МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА ГАЛУЗЕВОГО ПРАВА

МЕТОДИКА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконав: студент 2 курсу 13-283-Мз групи
Спеціальності 262 Правоохоронна діяльність
Освітньо-професійної програми
«Правоохоронна діяльність»

Гнип Сергій Геннадійович
Керівник: к.ю.н., доц. Проценко М.В.
Рецензент: к.ю.н., доц. Петренко Н.О.

Херсон – 2020

ЗМІСТ

ВСТУП

Актуальність теми. Ефективність боротьби зі злочинністю не в останню чергу залежить від досконалості прийомів та способів, які використовують правоохоронці під час розкриття та розслідування злочинів.

Комп’ютерні становлять велику суспільну небезпеку. Вдосконалення злочинцями прийомів та способів їх вчинення є серйозною перешкодою на шляху розбудови в Україні демократичної та правової держави.

Криміналістична методика покликана розробити та надати практичним працівникам правоохоронних органів науково розроблені методичні рекомендації із розслідування зазначених злочинів.

Питання, пов’язані з криміналістичною методикою, раніше були предметом досліджень таких вчених, як Аверьянова Т.В., Біленчук П.Д., Гуцалюк М.В., Губанов В.А., Іщенко А.В., Колесник В.А., Крилов В.В., Калюжний Р.А., Камлик М.І., Котляревський О.І., Міщенко В.Б., Оборський В.І., та ін. Зазначені вчені внесли вагомий вклад у розвиток як вітчизняної, так і зарубіжної науки. Однак, низка проблемних питань досліджена лише фрагментарно, а інші до теперішнього часу є дискусійними. До них відносяться, зокрема, проблемні питання, пов’язані з методикою розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Мета і задачі дослідження. Метою дослідження є аналіз методики розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Для досягнення даної мети були сформовані такі **завдання:**

– дослідити способи вчинення і приховування комп’ютерних злочинів;

– проаналізувати предмет злочинного посягання комп’ютерних злочинів;

– проаналізувати особливості початкового етапу розслідування комп’ютерних злочинів;

– проаналізувати проведення окремих слідчих (розшукових) дій під час розслідування комп’ютерних злочинів

Об’єктом дослідження є суспільні відносини, пов’язані із розслідуванням кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Предметом дослідження є результати наукових досліджень, правові норми, за допомогою яких визначається розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методи дослідження обирались, із урахуванням мети роботи та завдань, які були поставлені автором для дослідження. Також при обранні методів дослідження автором були враховані об’єкт та предмет дослідження. Метод ідеалістичної діалектики, який є фундаментальним (філософським) методом наукового пізнання, покладено в основу цього дослідження.

Крім методу ідеалістичної діалектики під час проведення дослідження При проведенні дослідження використовувались загально наукові методи: формально-юридичний, статистичний, порівняльно-правовий, системно-структурний, порівняльний, описовий, експериментальний, ряд логічних методів (аналізу, синтезу, індукції, дедукції, аналогії, версії та ін.).

Наукова новизна одержаних результатів. Під час проведення дослідження автор зробив спробу комплексно дослідити методику розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Практичне значення роботи полягає у виявленні основних проблемних питань щодо методики розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Висновки, які сформульовані у роботі, а також відповідні пропозиції та рекомендації можуть бути використані в подальшому дослідженні зазначеної теми. Крім того, окремі положення та висновки цієї роботи можуть бути використані при підготовці та проведення практичних занять з курсу «Криміналістика» та «Актуальні проблеми кримінального процесу».

Публікації: Гнип С.Г. Способи вчинення і приховування комп’ютерних злочинів *Актуальні дослідження правової та історичної науки (випуск 27)* : матеріали міжнародної науково-практичної інтернет-конференції / Збірник тез доповідей: випуск 27 (м. Тернопіль, 11 грудня 2020 р.). – Тернопіль, 2020. – 111 с.

Структура роботи обумовлена метою та завданнями дослідження і складається із вступу, двох розділів, які поділяються на чотири підрозділи, висновків, списку використаних джерел. Загальний обсяг роботи складає 56 с. Список використаних джерел налічує 64 найменувань.

РОЗДІЛ 1
ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

1.1. Способи вчинення і приховування комп'ютерних злочинів

Необов'язковими ознаками об'єктивної сторони правової структури злочину в кримінально-правовій теорії є час, місце, спосіб, ситуація, засоби та засоби вчинення суспільно небезпечного діяння [8].

Ознаки об'єктивної сторони комп'ютерних злочинів впливають на їх кваліфікацію. Якщо відповідні ознаки не передбачені у статті, їх наявність не впливає на кваліфікацію; однак їх установка є обов'язковою, оскільки:

– ці фактори можуть бути ознаками кваліфікованого злочину;

– наявність цих факторів може свідчити про ступінь суспільної небезпеки діяння та / або злочинця;

– цими факторами можуть бути пом'якшувальні або обтяжуючі обставини;

– може вказувати на зв'язок з іншими злочинами (сукупними) тощо.

На сьогодні фактично не існує визначення поняття засобів, засобів та засобів для вчинення злочинних дій у значенні ст. 361 Кримінального кодексу України, що, в принципі, є несумісним із законодавчим визначенням норми. Як зазначає М. І. Панов, «Усі дії (...) поділяються на прості та складні, фізичні та інформативні. Дія має особливу якість - особливий формуючий метод - реалізація (методи), що є частиною макроструктури дії як відносно самостійної та постійної одиниці. Це властиво всій добровільній поведінці суб'єкта (...) »[12]. Очевидно, що злочинні дії, що становлять незаконне втручання в

комп'ютерні системи, як типовий приклад інформаційного злочину, вчиняються певним чином.

Є. Панов також наполягає на тому, що в структурі злочинного посягання спосіб його вчинення є невід'ємною частиною діяння, «захованим у ньому», формує його конкретний зміст і водночас визначає форму зовнішній прояв діяння та злочину в цілому [12].

У цьому випадку під способом вчинення злочину традиційно розуміють сукупність підходів і методів, що використовуються злочинцем у процесі досягнення його злочинного умислу [26].

Отже, на наш погляд, що стосується конкретно теорії кримінального права, а також нового для обвинувальних актів за п. 361 Кримінального кодексу України, встановлення засобу вчинення злочину є необхідним для належної кваліфікації.

Ми також вважаємо, що для ретельного вивчення елементів та характеристик правової природи злочинних діянь, пов’язаних з несанкціонованим доступом до комп’ютерної інформації та навмисного розповсюдження шкідливих комп’ютерних програм, необхідно „проаналізувати детально ці характеристики як знаряддя та знаряддя злочину.

Засобами злочинності у значенні кримінального закону є явища, які прямо вказуються у кримінальному праві та значно підвищують соціальну небезпеку діяння, що враховується для полегшення вчинення злочину [27].

