УДК 343
DOI https://doi.org/10.32841/2307-1745.2022.57.18

Думчиков М. О.,
старший викладач кафедри кримінально-правових дисциплін та судочинства
Навчально-наукового інституту права
Сумського державного університету

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ В СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ: РЕТРОСПЕКТИВНИЙ АНАЛІЗ

Анотація. Кримінальні правопорушення в сфері комп'ютерної інформації, є архіважливою проблемою сьогодення. Враховуючи специфічні ознаки, кримінальних правопорушень в сфері комп'ютерної інформації, і динамічний розвиток такої категорії, постають виклики перед суспільством та міжнародною спільнотою в цілому з кримінально правової охорони кіберпростору. Актуальність теми додатково зумовлена, проблемами доктринального характеру науки кримінального права з приводу визначення понятійних категорій, щорічне збільшення кримінальних проваджень з приводу вчинення кримінальних правопорушень в сфері комп'ютерної інформації.

Метою статті є дослідження феномену кримінальних правопорушень у сфері комп'ютерної інформації, визначення поняття кримінальних правопорушень в сфері комп'ютерної інформації та видів зазначених злочинів, надати загальну характеристику кримінальним правопорушенням в сфері використання комп'ютерної інформації, а також визначити ознаки які притаманні зазначеному виду кримінальних правопорушень.

Статтю присвячено дослідженню доктринальних підходів до визначення поняття кримінального правопорушення в сфері комп'ютерної інформації та аналіз основних видів кримінальних правопорушень в сфері комп'ютерної інформації.

В статті розглянуто доктринальні визначення дефініції поняття кримінального правопорушення в сфері комп'ютерної інформації. Визначено, що кримінальним правопорушенням в сфері комп'ютерної інформації є умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист.

Проаналізовано такі види кримінальних правопорушень в сфері комп'ютерної інформації як: кримінальні правопорушення у сфері використання платіжних систем, шахрайства сфері комп'ютерної інформації, кримінальні правопорушення у сфері інтелектуальної власності, кримінальні правопорушення у сфері інформаційної безпеки.

Ключові слова: кримінальне правопорушення в сфері комп'ютерної інформації, кіберпростір, кримінальні правопорушення вчинені у кіберпросторі, кіберзлочини.

Актуальність. Кримінальні правопорушення в сфері комп'ютерної інформації є дуже актуальною проблемою сучасного суспільства. Про його актуальність свідчать світові новини, статистика кримінальних правопорушень, проблемні питання кримінальної юриспруденції, проблеми кримінального процесу. Все тому, що кримінальні правопорушення в сфері комп'ютерної інформації як явище є дуже специфічною категорією, яка постійно розвивається паралельно з технічним прогресом.

Метою статті є дослідження феномену кримінальних правопорушень у сфері комп'ютерної інформації, визначення поняття кримінальних правопорушень в сфері комп'ютерної інформації та видів зазначених злочинів, надати загальну характеристику кримінальним правопорушенням в сфері використання комп'ютерної інформації, а також визначити ознаки які притаманні зазначеному виду кримінальних правопорушень.

Об'єктом дослідження є суспільні відносини, щ виникають у сфері використання комп'ютерної інформації а також використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в рамках кіберпростору.

Предметом дослідження є різні види кримінальних правопорушень у сфері комп'ютерної інформації.

Методологічною базою для написання даної статті було використано різні методи наукового пізнання. Зокрема було використано методи порівняння, аналогії та метод узагальнення.

В наш час кіберзлочинність вийшла з-під контролю правоохоронних органів однієї держави та стала значною міждержавною і транснаціональною проблемою.

Активне використання комп'ютерних технологій практично у всіх сферах суспільного життя, стало невід'ємною частиною сучасності. Можна наголосити, що XXI століття – є століттям диджиталізації, цифрових та інформаційних технологій.

Ще декілька десятиліть назад про кримінальні правопорушення в сфері комп'ютерної інформації було дуже мало згадок, однак за короткий проміжок часу, дані кримінальні правопорушення почали нести не лише окрему загрозу для осіб чи суспільства, а й для держав в цілому. Більш того проблема розвитку злочинності в сфері комп'ютерної інформації стоїть найбільш гостро, оскільки наслідки несвоєчасного реагування на таку загрозу набагато небезпечніші ніж в більшості інших кримінальних правопорушеннях.

