мережі Інтернет;

• залучення коштів до удаваної благодійності;

• шахрайство в електронних платіжно-розрахункових системах мережі Інтернет;

• шахрайство в Інтернет-казино, букмекерських конторах, в розіграшах лотерей та на аукціонах;

• шахрайство, вчинене з використанням фіктивних шлюбних Інтернет-агенцій;

• створення фінансових пірамід з використанням мережі Інтернет.

6. Викрадення електронних реквізитів та продаж підроблених кредитних чи розрахункових карток.

7. Незаконне підприємництво в сфері надання послуг в мережі Інтернет;

8. Кібервимагання за допомогою мережі Інтернет.

9. Кібертероризм.

До кіберзлочинності додаються і деякі дії, спрямовані на підтримку умов для її існування і розвитку (використання електронної пошти для комунікації, створення сайтів, спрямованих на поширення кримінальної та протиправної ідеології, а також з метою обміну кримінальним досвідом і спеціальними знаннями). У всьому світі налічується десятки тисяч орієнтованих на злом і навчальних цим прийомам сайтів.

До кіберзлочинів належать кібершахрайства, які зловмисники вчиняють з метою:

1. *Крадіжки:*

• особистих даних користувачів (наприклад, для отримання кредитів, створення фейкових акаунтів);

• логінів та паролів доступу до сайтів (наприклад, для розсилки спаму, шантажування);

• реквізитів банківських платіжних карток (кардінг);
• змісту листування;
• фотографій та відеозаписів приватного характеру тощо.

2. *Незаконного заволодіння коштами користувача через:*

1) *фейкові вебсайти*:
• інтернет-магазини;
• поповнення рахунків мобільних телефонів;
• переказ грошей;
• участь у розіграші товарів;

2) *шахрайські оголошення про продаж товарів та послуг у мережі Інтернет* тощо.

Найчастіше для ошукування громадян кібершахраї використовують методи соціальної інженерії та інформаційні приводи. Також продовжується розсилка фішингових електронних листів, під час відкриття яких користувачем відбувається зараження його персонального пристрою шкідливим програмним забезпеченням.

З урахуванням мотивації злочинців кіберзлочини можна умовно поділити на такі категорії:

• *кібершахрайство з метою заволодіння коштами*;

• *кібершахрайство з метою заволодіння інформацією* (для власного користування або для подальшого продажу);

• *втручання в роботу інформаційних системи з метою одержання доступу до автоматизованих систем управління* (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам) тощо. Наприклад, злом баз даних та виведення з ладу комп'ютерних систем компаній і урядових організацій.

Серед найбільш уразливих до кіберзлочинів сфер суспільного життя належить фінансовий сектор економіки, а саме банки. Найбільш поширеними злочинами у банківській сфері є шахрайство з використанням платіжних карток та їх реквізитів і шахрайство з використанням дистанційного банківського обслуговування (система "Клієнт-Банк").

За інформацією Національного банку України, у банківській системі України розповсюдженими є такі види кіберзлочинів:

1) *банкоматне шахрайство*:

• *скімінг* – виготовлення, збут та встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї;

• *використання "білого пластику"* для "клонування" (підробки) платіжної картки та зняття готівки в банкоматах;

• *Transaction Reversal Fraud* – втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником;

• *Cash Trapping* – заклеювання диспенсеру для привласнення зловмисником готівки, яка була списана з карткового рахунку законного держателя картки;

2) *шахрайство в торгівельно-сервісних мережах*:

• *укладання фіктивних угод торговельного еквайрінгу* для обслуговування підроблених платіжних карток;

• *викрадення реквізитів платіжних карток*, зокрема із застосуванням технічних засобів їх "клонування";

• *здійснення операцій на суму нижче встановленого ліміту без проведення авторизації*;

• *використання втрачених/викрадених/підроблених платіжних карток*;

3) *шахрайство в мережі Інтернет*:

• *викрадення реквізитів платіжних карток*;

• *проведення операцій із використанням викрадених реквізитів платіжних карток*;

• *діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток* (створення фіктивних вебсайтів, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).

4) *шахрайство в системах дистанційного банківського обслуговування (ДБО)*:

• створення комп'ютерних вірусів та троянських програм для *прихованого перехоплення управління комп'ютером клієнта* зі встановленим програмним забезпеченням ДБО;

• відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті *несанкціонованих операцій у системах ДБО*;

• отримання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання у роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.