У цьому випадку, як зазначалося, деякі експерти з питань злочину включають програмне та апаратне забезпечення, призначене для проникнення в комп'ютерні системи і може спричинити руйнування або спотворення комп'ютерної інформації, завдяки використанню яких, на думку законодавця, бути поширеним комп’ютерним вірусом, як і сам комп’ютерний вірус [44].

На наш погляд, комп’ютерний вірус - це інструмент злочину, поряд з іншим програмним та апаратним забезпеченням, призначеним для незаконного впливу на роботу комп’ютерної системи. Якщо комп’ютерний вірус впроваджується в комп’ютерну систему за допомогою програмного та апаратного забезпечення, призначеного для проникнення в комп’ютерні системи, таке специфічне використання комп’ютерного вірусу є засобом вчинення злочину. У той же час важливо з’ясувати вищезазначені характеристики об’єктивної сторони злочину, сформульовані у ст. 361 Кримінального кодексу України, стосовно деяких діянь, що регулюються цим правилом, оскільки при кваліфікації діянь відповідно до цього правила встановлення зброї та способів вчинення цього злочину є, на наш погляд, обов’язковим.

На відміну від юридичної структури, умовно названої «Несанкціонований доступ до комп’ютерної інформації», для якої законодавець не передбачає обов’язкового встановлення необов’язкових ознак об’єктивної сторони злочину, для юридичної структури «Навмисне розповсюдження шкідливих комп’ютерних програм» необхідно встановити об’єктивну сторону зазначеного засобу розповсюдження комп’ютерного вірусу – програм для незаконного проникнення в комп’ютери, їх комп’ютерні системи чи мережі, за умови, що їх здатність спричиняти спотворення чи знищення комп’ютерної інформації комп'ютер або носій цієї інформації, за допомогою якого може бути занесений комп'ютерний вірус.

Стосовно самого комп'ютерного вірусу, для навмисного поширення якого ст. 361 Кримінального кодексу України передбачає кримінальну відповідальність, слід зазначити, що вона також виступає як знаряддя злочину і не може бути включена до переліку інших суб’єктів злочину, що розслідуються .

Таким чином, виникає суттєве питання: яка ознака є складовою злочину, передбаченого ст. 361 Кримінального кодексу України, є

комп’ютерний вірус, який безпосередньо загрожує об’єкту, що охороняється.

Встановлений арт. 361 Кримінального кодексу України, кримінальна відповідальність за поширення комп'ютерного вірусу є новою для ст. 1981 Кримінального кодексу України 1960 р. Комп’ютерні віруси становлять значну загрозу “віртуальним стосункам” у всьому світі [28]. Однією з головних причин цього є те, що програмне забезпечення не може бути досить надійним. Як зазначає Ю. М. Батурин, цей факт відомий усім спеціалістам у галузі програмного забезпечення, оскільки всі програми мають недоліки і багато з них виявляються протягом багатьох років [31].

В. В. Крилов зазначає, що на російському ринку програмного забезпечення в 1997 р. Було зафіксовано появу від двох до десяти раніше невідомих комп'ютерних вірусів [32].

У популярній літературі комп’ютерний вірус визначається як комп’ютерна програма, яку можна ввести в інші програми без відома користувача та проти їх волі, а також відтворювати при повторному запуску зараженого файлу. Комп’ютерний вірус заважає нормальній роботі комп’ютера, може знищувати дані, спотворювати зображення на екрані дисплея, уповільнювати процес обчислення [8].

Комп’ютерний вірус також трактується фахівцями як програма для комп’ютера, яка здатна без відома користувача та проти його волі самостійно розмножуватися та поширюватися, порушуючи здатність працювати з комп’ютерним програмним забезпеченням [22].

Простіше кажучи, комп’ютерний вірус - це комп’ютерна програма, покликана порушити нормальне функціонування комп’ютерної системи в цілому, оскільки вихід з ладу програмного забезпечення та порушення його належного функціонування в майбутньому призводить до несправності всієї системи (в теч. включаючи мережевий комп'ютер). Шкода, яку вірус може завдати

комп’ютерам, їх комп’ютерним системам або мережам, може призвести не тільки до спотворення або знищення комп’ютерної інформації, а й до знищення комп’ютерних носіїв інформації.

Принцип дії комп'ютерного вірусу полягає в тому, що він здатний розмножуватися у "зараженій" комп'ютерній системі без додаткового контролю. Відтворювані частинки вірусу заповнюють вільний простір автоматизованої системи, «вкладаючи» в програмне забезпечення комп’ютерної системи.

За методом впливу на комп’ютерну інформацію віруси поділяються на: маніпуляції вірусами, ключові віруси, віруси, що генерують файли заражених програм, віруси - маніпулятори даними [34], ілюзіоністські віруси [35].

За формою написання Ю. М. Батурин та А. М. Жодзішський поділяють віруси на вульгарні та фрагментовані [36].

Вульгарний комп’ютерний вірус - це програма, написана цілим твором, яку можна виявити на початковій стадії епідемії в комп’ютері («зараження» комп’ютера).

Фрагментований вірус - це окрема частинка, яка, на перший погляд, не зв’язана. Однак вони містять інструкції, які вказують комп'ютеру, як зібрати ці частинки в єдине ціле, що є повною антивірусною програмою. Цей зв’язок є початком епідемії, вірусною інфекцією комп’ютера.

На наш погляд, комп’ютерний вірус - це специфічна комп’ютерна програма, яку при прикріпленні до інших файлів можна непомітно імпортувати для власника (користувача) в комп’ютери, в їх систему та шляхом самовідтворення (аналогія з біологічний вірус) мають наслідки у вигляді: знищення, блокування, зміни, копіювання в автономному режимі, надсилання небажаним реципієнтам тощо. комп’ютерна інформація, а також (або) спрямована на заподіяння шкоди

комп’ютерним носіям, програмному та апаратному забезпеченню комп’ютерної системи.

Як зазначає В. П. Леонтьєв, вірусні віруси в більшості випадків - це електронні листи з вкладеннями [33].

експерти вважають, що комп’ютерні віруси повинні впливати лише на комп’ютерну інформацію (включаючи програмне забезпечення), а фактичний збиток на апаратному забезпеченні комп’ютера не може безпосередньо спричинити, вказуючи на те, що сьогодні майже не існує такі прості засоби. пошкодження обладнання (за винятком маси, якій немає рівних у фізичному знищенні всього живого та неживого) [34].

Ми вважаємо, що комп'ютерний вірус є прямим знаряддям злочину "умисне поширення комп'ютерного вірусу", оскільки є основним незаконним та небезпечним навантаженням, що передається певними засобами - програмним та апаратним забезпеченням, призначеним для незаконного проникнення в комп'ютери, їхні комп’ютерні системи та мережі та здатні спотворювати чи руйнувати інформацію чи комп’ютерні носії інформації.