Наразі кримінальні правопорушення в сфері комп'ютерної інформації охоплюють фактично всі сфери життя суспільства, починаючи від банківської сфери, закінчуючи національною безпекою держави.

Аналізуючи правовий аспект злочинів, які вчиняються за допомогою електронно обчислювальних машин, варто зауважити, що поняття злочину в сфері комп'ютерної інформації та злочину який скоється за допомогою комп'ютерних технологій не є ідентичними поняттями. На нашу думку кримінальні правопорушення у сфері комп'ютерної інформації варто розглядати як один з підвидів злочинів з використанням комп'ютерних технологій.

Суспільна небезпека злочинів в сфері комп'ютерної інформації полягає у тому, що неправомірний доступ до комп'ютерної інформації може шкодити діяльності різноманітних систем

державної оборони, банківського сектору, систем муніципальної діяльності. Так само різного типу дії щодо спотворення достовірності інформації можуть привести як до проблем загальнонаціонального характеру так і заподіяти шкоду правам та інтересам окремої особи.

В перше поняття «злочин в сфері комп'ютерної інформації» було використане в 60-х роках 20 століття, саме тоді були виявлені перші злочини з використанням електронно обчислювальних машин.

Сьогодні немає єдиного визначення, що слід розуміти під злочинами в сфері комп'ютерної інформації. Зокрема Боглов В.М. під злочинами в сфері комп'ютерної інформації розуміє передбачене кримінальним законодавством протиправне, винне порушення чужих прав та інтересів щодо автоматизованих систем обробки даних, повноцінного впливу, що підлягають правовій охороні майнових прав та інтересів, громадської та державної безпеки [1, с. 156].

Миколенко О.М. під злочинами в сфері комп'ютерної інформації розуміє заборонені кримінальним законом суспільно – небезпечні умисні, винні та противоправні діяння, які спрямовані на порушення недоторканості комп'ютерної інформації, яка охороняється законом та її матеріальних носіїв, що завдають шкоду правам та інтересам окремих осіб та державної та громадської безпеки [2, с. 104].

Погорецький М.В. злочини в сфері комп'ютерної інформації визначає як навмисні суспільно небезпечні діяння, які заподіюють шкоду або створюють загрозу заподіяння шкоди суспільним відносинам, що регулює безпечне виробництво, зберігання, використання або поширення інформації або інформаційних ресурсів [3, с. 90].

Голубєв В.О. під даними злочинами розуміє передбачені законом про кримінальну відповідальність винне, суспільно небезпечне діяння скоєне задля порушення цілісності, конфіденційності, достовірності та доступності охоронюваної законом цифрової інформації» [4, с. 54].

Амелін О. М. вважає, що в юридичному сенсі злочини в сфері комп'ютерної інформації як особлива група злочинів не існують, але при цьому підкреслює, що багато традиційних видів злочинів удосконалилися в результаті залучення коштів обчислювальної техніки, і, отже, можна говорити лише про комп'ютерні аспекти злочинів без виділення їх в окрему групу [5, с. 6].

Юртаєва К. В. під поняттям злочин в сфері комп'ютерної інформації розуміє передбачені кримінальним законом винні суспільно небезпечні діяння, спрямовані на порушення недоторканності охоронюваної законом електронної інформації та її матеріальних носіїв, що здійснюються у процесі створення, використання та розповсюдження електронної інформації, а також спрямовані на порушення роботи ЕОМ, системи ЕОМ або їх мережі, що завдають шкоди законним інтересам власників або власників, життя здоров'ю, правам та свободам людини та громадянина, національній безпеці [6, с. 336].

Пропонуємо під злочинами в сфері комп'ютерної інформації розуміти умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист.

Злочини у сфері використання платіжних систем

В кримінальному законодавстві України, як і в науковій літературі, немає поняття злочинів у сфері використання платіжних систем, більшість науковців розглядають такі злочини як злочини в фінансовій та банківських сферах, або злочини в сфері забезпечення фінансової та банківської інформації. Злочини в сфері комп'ютерної інформації в сфері використання платіжних систем є одним з видів кіберзлочинів. В Україні цей вид шахрайства поступово набуває масового характеру. Зокрема, одним з таких злочинів є скімінг [7].

Скімінг – крадіжка даних карти за допомогою спеціального пристрою – скімера [8].