Загалом серед найпоширеніших різновидів кіберзлочинів в Україні виділяються кібершахрайство, крадіжка даних банківських карток, протиправний контент, поширення шкідливого програмного забезпечення та створення майданчиків для продажу викраденої інформації.

До найбільш розповсюджених видів кіберзлочинів на міжнародному рівні можна віднести:

I. *У сфері використання платіжних систем*:

1. *Скімінг (шимінг)* – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток.

2. *Кеш-трепінг* – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки.

3. *Кардінг* – незаконні фінансові операції з використанням платіжних карток або їх реквізитів, що не ініційовані або не підтверджені її володільцем.

4. Несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

II. *У сфері електронної комерції та господарської діяльності*:

1. *Фішинг* – виманювання у користувачів Інтернету їх логінів та паролів до "електронних гаманців", сервісів онлайн-аукціонів, переказування або обміну валюти тощо.

2. *Онлайн-шахрайство* – заволодіння коштами громадян через Інтернет-аукціони, Інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

III. *У сфері інтелектуальної власності*:

1. *Інтернет-піратство* – незаконне розповсюдження інтелектуальної власності в Інтернеті. Основні види Інтернет-піратств:

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).9

• аудіопіратство;
• відеопіратство;
• піратство літературних 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 та шкідливого програмного забезпечення.

3. *Протиправний контент* – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

4. *Рефайлінг* – незаконна підміна телефонного трафіку.

Фахівці поділяють осіб і організації, що здійснюють кібератаки, на декілька видів, відповідно до яких формуються види самих кіберзлочинів:

• *хакери* – особи, що мають високий рівень знань у галузі комп'ютерних технологій і проводять багато часу за комп'ютером у пошуках слабких місць комп'ютерних систем (для них притаманним є вчинення таких злочинів, як DoS-атаки, дефейс, розповсюдження шкідливих програм (вірусів), фішинг);

• *хактивісти*, діяльність яких є своєрідним синтезом соціальної активності, ставлячи за мету протест проти чого-небудь, та хакерства (використання Інтернет-технологій з метою спричинення шкоди комп'ютерним мережам та їх користувачам). Для них притаманне вчинення таких злочинів, як розповсюдження шкідливих програм (вірусів), особиста образа або наклеп;

• *власне кіберзлочинці*, діяльність яких спрямована на незаконне отримання прибутків (для них притаманне вчинення таких злочинів, як кардерство, фішинг, кібершахрайство тощо);

• *особи, що професійно займаються промисловим шпигунством у кіберпросторі*;

• *кібертерористи*, діяльність яких пов'язана з різними екстремістськими проявами в мережі. На сьогодні терористи досягли того рівня, за якого вони можуть використовувати Інтернет (як сам по собі, так і у поєднанні з фізичною атакою) як інструмент для спричинення реальної шкоди.

Отже, нині загальноприйнятне визначення кіберзлочину, загальновизнана класифікація кіберзлочинів, що може бути використана для розробки відповідних норм кримінального права, досі відсутні. Крім того, оскільки явище кіберзлочинності перебуває у постійному розвитку, надати повну та вичерпну класифікацію всіх можливих кіберзлочинів наразі неможливо. Водночас серед науковців та фахівців із кібербезпеки спостерігається досить широке та вичерпне розуміння його суті та способів учинення кіберзлочинів, що дає можливість розробляти та впроваджувати заходи протидії цьому суспільно небезпечному явищу.

DOI (Issue): https: //doi.org/10.36486/np.2022.3(57) Issue 3(57) 2022

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Єрема М.* Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 02.10.2022).

2. *Шиян Д.Г.* Актуальні питання забезпечення кібербезпеки України. *Актуальні проблеми кібербезпеки*: Всеукраїнська наукова конференція. 2019. Київ: Державний університет телекомунікацій. С. 42–44. URL: http://www.dut.edu.ua/uploads/p_1895_91824930.pdf (дата звернення: 02.10.2022).

3. *Веселова Л.Ю.* Адміністративно-правові основи кібербезпеки в умовах гібридної війни: автореф. дис. ... д-ра юрид. наук. Одеса, 2021. 35 с.