Насправді комп’ютерні віруси не «закріплюються». Поширення комп’ютерного вірусу може відбуватися за допомогою використання програмного та / або апаратного забезпечення, включаючи звичайні файли [37], які виступають як «носії вірусу». У разі власної придатності для техніко-технологічного обслуговування програмно-технічне забезпечення автоматично стає здатним завдати шкоди об’єкту через те, що вони містять (або через них) комп’ютерний вірус. Коли їх «завантажує» комп’ютерний вірус, фактична ідентифікація їх небезпеки із самим комп’ютерним вірусом відбувається автоматично, оскільки такий вірус безпосередньо міститься в ньому.

За змістом ст. 361 Кримінального кодексу України, випливає, що злочином визнається лише поширення комп’ютерного вірусу, яке

сталося через використання програмного та апаратного забезпечення, яке:

1) призначені для введення в електронний комп’ютер;

2) мають можливість спотворювати чи руйнувати комп’ютерну інформацію.

На наш погляд, у формулюванні законодавчого положення ч. 1 с. 361 Кримінального кодексу України було визнано важливим для практичного застосування цієї неточності правила. По суті, терміни "програмне та апаратне забезпечення, призначене для незаконного проникнення в АЕОМ, їхніх комп'ютерних систем або мереж і здатні спотворювати або знищувати комп'ютерну інформацію або її носії", не повинні застосовуватися до правила, що регулює навмисний розподіл. безпосередньо на комп’ютері. вірус матки.

Ці положення були запозичені з відповідної статті Кримінального кодексу України 1960 р., який передбачав кримінальну відповідальність за «порушення автоматизованих систем». Це не передбачало криміналізації навмисного розповсюдження комп’ютерного вірусу, але криміналізувало розповсюдження програмного та апаратного забезпечення, призначеного для посягання на комп’ютерні системи та здатного спотворювати чи знищувати інформацію чи засоби масової інформації. У стандарті, передбаченому ст. 361 Кримінального кодексу України, таке формулювання майже збереглося, тоді як воно втрачає своє попереднє значення, через те, що таке програмне та апаратне забезпечення законодавець не визнає саме знаряддя злочину, як у ст. 1981 року Кримінального кодексу України 1960 р. Та як засіб поширення комп’ютерного вірусу.

Що стосується фактичної редакції положення ч. 1 ст. 361 Кримінального кодексу України, ми вважаємо, що таке формулювання є нелогічним, оскільки:

1. Комп’ютерний вірус може поширюватися, приєднуючись до будь-якої програми, як небезпечної, так і безпечної, наприклад, електронної пошти, повідомлень, електронної пошти тощо. Тобто для його розповсюдження не потрібно використання спеціального програмного забезпечення, призначеного для потрапляння в комп’ютер, систему або мережу, оскільки власник (користувач) може «запустити» комп’ютерний вірус, перевіривши відповідність, відкривши вкладення. , що містять програмний вірус.

2. Комп’ютерний вірус є одним із таких шкідливих програм. Іншими словами, поняття "програмне та апаратне забезпечення для вторгнення та АЕОМ, їх комп'ютерні системи та мережі, здатні спричинити спотворення або знищення інформації", ширше, ніж поняття "комп'ютерний вірус", і повинно поглинати останнє.

Якщо комп’ютерний вірус розглядається як пряма загроза функціонуванню комп’ютерів, їх комп’ютерних систем та мереж, неможливо вказати засоби його розповсюдження, оскільки спектр засобів занадто широкий, а характеристики засобів не є 'не впливає на остаточне визначення інструменту. цей злочин - безпосередньо комп'ютерний вірус.

Комп’ютерний вірус (програмне забезпечення) може поширюватися як за допомогою шкідливих програм, так і за допомогою програм, які спеціально не створювались для незаконних дій, не призначені для проникнення на комп’ютери інших людей, їх системи чи комп’ютерні мережі. Вірус - це програма, створена для "руйнівних" чи інших шкідливих цілей.

Крім того, вірус може поширюватися шляхом його безпосереднього впровадження в комп’ютер, в комп’ютерну систему або комп’ютерну мережу, відкриваючи його, зберігаючи, переносячи. «Пряме» впровадження програмного вірусу може відбуватися шляхом впровадження певних технічних пристроїв як у випадку його

впровадження в автоматизовану систему з певного середовища, так і шляхом впровадження шкідливого вірусу шляхом набору тексту команди, що складають його або активують на клавіатурі комп'ютера, або передають його за допомогою телекомунікаційних каналів для обміну інформацією.

Відповідно до формулювання ст. 361 Кримінального кодексу України, увага законодавця при прийнятті цієї норми була зосереджена на обов’язковому регулюванні кримінальної відповідальності за поширення комп’ютерних вірусів. Однак інша шкідлива програма, яка не підпадає під ознаку комп’ютерного вірусу, не значиться як інструмент для вчинення цього злочину.

Однак перелік шкідливих комп’ютерних програм не обмежується лише комп’ютерними вірусами.

Наприклад, К. Кауфман, Р. Перлман та М. Спенсер до зловмисного програмного забезпечення включають такі типи шкідливих програм, визначаючи їх зміст таким чином:

«Троянський кінь - це інструкція, прихована серед шкідливих програм. Вірус - це тип інструкцій, який, будучи необхідним, копіює себе в інші програми. Бактерія - це програма, яка, звільнившись, копіює себе, поглинаючи ресурси. Черв'як - це програма, яка відтворює себе, відтворюючи власні копії на інших машинах посеред мережі. Схожий на бактерію, але поширюється по всій системі, тоді як бактерії, як правило, залишаються в одній машині. Пастка - це неописана точка входу, навмисно введена в програму, часто з метою налагодження програми, яка може бути використана як незручність для захисту від несанкціонованого доступу. Логічна бомба - це шкідлива інструкція, яка швидко реагує на певні майбутні дії, наприклад у випадку збігу часових обставин» [24].

Тому, на наш погляд, недоцільно визначати програмне забезпечення, яке може самостійно пошкодити комп’ютерні системи та

комп’ютерну інформацію, як засіб поширення комп’ютерного вірусу, оскільки у випадку їх власного впровадження, згідно з формулюванням ст. . 361 Кримінального кодексу України особи, які вчинили такі дії, як підкладання бомби із затримкою або бомби із затримкою до комп’ютерної системи, не можуть бути притягнуті до відповідальності.

Ми вважаємо, що програмне та апаратне забезпечення, що використовується для впровадження комп’ютерного вірусу в комп’ютерну систему, повинно визнаватися таким.

Однак, якщо вони вводяться в комп’ютерну систему як безпосередньо завдають шкоди, вони повинні розглядатися як альтернативний інструмент злочину "навмисне розповсюдження шкідливих комп'ютерних програм".

Слід зазначити, що у разі використання програмного та апаратного забезпечення для несанкціонованого доступу до комп’ютерних систем вони виступають інструментом, за допомогою якого здійснюється таке вторгнення.