Загалом варто розділяти скімінг на 2 види:

1. Фізичний скімінг. Зловмисники копіюють всю інформацію з магнітної смуги картки (ім'я власника, номер картки, термін закінчення терміну її дії, CVV- та CVC-код), дізнатися про ПІН-код можна за допомогою міні-камери або накладок на клавіатуру, встановлених на банкоматах. Стати жертвою скімінгу можна не лише знімаючи готівку, а й оплачуючи покупки у торгових точках. Для копіювання даних офіціанти, касири, службовці готелів використовують переносні скімери або пристрої, прикріплені до терміналу.

2. Програмний скімінг. Полягає у встановленні зловмисниками на банкомат певного шкідливого програмного забезпечення яке буде здійснювати копіювання магнітної стрічки картки, ссв коду та дати дії картки, та подальше надіслання таких даних на сервери зловмисників.

ПриватБанк України, наголошує, що наразі використовуються так звані антискімінгові накладки, які значно знижують ризик встановлення скімерів на банкомати. Крім того спеціалісти відділу кібербезпеки приват банку рекомендують використовувати чіпові картки, які мають значно вищий рівень захисту, оскільки інформація яка міститься у чіпі має захист криптографічного характеру який унеможливлює його компрометування [9].

Ще одним з підвидів злочинів у сфері платіжних систем є кардинг. Кардинг це незаконні фінансові операції з використанням платіжних карток та електронних платіжних систем, які не були підтвердженні або ініційовані володільцем карти або електронного гаманця. Реквізити платіжних карток беруть як правило з різноманітних сервісів даркнету. Вартість електронного гаманця чи пластикової картки варіюється від 2 до 300 доларів, це залежить від країни володільця карти чи електронного гаманця, кількості грошових коштів на них, типу картки (бизнес, корпоративна, золота), банку який випустив картку.

Зловмисник маючи картку чи електронний гаманець може використати кошти які на них знаходяться, на товари електронної комерції в інтернеті, поповнити номер телефону з подальшим переведенням в готівкову форму, купувати техніку в онлайн магазинах з подальшим їх продажом. Найпопулярнішим способом використання таких карт є покупка товарів на різних маркетплейсах у самого себе, такий спосіб на відміну від інших дає можливість використати весь баланс картки, по – перше без посередників, а по – друге без комісії з подальшим перепродажем куплених товарів.

Схожим с кардингом виступає ще один злочин в сфері платіжних систем, Enroll можна назвати певним предикатним злочином щодо деяких направлень у кардингу, а саме Enroll це процедура за допомогою якої зловмисник отримує, або створює новий доступ до онлайн банкінгу жертви. Після отримання доступу до онлайн банкікгу жертви, зловмисник суттєво спрощує процедуру підтвердження транзакції (навіть дуже підозрілої) оскільки підтвердження можна зробити в самому онлайн банкінгу.

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

Для здійснення такого злочинного дійства злочинці закривають отвір для видачі грошей в банкоматі спеціальною накладкою (планкою) з липкою стрічкою з іншої сторони. Таким чином, при проведенні громадянами операцій по зняттю готівки здійснюється захват купюр – грош прилипають до скотчу, що перешкоджає їх видачі законому власнику карти. В більшості випадків користувач банкомата, не отримавши гроші грошей, вирішує, що в його роботі виник збій чи закінчилася готівка і йде не підозрюючи про факт шахрайства. Після цього, шахраї підходять і забирають готівку[10].

Шахрайства сфері комп'ютерної інформації

Фішинг є інноваційним видом шахрайства в мережі інтернет, метою якого виступає можливість заволодіти персональними даними, банківськими реквізитами, реквізитами електронних платіжних систем та крипто гаманців та дані від електронних кабінетів інтернет магазинів, з подальшим продажом таких даних або з використанням таких даних на власний розсуд.

Варто зазначити, що фішингові веб сайти дуже складно розпізнати на їх оригінальність. Фішингові веб-сайти повністю копіюють оригінальні веб-сайти, відмінність становитиме лише адресу доменного імені, який не привертає увагу непідготовленого громадянина з причини незначної відмінності у буквах чи цифрах. Як приклад можна згадати приклад крипто веб-сайту MyEtherWallet.com, кіберзлочиниці за допомогою фішингового сайту викрали близько 700000 доларів за декілька днів. Зловмисники скопіювали оригінал веб сайту та присвоїли йому доменне ім'я myetherwallet.com і таким способом викрадали приватні ключі які відповідають за доступ до адресів ETH і ETC.