4. *Дем'янчук М.А.* Процесний підхід до визначення засобів захисту активів телекомунікаційного підприємства внаслідок виникнення кіберінцидентів. *Інтелект XXI*. 2020. № 1. С. 36–43. URL: http://www.intellect21.nuft.org.ua/journal/2020/2020_1/6.pdf (дата звернення: 03.10.2022).

5. *Кулешов М.В.* Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України. Інформація і право. 2019. № 2(29). С. 115–122. URL: http://ippi.org.ua/sites/default/files/15_10.pdf (дата звернення: 02.10.2022).

6. *Трофименко О., Прокоп Ю., Логінова Н., Задерейко О.* Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21. № 3. С. 150–157.

7. *Трофименко О.* Моніторинг стану кібербезпеки в Україні. *Правове життя сучасної України*: матер. Міжнар. наук.-практ. конф., 17 травня 2019 р. Одеса: Видавничий дім "Гельветика", 2019. Т. 1. С. 642–646.

8. *Черней В.В.* Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні. *Науковий вісник Національної академії внутрішніх справ*. 2014. № 3. С. 3–15.

9. *Чинник П.А.* Світовий досвід боротьби з кіберзлочинністю. *Протидія кіберзлочинності та торгівлі людьми*: зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків), МВС України, Харків. нац. ун-т внутр. справ; Координатор проєктів ОБСЄ в Україні. Харків: ХНУВС, 2020. С. 221–223.

10. *Самойленко О.А.* Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія; за заг. ред. А.Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

11. *Яцишин М.Ю.* Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. № 5. С. 92–99.

12. *Білобров Т.В.* Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дис. ... канд. юрид. наук. Київ, 2020. 209 с.

13. *Шемчук В.В.* Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Юридичні науки. 2018. Т. 29. № 6. С. 119–124.

14. *Довженко О.Ю.* Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

REFERENCES

1. *Yerema M.* Borotba z kiberzlochynnistyu v umovakh dii voiennoho stanu. "Fighting cybercrime under martial law: Law 2149-IX". URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix. (Date of Application: 02.10.2022) [In Ukrainian].

2. *Shyian D.H.* (2019). Aktualni pytannia zabezpechennia kiberbezpeky Ukrainy. "Current issues of ensuring cyber security of Ukraine". Actual problems of cyber security: All-Ukrainian scientific conference. Kyiv: State University of Telecommunications. P. 42–44. URL: http://www.dut.edu.ua/uploads/p_1895_91824930.pdf (Date of Application: 02.10.2022) [In Ukrainian].

3. *Veselova L.Yu.* (2021). Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoi viiny. "Administrative and legal foundations of cyber security in conditions of hybrid warfare". Extended abstract of Doctor's thesis. Odesa. 35 p. [In Ukrainian].

4. *Demianchuk M.A.* (2020). Protsesnyi pidkhid do vyznachennia zasobiv zakhystu aktyviv telekomunikatsiinoho pidpryiemstva vnaslidok vynyknennia kiberintsydentiv. "A process approach to determining the means of protecting the assets of a telecommunications enterprise due to the occurrence

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).9

of cyber incidents". Intelligence XXI, 1, 36–43. URL: http://www.intellect21.nuft.org.ua/journal/2020/2020_1/6.pdf (Date of Application: 03.10.2022) [In Ukrainian].

5. *Kuleshov M.V.* (2019). Sutnist ta zmist rozsliduvannia kiberintsydentiv ta kiberatak pidrozdilamy SB Ukrainy. "The essence and content of the investigation of cyberincidents and cyberattack units of the Security Service of Ukraine". Information and law. No 2(29). P. 115–122. URL: http://ippi.org.ua/sites/default/files/15_10.pdf (Date of Application: 02.10.2022) [In Ukrainian].

6. *Trofymenko O., Prokop Yu., Lohinova N., Zadereiko O.* (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu. "Cybersecurity of Ukraine: analysis of the current state". Protection of information. Vol. 21. No 3. P. 150–157. [In Ukrainian].

7. *Trofymenko O.* (2019). Monitorynh stanu kiberbezpeky v Ukraini. Pravove zhyttia suchasnoi Ukrainy. "Monitoring of cybersecurity in Ukraine". Proceedings from MIIM '19: International Scientific and Practical Conference "Legal life of modern Ukraine". Odesa: Helvetyka Publishing House. Vol. 1, P. 642–646. [In Ukrainian].