Здійснення несанкціонованого доступу до комп'ютерної інформації, як законний компонент конкретного злочину, може використовуватися разом із ключовими вірусами, "логічними бомбами", які можуть розблокувати системи безпеки, "пастками", які можуть бути інтегрованою в програму для полегшення несанкціонованого доступу в майбутньому до спеціального програмного забезпечення, яке може "допомогти" хакеру вибрати паролі та коди доступу для комп'ютера, комп'ютерної системи або мережі комп'ютер атакував.

На наш погляд, технічні засоби взагалі не слід визначати як засоби вчинення злочину, що розслідується (злочини, що розслідуються), оскільки вони самі по собі не є загроза громадській безпеці. У цьому випадку правопорушник може використовувати їх для передачі, розповсюдження шкідливих комп’ютерних програм, створених для вчинення або сприяння здійсненню несанкціонованого доступу до

комп’ютерної інформації в засобах масової інформації [139]. Неможливо не припустити можливості злочинців використовувати спеціально пристосовані та спроможні технічні засоби, аналізуючи системи безпеки автоматизованої системи, вказувати хакеру найкращі варіанти вчинення несанкціонованого доступу, допомагати для вибору паролів безпеки, кодів тощо.

Визначати (розглядати) технічні засоби як обов’язкову ознаку даної структури не зовсім правильно, оскільки технічні засоби при цьому є лише одним із засобів передачі такого програмного забезпечення. Тому, на наш погляд, програмне та апаратне забезпечення не є обов’язковою ознакою об’єктивної сторони юридичного складу злочину, оскільки їх визнання може призвести до неможливості притягнення до відповідальності винних у несанкціонованому доступі до комп’ютера. . інформація.

Слід зазначити, що зловмисне програмне та апаратне забезпечення повинно встановлюватися як необов’язкова частина об’єктивної сторони зазначених злочинів як знаряддя вчинення злочину, оскільки їх характеристики та / або характеристики їх досліджень слід враховувати. при оцінці ступеня суспільної небезпеки вчинених дій, а також при характеристиці особи злочинця.

1.2. Предмет злочинного посягання комп’ютерних злочинів

Предметом злочину в класичній теорії кримінального права є речі матеріального світу, діючи на які людина посягає на цінності (вигоди), що належать суб'єктам суспільних відносин [7].

У світі підхід до визначення предмета злочинів, що посягають на безпеку комп’ютерних систем, різний. Так, Кримінальний кодекс штату Юта (США), як предмет таких злочинів, включає "матеріальні та

нематеріальні елементи, пов'язані з комп'ютерами, системами та комп'ютерними мережами" [34].

Щодо визначення предмета злочину згідно зі ст. 361 Кримінального кодексу України висловлюється кілька точок зору.

Об'єкт злочину у розумінні ст. 361 Кримінального кодексу України А. М. Ришелюк визначає як: «1) автоматизовані електронні комп’ютери (комп’ютери, АЕОМ), у тому числі персональні; 2) їх системи; 3) комп’ютерні мережі» [40].

На думку М. І. Панова, об’єктом злочину є: 1) електронний комп’ютер; 2) автоматизовані комп’ютерні системи (АКС); 3) комп’ютерні мережі; 4) комп’ютерні носії; 5) комп’ютерна інформація [8].

П. П. Андрушко включає автоматизовані електронні комп’ютери про вказаний злочин; Системи АЕОМ або автоматизовані системи; комп’ютерні мережі; ІТ-підтримка; комп'ютерні віруси; комп'ютерна інформація; програмно-технічне забезпечення, призначене для незаконного проникнення в автоматизовані комп’ютери, їх комп’ютерні системи та мережі [4].

В. Б. Вехов наполягає на тому, що до суб’єктів цих злочинів належить «інформація про машини, комп’ютерну систему та комп’ютерну мережу» [9].

Ці погляди на коло суб'єктів злочину у значенні статті 361 Кримінального кодексу України свідчать про низку відмінностей. Водночас слід зазначити, що деякі експерти не включають комп’ютерну інформацію до спектру альтернативних тем злочинності [30], що прямо зазначено у статті 361 Кримінального кодексу України як предмет спотворення чи знищення якого діями злочинця.

Спираючись на думку С. В. Фесенка щодо предмета злочину, під яким він розуміє "що, діючи на те, що суб’єкт зазіхає" на об’єкт злочину, ми вважаємо, що невизнання комп'ютерної інформації окремими

експертами щодо якості предмета злочину зумовлене "матеріалістичним" підходом класичної теорії кримінального права щодо визначення предмета злочину як певних матеріальних цінностей. На той час комп'ютерна інформація була віртуальним об'єктом, тобто "умовною, фізично відсутньою, але спеціальними методами, доступними".

На наш погляд, під віртуальним слід розуміти об’єкт об’єктивного світу, який створений спеціальними методами та (або), фізично відсутній, але має зовнішнє уявлення, або може набути такого подання спеціальними методами. або методи впливу.

О.Н. Радутний, шукаючи інформацію як предмет злочину, дійшов висновку, що сучасні реалії вимагають подальшого визнання суб'єктом злочинних речей або інших явищ об'єктивного світу (інформація, енергія, та ін.), з певними властивостями, наявність яких стосується кримінального права. у тому, що особа вчиняє конкретний злочин [42].

Однак, якщо проаналізувати предмет злочину згідно з наведеним вище визначенням, поняття суб’єкта злочину включає всі речі та явища об’єктивного світу, властивості яких пов’язані з наявністю злочину в певних діях. . У цьому випадку дія злочинця може не бути спрямована проти них, або вони не можуть зазнати кримінального впливу. Наприклад, поняття "час" для деяких злочинів є обов'язковою ознакою з об'єктивної сторони, оскільки закон пов'язує наявність певного часу або повного типу часу з визначенням конкретного злочину. У цьому випадку час не є предметом злочину, оскільки на нього не впливає людина; термін "час" стосується необов'язкових ознак з об'єктивної сторони, серед інших: місце, метод, ситуація та інші. Так само необхідно відрізняти знаряддя злочину від об’єкта злочинного посягання, знаючи, що знаряддями можуть бути як матеріальні, так і віртуальні речі.

Тому ми вважаємо, що необхідно уточнити це визначення з урахуванням особливостей безпосереднього визначення предмета злочину, як одного із обов’язкових елементів злочину.

На наш погляд, під предметом злочину слід розуміти речі чи інші явища об'єктивного світу, як матеріального, так і віртуального, з певним впливом, до якого кримінальне право пов'язує наявність у діянні особа певного злочину.

На думку В.С.Комісарова, комп’ютерна інформація - це інформація про людей, предмети, факти, події та явища обмеженого доступу або необмеженого характеру, які знаходяться в NOM, комп’ютерних системах або їх мережах [23].

В. А. Мазуров наголошує, що комп’ютерну інформацію слід розуміти як інформацію на носіях машин, комп’ютерів, комп’ютерних систем або їх мереж [24].