Суспільно небезпечний характер фішингу обумовлений передусім прямою фінансовою шкодою та породженням кризовою довіри до фінансових операцій які здійснюються в інтернеті. Через витрати обумовлені фішинговими атаками, багато з фінансових та банківських інститутів, відмовляються від оплати та покладають усю відповідальність на клієнта. У широкому сенсі фішинг підриває маркетинговий імідж компанії або фінансової установи і сильно впливають на її загальний імідж, завдає сильного удару по електронній комерції [11].

Пересічному інтернет-користувачу розпізнати фішинг-атаку буває досить складно через його довірливість і погану обізнаність з методами і тактиками фішингу, які постійно оновлюються (спам дедалі частіше поєднується зі зловмисним програмним забезпеченням).

На нашу думку можна виділити 3 основні види фішингу:

1. Масовий фішинг. Зазначений вид фішингу передбачає використання зловмисниками спам емейл листів, веб-сайтів, підроблених рекламних банерах та пуш повідомлень, які адресовані великій кількості людей. Як правило жертвами такого виду фішингу стають клієнти банків і тд. Основною ознакою такого виду фішинга є те, що він не передбачає виявлення заздалегідь конкретних жертв, оскільки адресати фішингової атаки беруться з випадкових отриманих баз даних.

2. Цільовий фішинг. Найбільш небезпечним видом фішингу є саме цільовий фішинг який спрямований на цільову аудиторію, стосовно якої спеціально збирається інформація аби зробити адресоване їй послання більш переконливим. Для даного виду фішинга характерні наступні етапи: планування, підготовка, атака, збір, шахрайство, стадія завершення. На стадії планування зловмисник проводить певну розвідку щодо жертви або групи жертв, підбирає вразливі місця та робить їх аналіз. Стадія підготовки характеризується складанням фішингового листа, або створення фішингово веб – сайту та розробка засобів атаки. На стадії атаки зловмисник відправляє фішинговий лист або шкідливе програмне забезпечення. Наступною стадією є збір інформації шкідливим програмним забезпеченням та наступний аналіз зібраної інформації. Стадія шахрайства характеризується продажом зібраної інформації, шантажем. На кінцевій стадії зловмисник ліквідує докази та замітає сліди.

3. Корпоративний фішинг. Характеризується у створенні веб-сайтів, які ззовні повністю є копією оригіналу однак мають іншу адресу домену. Такі веб-сайти вузько визначають клас жертв фішерів. Основною метою фішерів є те щоб жертва сприйняла підроблений веб-сайт як легальний і надала інформацію про особисті данні. Мета шахрая полягає або в отриманні доступу до захищеного сайту, або в маскуванні його справжньої особи. При цьому шахрай може викрасти адресу жертви, фальсифікуючи інформацію про маршрутизацію повідомлення, щоб здавалося, що воно прийшло з акаунта жертви замість його власного [12].

Шахрайство в сфері проведення інтернет аукціонів. З-поміж усіх видів інтернет шахрайств у сфері комп'ютерної інформації, інтернет аукціони стоять на перших місцях. Переважно на інтернет аукціонах виставляють міфічні лоти, коли за картинкою та описом на екрані монітора стоїть неіснуюча річ. За допомогою інтернет аукціонів довірливі покупці готові витрачати тисячі доларів за фіктивний лот. Процедура шахрайських дій полягає у тому, що товар виставляється за нижчою ціною від побібного роду товарів, але не настільки щоб жертва що – небуть запідозрила.

Використання фіктивних суб'єктів електронної комерції. Досить поширений вид шахрайства, представлений одно сторінковими веб – сайтами з унікальною ціновою пропозицією на будь-якій товар. Як правило, фіктивні Інтернет-магазини працюють за частковою або стовідсотковою передоплаті. Відповідно, жертва, здійснивши переказ коштів, не отримує необхідного товару. Далі сайт блокується, і згодом «переїжджа» на інший хостинг або змінює доменне ім'я та продовжує свою протиправну діяльність. Такий сайт може бути наповнений великим кількістю фальшивих відгуків з метою створення образу доброчесного Інтернет-магазину та введення в оману потенційних жертв. Такий вид шахрайства є одним із самих простих методів здійснення злочинної діяльності в мережі Інтернет і завдає великої шкоди щодо фінансової спроможності слабо захищених та необізнаних громадян з урахуванням низького рівня їхньої інформаційної грамотності [13].