8. *Cherniei V.V.* (2014). Rol vidomchoi osvity ta nauky v zabezpechenni protydii kiberzlochynnosti v Ukraini. "The role of departmental education and science in ensuring the counteraction of cybercrime in Ukraine". Scientific Bulletin of the National Academy of Internal Affairs. No 3. P. 3–15. [In Ukrainian].

9. *Chynnyk P.A.* (2020). Svitovyi dosvid borotby z kiberzlochynnistiu. "World experience in combating cybercrime". Proceedings from MIIM '20: International Scientific and Practical Conference "Counteracting cybercrime and trafficking in human beings". (pp. 221–223). Kharkiv: KhNUVS. [In Ukrainian].

10. *Samoilenko O.A.* (2020). Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori: monohrafiia. "Fundamentals of the Crime Investigation Methodology committed in cyberspace" monograph; in general ed. A.F. Volobueva. Odesa: TES. 372 p. [In Ukrainian].

11. *Yatsyshyn M.Yu.* (2018). Kryminalizatsiia kiberzlochyniv u mizhnarodnomu pravi: porivnialnyi analiz. "Criminalization of cybercrime in international law: comparative analysis". Law forum. No 5. P. 92–99. [In Ukrainian].

12. *Bilobrov T.V.* (2020). Administratyvno-pravovyi status Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy. "Administrative and legal status of the Cyber Police Department of the National Police of Ukraine". Candidate's thesis. Kyiv. 209 p. [In Ukrainian].

13. *Shemchuk V.V.* (2018). Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini. "Cybercrime as an obstacle to the development of information society in Ukraine". Academic notes of V.I. Vernadskyi TNU. Series: Legal Sciences. Vol. 29. No 6. P. 119–124. [In Ukrainian].

14. *Dovzhenko O.Yu.* (2019). Klasyfikatsiia kiberzlochyniv u kryminalistytsi. "Classification of cybercrime in forensics". South Ukrainian legal journal. No 1. P. 19–22. [In Ukrainian].

UDC 343.973

Blyzniuk Ihor,
Candidate of Juridical Sciences, Senior Research Officer, Chief Scientist,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-3882-5790

CHARACTERISTICS OF TYPICAL METHODS OF COMMITTING CIBERCRIME UNDER MARTIAL LAW

This article presents a description of typical ways of committing cybercrime. Author reveals the peculiarities of the causal complex of cybercrime. Along with this, the article details the reasons why cyber threats are evolving at an accelerated pace, and cybercrimes are becoming more advanced, better organized and transnational.

At the same time, in the article, the author outlines the types of cybercrimes that pose the greatest threat today, i.e., under martial law. Changes in the criminal and

criminal procedural legislation that occurred during the war, with the improvement of the grounds and procedural mechanisms for bringing cybercriminals to justice, were not left without consideration.

The author pays special attention to the characteristics of the crimes provided for in Articles 361 ("Unauthorized interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks"), 361-1 ("Creation for the purpose of illegal use, distribution or sale of malicious software or hardware, as well as their distribution or sale"), 361-2 ("Unauthorized sale or distribution of information with restricted access stored in electronic computers (computers), automated systems, computer networks or on carriers of such information") , 362 ("Unauthorized actions with information that is processed in electronic computers (computers), automated systems, computer networks or that is stored on the media of such information, committed by a person who has the right to access it", 363 ("Violation of the rules for the operation of electronic - computers (computers), automated systems, computer networks or telecommunication networks or the procedure or rules for protecting the information processed in them"), 363-1 ("Obstruction of the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks by mass dissemination of messages Telecommunications") of the Criminal Code of Ukraine contained in Section XVI "Criminal offenses in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks".

According to the classification of criminal offenses introduced by the Criminal Code of Ukraine, the author defines criminal offenses covering the concept of cybercrime. In conclusion, the author gives the most common types of cybercrime at the international level.

Keywords: cybercrime, cyberthreats, martial law, criminal law and criminal procedure, malware, cyberfraud, phishing, cyberterrorism, cyberespionage, DDoS or DoS attacks, deface, skimming, remote banking.

Отримано 06.10.2022