Важливо правильно визначити значення термінів «комп’ютерний вірус» та «програмне та апаратне забезпечення, призначене для незаконного проникнення в комп’ютери, їх комп’ютерні системи та мережі», які, на наш погляд, належать до інструментів дослідження злочинів.

Відповідно до законодавчого визначення стандарту „незаконне втручання в роботу електронних комп’ютерів (комп’ютерів), комп’ютерних систем та мереж”, передбаченого ст. 361 Кримінального кодексу України, іншими суб’єктами цього злочину, на наш погляд, є: комп’ютери, їх комп’ютерні системи та мережі, комп’ютерна інформація та комп’ютерні носії.

У цьому розділі ми аналізуємо перші три альтернативні теми, а саме комп’ютери, комп’ютерні системи та комп’ютерні мережі.

У пункті 7.3 ДСТУ "Автоматизовані системи. Терміни та визначення", цифровий комп’ютер (синонім "електронний комп’ютер") означає набір системного обладнання та програмного забезпечення, що

створює можливість обробляти інформацію та отримувати вихідні дані у вигляді потрібно [21].

П. П. Андрушко слушно зазначає, що: «Автоматизовані електронні комп’ютери (комп’ютери) - це комплекси електронних пристроїв, побудованих на базі мікропроцесора, які використовуються для виконання операцій, визначених комп’ютерною програмою або користувачем (послідовність дій для пристрої обробки інформації та електронного управління) символічна та образна інформація, зокрема, їх введення та виведення, їх знищення, їх копіювання, їх модифікація, їх передача інформації в комп'ютерній системі або мережі та інші інформаційні процеси. АЕОМ, як правило, складається з трьох частин: центрального блоку, який включає мікропроцесор та інші периферійні пристрої, необхідні для його роботи (акумулятори даних, джерело живлення тощо), клавіатуру, яка використовується для введення символів у АЕОМ, а також монітор, на якому відображається текстова та графічна інформація» [24].

На наш погляд, комп’ютер - це сукупність апаратного та програмного забезпечення, призначеного для автоматичної обробки інформації, частково керованої оператором.

Що стосується комп’ютерних систем, визначення фахівців також дуже різні. Таким чином, деякі вчені ототожнюють поняття "комп'ютерні системи" з поняттям "автоматизовані системи", тоді як деякі визначають комп'ютерні системи окремо.

На думку А. М. Ришелюка, «Автоматизовані електронні комп’ютерні системи відносяться до операційних систем (MS-DOS, Windows та інших), які встановлені на певній машині і з якими виконується її робота, а також різних прикладних систем (тобто, включаючи системи управління), як встановлені для локальної роботи на окремій машині, так і відкриті для доступу з інших машин через комп’ютерну мережу» [20].

П. П. Андрушко вважає, що поняття "система АЕОМ" ідентичне поняттю "автоматизовані системи" [24], а оскільки їх тлумачення стосується законодавчого тлумачення автоматизованих систем [7].

Відповідно до визначення законодавця, автоматизовані системи (АС) - системи, що здійснюють автоматизовану обробку даних і які включають технічні засоби їх обробки (обчислювальна техніка), а також методи та процедури, програмне забезпечення [7]. Державний стандарт України визначає автоматизовану систему як організаційно-технічну систему, що складається із засобів автоматизації певного типу (або декількох типів), діяльності осіб та персоналу, що здійснює цю діяльність [21] .

На наш погляд, поняття "комп'ютерна система" не є таким, як поняття "автоматизовані системи".

Під поняттям "їх система" в контексті с. 361 Кримінального кодексу, на наш погляд, слід розуміти операційні системи електронних комп'ютерів, що забезпечують безпосередню роботу на певному комп'ютері, а також спеціальні операційні системи, призначені як для роботи локальний і працювати в комп’ютерній мережі.

Таким чином, до операційних систем комп’ютерів належать зокрема такі операційні системи, як Norton Commander, MS-DOS, Windows, які є програмним пакетом для запуску на окремому комп’ютері або в локальній мережі (у випадку встановлення в локальній мережі версії операційної системи).

Операційні системи, які мають особливий характер застосування, зокрема, включають бухгалтерські операційні системи, поширені в колишньому СРСР, такі як "1-С" та "Фат Ганс".

Операційні системи, що працюють у комп’ютерній мережі, включають, але не обмежуючись ними, Netscape Communicator, Internet Explorer, Opera тощо.

Операційні системи електронних комп’ютерів - це компоненти самих комп’ютерів, з яких вони забезпечують роботу (загальну чи специфічну).

Тому, на наш погляд, поняття "комп'ютерні системи" набагато ширше поняття "комп'ютерні системи", а також більш широке поняття "комп'ютери" та "комп'ютерні мережі". Іншими словами, термін "комп'ютерні системи" поглинає "комп'ютери, їх комп'ютерні системи та мережі".

Подібну думку також висловлює А. Г. Волеводзь, посилаючись, зокрема, на пункт „а” ст. 1 Конвенції про кіберзлочинність, прийнятої 23 листопада 2001 р. Відповідно до пункту а ст. 1 з яких комп’ютерна система позначає будь-який пристрій або групу взаємопов’язаних або суміжних пристроїв, один або кілька з яких, діючи за програмою, виконують автоматизовану обробку даних [8].

Щоб остаточно визначити цю потребу, ми проаналізуємо наукове визначення поняття "комп'ютерна мережа".

У популярній літературі комп’ютерна мережа - це сукупність автономних електронних комп’ютерів, пов’язаних лініями передачі даних для взаємної координації обміну інформацією [28].

Державний стандарт України визначає комп’ютерну мережу як систему «взаємопов’язаних засобів зв’язку комп’ютерів різної продуктивності та конфігурації» [41].

В. Н. Кононихін зазначає, що «інформацію та комп’ютерну мережу як сукупність географічно розділених комп’ютерів та терміналів, пов’язаних віддаленою обробною мережею. Термінал комп’ютерної системи - це «набір апаратного та програмного забезпечення (від найпростішого пристрою вводу-виводу до комп’ютера), призначений для підключення користувача до комп’ютерної системи чи інформаційної мережі» [21].

На думку П. П. Андрушка, комп’ютерна мережа - це комплекс АЕОМ або їх системи, пов’язані лініями зв’язку [24].

Комп’ютерна мережа, на думку А. М. Ришелюка, являє собою «набір програмно-апаратних засобів, що забезпечує доступ від одного АЕОМ до програмного або апаратного забезпечення іншого (іншого) АЕОМ та до інформації, що зберігається в системі іншої АЕОМ» [30].

На думку М. І. Панова, комп’ютерна мережа - це зв’язок декількох комп’ютерів (комп’ютерів) та комп’ютерних систем, які пов’язані між собою та розташовані у фіксованій зоні та орієнтовані на колективне використання мережевих ресурсів. Комп’ютерні мережі передбачають спільний доступ до ресурсів комп’ютерного центру, запуск загальних програм, що входять до складу комп’ютерних систем [28].