Злочини у сфері інтелектуальної власності. Інтернет піратство. В законі США про авторське право надається визначення інтернет піратство, а саме – використання інтернету для незаконного копіювання і / або поширення програмного забезпечення [14].Основною метою інтернет піратства є одержання прибутку від такої діяльності. У мережі інтернет інтернет пірати можуть отримувати прибуток від надання платного доступу до матеріалів які знаходяться в закритому доступі або є платними за ціною значно нижчою від ціни яку пропонує автор. Також інтернет пірати можуть надавати доступ до авторських матеріалів на безкоштовній основі, а прибуток отримувати за

рахунок реклами на ресурсі де розміщені піратські матеріали, або взагалі інтегрувати рекламу безпосередньо в піратські матеріали. В найгіршому випадку піратські файли можуть містити вірусні програми, як результат отримання персональних даних які зловмисник може використовувати на свій розсуд. На нашу думку інтернет піратство це використання інтернет простору для незаконного копіювання, злому та розповсюдження видеоконтенту, аудіоконтенту, літературних творів, програмного забезпечення та інших видів цифрової продукції, яка розміщена в інтернет мережі для подальшого розповсюдження як на платній так і безоплатній основі.

Одним з видів злочинів у сфері інтелектуальної власності є кардшарінг. Кардшарінгом називають надання незаконного доступу до перегляду супутникового та кабельного TV.

Злочини у сфері інформаційної безпеки

Для злочинів в сфері інформаційної безпеки характерними є наступні ознаки: неоднорідність об'єкта посягання(на практиці маємо, що об'єктом злочинів у сфері інформаційної безпеки є не тільки комп'ютерна інформація, а й національна безпека держави, громадська безпека, економічна сфера), використання комп'ютера в якості як предмета так і способу вчинення злочину, використання комп'ютерної інформації в якості як засобу вчинення злочину так і в якості об'єкта злочину.

Створення, розповсюдження та продаж шкідливого програмного забезпечення як правило виступають у сукупності такого виду злочину в сфері комп'ютерної інформації. Йдеться перш за все свідоме створення та застосування такого програмного забезпечення за допомогою якого допускається: блокування, знищення, модифікація комп'ютерної інформації, копіювання даних які охороняються.

Прикладами подібного роду проєктів можуть виступати, віруси локери, віруси трояни, віруси кліпери, віруси стилери, віруси кейлогери. Віруси локери або як їх ще називають мальваре це віруси які при потраплянні на комп'ютер або телефон повністю блокують систему, натомість на екрані девайсу жертви вискакує повідомлення про необхідність переведення певною суми грошових коштів, як правило у криптовалюті для зняття блокування системи девайсу. Однак навіть після оплати зловмиснику грошових коштів і отримання паролю для розблокування, система девайсу жертви повністю само знищується.

Віруси кліпери – це вид вірусів, який підмінює картковий або електронний рахунок жертви, на рахунок зловмисника і при переведенні грошових коштів жертва фактично переводить гроші зловмиснику.

Віруси стілери – це такий вид вірусів, які крадуть інформацію з вашого браузера і роблять на сервері зловмисника відбиток браузера жертви. З такими даними зловмисник може з легкістю використовувати весь спектр інформації яка міститься у браузері жертви, починаючи від дій у соціальних мережах закінчуючи купівлею товарів за рахунок жертви.

Підроблення комп'ютерної інформації. Створення, зміна, знищення, приховування комп'ютерних даних чи комп'ютерних програм або інше втручання в хід обробки даних різними способами, або створення таких умов, які згідно з національним законодавством будуть становити таке правопорушення, як підробка в традиційному розумінні цього значення.

Пошкодження комп'ютерних даних чи даних комп'ютерних програм. Несанкціоноване знищення, пошкодження, погіршення комп'ютерних даних чи комп'ютерних програм.

Зміна комп'ютерних даних чи даних комп'ютерних програм Несанкціонована зміна комп'ютерних даних або комп'ютерних програм.

Комп'ютерне шпигунство. Придбання з використанням протиправних засобів або шляхом несанкціонованого розкриття, передавання або використання торгівельної або комерційної таємниці з метою заподіяння економічного збитку особі, яка має право на таємницю, або отримання незаконної економічної переваги для себе або третьої особи.