Комп’ютерні мережі на невеликій території (бізнес, організація) прийнято називати приміщеннями; мережі, що охоплюють великі території (регіон, держава, континент) - глобальні. Інтернет слід визнати глобальною комп’ютерною мережею..

Під каналами або лініями зв'язку розуміють фізичні канали або засоби зв'язку між технічними засобами інформаційної мережі.

Таким чином, поняття «електронні комп’ютери», «комп’ютерні системи», «комп’ютерні мережі» є вужчими поняттями, ніж поняття «автоматизовані системи», викладені у статті 1 українського Закону про захист персональних даних. інформація в автоматизованих системах. "З 5 липня 1994 року:" автоматизована система (АС) - система, що здійснює автоматичну обробку даних і яка включає технічні засоби обробки (засоби обчислювальної техніки та зв'язку), а також методи та процедури, програмне забезпечення» [7].

Конвенція про кіберзлочинність, як загальний термін для комп’ютерів, їх комп’ютерних систем та мереж, використовує, як уже згадувалося вище, загальний термін - „комп’ютерні системи”, що

стосується будь-якого пристрою або групи взаємопов’язаних людей. підключені або суміжні пристрої, один або кілька з яких, діючи за програмою, виконують автоматизовану обробку даних.

З огляду на той факт, що Україна як держава-учасниця Конвенції про кіберзлочинність прийняла прийняття такої норми, поняття "комп'ютерні системи" може застосовуватися в Україні стосовно злочину в за ст. 361 Кримінального кодексу України та в загальному розумінні всіх електронних комп’ютерів, їх комп’ютерних систем та мереж.

Узагальнююче поняття альтернативних суб’єктів злочину, передбачене с. 361 Кримінального кодексу України, а саме комп’ютери, їх комп’ютерні системи та мережі, слід використовувати термін „комп’ютерні системи”, який повністю охоплює ці інші елементи.

Важливо визначити поняття «комп’ютерна інформація», яке є суперечливим і не має єдиного визнання в українському законодавстві та в теорії внутрішнього права [10].

Закон України про інформацію «визначає інформацію як задокументовану або публічно оголошену інформацію про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі. Однак у переліку видів інформації, визначених ст. 8 цього закону інформація про комп’ютер не згадується. Іншими словами, законодавець не демонструє сучасного підходу до визначення комп’ютерної інформації як одного з найпопулярніших видів інформації, яка існує у світі та в Україні» [45].

Крім того, поняття «комп’ютерна інформація» не входить до деяких нормативних актів, де її наявність як об’єкта захисту має бути обов’язковою. Так, законі «Про науково-технічну інформацію» від 25 травня 1993 р. Про розкриття поняття «науково-технічна інформація» (ст. 1) жодне з понять «комп'ютерна інформація», «інформація в автоматизованих системах», інформація в комп'ютерних системах", - не

визначено. У цьому випадку цей закон у переліку інформаційних ресурсів національної науково-технічної інформаційної системи (стаття 10) називається "технічними засобами зберігання, обробки та передачі", під яким ми маємо на увазі комп'ютерне обладнання, робота контролюється програмним забезпеченням і складається безпосередньо з обробки інформації. Іншими словами, робота IT-обладнання в цілому тісно пов’язана з IT-інформацією» [46].

Закон України «Про захист інформації в автоматизованих системах» визначає інформацію в автоматизованих системах як «сукупність усіх даних та програм, що використовуються в АС, незалежно від засобів їх фізичного та логічного подання». Інформація, що міститься в автоматизованих системах, є синонімом термінів «комп’ютерна інформація» та «інформація, що міститься в комп’ютерних системах» [44].

У той же час деякі вчені визначають визначення комп'ютерної інформації як сукупність усіх даних і програм, а також їх зміст за умови, що зазначена інформація включає ідентифікаційні дані власника, який визначив режим (правила) його використання, а також інструкції щодо місцезнаходження. здійснює пошук вказаної інформації - «на носії в мережі АЕОМ або АЕОМ» [24].

Здається, це останнє тлумачення виключає можливість притягнення до відповідальності осіб, які спрямовують свої дії на комп’ютерному носії поза комп’ютером або комп’ютерною мережею, оскільки об’єктом злочину є такі предмети, як інформація на дискетах. та оптичні диски. Тобто, якщо особа пошкодила інформацію на дискеті, а сама дискета не була пошкоджена, то притягнення до відповідальності такої особи стає неможливим за фактичний злочин.

Також слід зазначити, що оцінювати комп’ютерну інформацію лише як набір (одиницю) програм, даних, файлів не є практичним, оскільки кожна програма, файл або база даних також є свого роду

комп’ютерна інформація, а за порушення цілісності або знищення хоча б одного з цих елементів повинна бути понесена кримінальна відповідальність. В іншому випадку, тобто визнання суб’єктом злочину всіх програм, баз даних та файлів на комп’ютерах, деякі інші важливі положення втрачають значення. Наприклад, визначення як кваліфікатора у ч. 2 ст. 361 КК України "заподіяти істотну шкоду" стає недоцільним, оскільки за ч. 1 ст. 361 Кримінального кодексу може бути притягнуто до відповідальності лише проти особи, яка завдала комп’ютеру повної шкоди, тобто коли вона руйнівно вплинула на все програмне забезпечення та інформацію, що зберігається в комп’ютері. У цьому випадку немає різниці між поняттям "шкода" та "істотна шкода", оскільки поняття "шкода" охоплюватиме лише загальний вплив на комп'ютерну систему - вплив на " всі дані та програми ". Якщо організація завдає шкоди програмі, така особа може, згідно із твердженням, уникнути кримінальної відповідальності.

Крім того, немає практичного сенсу згадувати наявність спеціального захисту як обов’язкову ознаку комп’ютерної інформації, якщо злочин, що підриває цілісність інформації, не сформульований як «Несанкціонований доступ до комп'ютерної інформації».

Однак ми вважаємо, що в деяких випадках, наприклад, при визначенні предмета злочину "Умисне розповсюдження шкідливих комп'ютерних програм", необхідно самостійно визначити поняття "програмне забезпечення" спільно з "апаратним забезпеченням" комп'ютерів. , їх системи та комп’ютери. комп’ютерні мережі. Пошкодження апаратного забезпечення в автоматизованих системах може бути спричинене лише опосередковано: на шкідливе програмне забезпечення впливає програмне забезпечення, а таке "пошкоджене" програмне забезпечення може пошкодити комп'ютерне обладнання, системи або комп'ютерні мережі.

Закон України «Про авторське право та суміжні права» визначає поняття «база даних» та «комп’ютерна програма», які є видами комп’ютерної інформації та на які поширюється дія цього закону» [43].

Відповідно до ст. 1. за. 14 цього закону комп'ютерна програма визнається "набором інструкцій у формі слів, цифр, кодів, діаграм, символів або будь-якої іншої форми, виражених у формі, що читається комп'ютером, які активують його для досягнення певної мети або результату (ця концепція охоплює як операційну систему, так і прикладну програму, виражену у вихідному коді або об’єкті)» [43].

База даних (компіляція даних), відповідно до українського Закону про авторське право та суміжні права (пункт 1 статті 1), являє собою сукупність творів, даних або іншої незалежної інформації за деякими будь-якої форми, включаючи - електроніка, вибір та розташування компонентів якої та їх розташування є результатом творчої роботи, а компоненти якої доступні окремо та можуть бути знайдені за допомогою спеціальна пошукова машина на основі електронних засобів (комп’ютер) або інших засобів.

Таким чином, терміни "комп'ютерна програма" та "база даних" охоплюють два основних типи комп'ютерної інформації, які визнані об'єктами авторського права та суміжних прав. Однак український Закон про авторське право та суміжні права не розкриває понять інших типів комп’ютерної інформації, таких як програмне забезпечення та засоби математичного захисту та інформація в Інтернеті, особливо електронна пошта. .

Водночас такі визначення на законодавчому рівні майже відсутні або не збігаються. Так, у статті 1 Закону України «Про національну програму комп'ютеризації» визначається як іменований набір даних, що відображає стан об’єктів та їх взаємозв’язок у певному домені. Іншими словами, така інтерпретація виходить за межі комп’ютеризації і може застосовуватися як до віртуальних об’єктів, так і до об’єктів

матеріального світу. Тому не існує визначення комп'ютерної бази даних як такої» [47].

У ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» [21] розкриває концепцію комп’ютерних даних, згідно з якою дані розпізнаються як інформація, що надається у формалізованій формі, придатній для зберігання, обробки, передачі та інтерпретації користувачем, процес подання заявки та технічні засоби.

Крім того, ДСТУ 2226-93 надає визначення так званих автоматизованих системних інформаційних баз даних, що означає "набір впорядкованої інформації, що використовується в роботі автоматизованої системи".

На наш погляд, концепція комп’ютерної програми, законодавче визначення якої була наведена вище, насправді є досконалою і за певних роз’яснень може застосовуватися в інших нормативних актах, що регулюють відносини у сфері комп’ютеризація.

Комп’ютерну інформацію слід визначати як інформацію, що зберігається або передається між електронними носіями, незалежно від їх фізичного чи логічного подання, і яка може використовуватися, оброблятися, модифікуватися комп’ютером.

Комп'ютерна інформація, з точки зору цього дослідження, повинна розглядатися як предмет злочинних дій, пов'язаних з несанкціонованим доступом до комп'ютерної інформації та навмисного розповсюдження шкідливих комп'ютерних програм.

Одним із альтернативних суб’єктів злочину згідно зі ст. 361 Кримінального кодексу України, є комп’ютерні носії інформації.

«Відповідно до українського Закону про захист інформації в автоматизованих системах від 5 липня 1994 р. Та Положення про захист технічної інформації в Україні, затвердженого Кабінетом Міністрів України 9 вересня 1994 р. № 632, Носії інформації - це фізичні об’єкти, поля та сигнали, хімічне середовище, накопичувачі даних в

інформаційних системах. П. П. Андрушко також визначає поняття «носії комп'ютерної інформації» відповідно до згаданого Положення про технічний захист інформації в Україні» [24].

Під поняттям «комп'ютерна підтримка» автори розуміють фізичні об'єкти призначені для постійного зберігання, передачі та обробки комп'ютерної інформації. Сюди входять магнітні диски (дискети), жорсткі магнітні диски (жорсткі диски), касетні стрічки (розтяжки), магнітні барабани, магнітні картки тощо» [28].

У пункті 24 «Положення про технічний захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9 вересня 1994 р. № 632, зазначено: «Інформаційні об'єкти з обмеженим доступом можуть бути фізичними об'єктами, поля та сигнали, хімічне середовище, накопичувачі даних в інформаційних системах» [48].

Отже, до комп'ютерних носіїв належать: фізичні об'єкти, поля, сигнали, хімічні середовища, акумулятори даних в інформаційних системах.

Поняття «інформаційні системи» в контексті пункту 24 Положення про технічний захист інформації в Україні є синонімом поняття «автоматизовані системи» [44].

«Низка авторів посилаються безпосередньо на ст. 24 Положення про технічний захист інформації в Україні, інші пояснюють тлумачення визначень заголовка, зазначаючи, що комп'ютерні носії включають: магнітні диски (дискети), жорсткі магнітні диски (жорсткі диски), магнітні касетні стрічки (банери), барабани магнітні, магнітні картки, оптичні диски (компакт-диски) тощо. Комп'ютерні носії інформації - це фізичні об'єкти, машинні носії, призначені для постійного зберігання, передачі та обробки комп'ютерної інформації» [28].

«Комп'ютерні носії повинні бути тими, які, незалежно від наявності певної комп'ютерної інформації та ідентифікації цієї комп'ютерної інформації, можуть бути ідентифіковані, тобто вони

можуть бути ідентифіковані як такі, що належать до приватний власник» [7].

Для остаточного визначення комп’ютерних ЗМІ як альтернативних суб’єктів злочину, що розслідується, необхідно звернутися до визначення ЗМІ Державним стандартом України. Таким чином, згідно з пунктом 7.20 ДСТУ 2226-93, носієм даних є "об'єкт, призначений для запису, зберігання, зчитування або передачі даних".

«Комп’ютерні носії інформації - це фізичні об’єкти - машинні носії у вигляді полів, сигналів, хімічних середовищ, накопичувачі даних у комп’ютерних системах тощо. інформація про комп’ютер» [64].

Комп'ютерні носії інформації включають: жорсткі диски, магнітні диски, дискети, оптичні диски.

Відповідно до ст. 10 Закону України про захист інформації в автоматизованих системах «захист інформації в комп’ютерній системі забезпечується повага суб’єктами правовідносин стандартів, вимог та правил організаційно-технічного характеру щодо захисту оброблюваної інформації; використання комп’ютерного обладнання, програмного забезпечення, засобів зв’язку та колонок (комп’ютерна система - NR) загалом, засобів захисту інформації, що відповідають встановленим вимогам щодо захисту інформації; перевірити відповідність комп'ютерного обладнання, програмного забезпечення, засобів зв'язку та АС загалом встановленим вимогам до захисту інформації (сертифікація комп'ютерного обладнання, засобів зв'язку та АС); здійснювати контроль за захистом інформації» [44].

Захист, згідно з ДСТУ 2226-93, означає засіб обмеження доступу до використання всієї комп’ютерної системи або її частини [91]. Захист даних - це "організаційні, програмні та технічні методи та засоби для впровадження обмежень доступу до набору даних для типів даних у системі обробки даних" (параграф 8.27).