Протиправне використання захищеної інформації.

Використання захищеної законом комп'ютерної програми без дозволу або її незаконне відтворення з метою отримання економічної вигоди для себе або третьої особи, або з наміром заподіяти шкоду законному власнику програми [15].

Кримінальні правопорушення в сфері комп'ютерної інформації, на сьогодні виступають одним з найбільш небезпечних видів кримінальних правопорушень у кіберпросторі, як результат заподіяння фінансової шкоди як, окремим суб'єктам кіберпростору, так і державам в цілому, тим самим становлять загрозу міжнародній та національній безпеці у кіберпросторі.

Література:

1. Болгов В. М. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. К. : Національна академія прокуратури України, 2015. 202 с.
2. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). 2016. 233 с.
3. Погорецький М. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.
4. Голубєв В.О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.
5. Амелін О. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–10
6. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права*. 2009. № 2. С. 434–441. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2009_2_69.pdf (дата звернення: 24.07.2022).
7. Vakulyk, O. O., Andriichenko, N. S., Reznik, O. M., Volik, V. V., Yanishevska, K. D. International aspect of a legal regulation in the field of financial crime counteraction by the example of special services of Ukraine and the CIS countries. *Journal of Legal, Ethical and Regulatory Issues*. 2019. 22(1). URL: http://repository.mdu.in.ua/jspui/handle/123456789/1013
8. Словник банківських термінів. URL: https://www.banki.ru/wikibank/skimming/
9. Офіційний сайт Приват Банку. URL: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva#:~:text=3.,4
10. Юрчук А.М. VII регіональна міжвузівська студентська науково-практична конференція Проблеми українського суспільства: кіберзлочинність. Види кіберзлочинності. URL: http://prog-rdak.16mb.com/wp-content/uploads/2017/04/kiberzlochunu.pdf
11. Klochko, A. N., Kulish, A. N., Reznik, O. N. The social basis of criminal law protection of banking in Ukraine. *Russian journal of criminology*. 10(4). Pp. 790–800.
12. Rusch, J. The compleat cyber-angler: A guide to phishing. *Computer Fraud & Security*. (1):4-6. doi: 10.1016/S1361-3723(05)00145-4

13. Lyubimenko O.O. Fraud on the Internet as a threat to the economic security of the state. URL: https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kak-ugroza-ekonomicheskoy-bezopasnosti-gosudarstva/viewer
14. Copyright Law of the United States. (Title 17). URL: https://www.copyright.gov/title17/
15. Болгов В. М., Гадіон О. З. Організаційно-правовий захист від кримінальних правоохоронців, які відповідають за інформаційні технології: наука і практика. Київ : Національна академія прокуратури України. URL: http://ir.nusta.edu.ua/jspui/handle/123456789/2337

Dumchykov M. Criminal offenses in the field of computer information: a retrospective analysis

Summary. Criminal offenses in the field of computer information are an archival problem today. Given the specific features of criminal offenses in the field of computer information, and the dynamic development of this category, there are challenges to society and the international community as a whole in terms of criminal law protection of cyberspace. The topicality of the topic is additionally determined by the problems of the doctrinal nature of the science of criminal law regarding the definition of conceptual categories, the annual increase in criminal proceedings regarding the commission of criminal offenses in the field of computer information.

The purpose of the article is to study the phenomenon of criminal offenses in the field of computer information, to define the concept of criminal offenses in the field of computer information and the types of these crimes, to provide a general description of criminal offenses in the field of use of computer information, as well as to determine the characteristics of the specified type criminal offenses.

The article is devoted to the study of doctrinal approaches to the definition of the concept of a criminal offense in the field of computer information and an analysis of the main types of criminal offenses in the field of computer information.

The article examines the doctrinal definitions of the definition of a criminal offense in the field of computer information. It was determined that a criminal offense in the field of computer information is intentional socially dangerous, illegal, culpable acts that encroach and cause damage to social relations that regulate the order of storage, distribution, use of information and their protection.

Such types of criminal offenses in the field of computer information were analyzed as: criminal offenses in the field of using payment systems, fraud in the field of computer information, criminal offenses in the field of intellectual property, criminal offenses in the field of information security.

Key words: criminal offense in the field of computer information, cyberspace, criminal offenses committed in cyberspace, cybercrimes.