Особлива увага приділяється на практиці питанню, чи є паролі та комп’ютерні коди, що забезпечують захист комп’ютерної інформації та її доступ, про злочин, який розслідується? Вирішення цієї проблеми вплине на визначення стадії злочину "Незаконне втручання в роботу комп'ютерів (комп'ютерів), комп'ютерних систем та мереж". Це питання виникає, насамперед, оскільки зазначений злочин за розміром штрафу належить до злочинів малої тяжкості, кримінальна відповідальність за підготовку яких до вчинення, згідно зі статтею 1 ст. 14 Кримінального кодексу України, не відбувається.

Низка авторів до переліку техніко-технічних заходів захисту інформації в автоматизованих системах відносять такі види:

- фізичний захист (за допомогою технічних пристроїв);

- програмно-математичний захист (паролі доступу, режими доступу користувачів тощо);

- захист апаратно-програмного забезпечення (комплексне використання апаратно-програмного забезпечення) [15].

Існує кілька різних тлумачень терміна "пароль" для доступу до комп'ютерної системи. Пароль у правилах та спеціалістах означає:

1) секретний код, що використовується для гарантування конфіденційності інформації;

2) інформація таємного розпізнавання, яка, як правило, складається з ряду ознак;

3) унікальний набір символів, що використовуються користувачем як ідентифікаційний код.

«Пароль для доступу до комп’ютерної системи слід розуміти як унікальний набір секретних символів, що розуміється комп’ютерною системою як ідентифікаційний код для доступу користувача чи особи. власник комп’ютерної системи або певної комп’ютерної інформації» [7].

Особа, яка користується комп’ютером, може ввести будь-який набір даних у комп’ютерну систему як пароль доступу, що в

майбутньому комп’ютерна система визнає його законним користувачем. Так, користувач Бондаренка Василь Степанович може ввести такі паролі:

- ті, що пов'язані з його ім'ям, ім'ям, по батькові - Бондаренко, вгасили, бондарви, бвс тощо;

- ті, що пов’язані з іменами його родичів та змінами до цих імен - marija (mary), alexandr (aleh, alexx), olga тощо.

- інші дані, які можуть бути відомі лише цьому користувачеві.

Визначення понять "код" і "кодування" доступу до комп'ютерної системи або комп'ютерної інформації також різне. Кодування - це процес ручного або автоматичного представлення символів одного алфавіту з використанням символів іншого алфавіту.

«Поняття «код», що використовується в комп'ютерних системах, визначається Національним стандартом України таким чином:

1) набір правил, що визначають подання даних у дискретному вигляді;

2) (у поданні даних) набір правил, які перетворюють елементи одного набору в елементи іншого набору» [7].

Крім того, термін "код" має кілька значень для комп'ютерних систем. Окрім поняття «код доступу» в інформатиці існують поняття вихідного коду, об’єктного коду тощо. Тому поняття кодування також неоднозначне лише з точки зору введення кодів доступу до певної комп’ютерної системи чи комп’ютерної інформації.

На наш погляд, під кодом комп’ютерної системи слід розуміти сукупність правил, що визначають порядок подання даних, розпізнаних комп’ютерною системою у перетвореному вигляді.

«Код доступу до комп'ютерної системи або комп'ютерної інформації слід розуміти як набір правил, що регулюють подання даних, за допомогою яких комп'ютерна система розпізнає власника або

користувача доступу до комп'ютерної інформації, що зберігається в ній» [57].

«Очевидно, що термін «код доступу» не є однаковим із терміном "пароль доступу" до комп'ютерної системи. Якщо пароль - це деякі дані, які користувач вводить безпосередньо в комп'ютер безпосередньо, тобто при його введенні, він не застосовує певні правила, які перетворюють введені дані в інші, то при введенні коду такі зміни відбуваються на рівні свідомості чи сприйняття. ці дані за допомогою комп’ютерної системи» [64].

Наприклад, введення кодового слова "базилік" при застосуванні правила введення цього слова в англійському режимі буде сприйматися комп'ютерною системою як "dfcbkm", оскільки розміщення кириличних та латинських літер на клавіатурі інакший.

«Отже, виходячи з визначення поняття "комп'ютерна інформація", програмне забезпечення та математичний захист, а саме паролі та коди доступу до комп'ютерних систем, а також комп'ютерна інформація та її носії, також повинні бути приписується предмету злочину за статтею 361 Кримінального кодексу України, оскільки вони:

1) відповідати характеристикам «комп’ютерна інформація»;

2) виконувати функцію захисту інших об’єктів зазначеного злочину» [13].

Системи безпеки, пов'язані із захистом апаратного та програмного забезпечення, слід трактувати як частину програмного забезпечення як частину комп'ютерної інформації.

У той же час, інші засоби захисту, які належать до суто апаратного захисту, та апаратно-програмне забезпечення з точки зору апаратного забезпечення залишаються поза увагою.

У разі апаратного захисту, а також у випадку апаратно-програмного захисту, вбудованого в сам комп’ютер, систему або комп’ютерну мережу, тобто якщо встановлені пристрої безпеки або

технічно пов'язані з комп'ютерами або системними терміналами, або комп'ютерною мережею, вони повинні розглядатися як технічні елементи комп'ютерів, їх систем та комп'ютерних мереж. Іншими словами, технічні (матеріальні) засоби захисту також слід визначати як один з інших розслідуваних суб'єктів злочину.

«Іншими словами, програмно-математичні та апаратно-програмні засоби в програмній частині захисту електронних комп’ютерів, їх комп’ютерних систем та мереж належать до свого роду комп’ютерної інформації; Апаратні та апаратно-програмні засоби захисту в апаратній частині належать до технічного обладнання електронних комп’ютерів, їх комп’ютерних систем та мереж» [7].

Деякі автори зазначають, що «файлова система повинна забезпечувати захист файлів від несанкціонованого доступу» [11].

Це говорить про те, що системи безпеки можуть бути розроблені для захисту як комп’ютерної інформації, так і засобів масової інформації.

РОЗДІЛ 2
ПОЧАТКОВИЙ ЕТАП РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ ТА ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

2.1. Особливості початкового етапу розслідування комп'ютерних злочинів

Ми можемо виділити інформацію, яка часто доступна слідчому на ранніх стадіях розслідування кіберзлочинності. Виходячи з цього, можна визначити початкову ситуацію. Сюди входять дані про:

1) зовнішній прояв злочину;

2) методи доступу до комп'ютерної системи та безпосередньо до носія інформації;

3) характер відповідної інформації;

4) особа, яка вчинила злочин.

Разом вони можуть сформувати такі типові початкові ситуації розслідування:

1. Немає фактів про втручання в комп'ютерну інформацію, яка циркулює в кредиті та фінансах, про інформацію про доступ до цієї інформації та про виконавців цього закону (це відбувається приблизно в 60% випадків).

2. Встановлено факти кримінального володіння комп'ютерними даними, і немає інформації про спосіб доступу та осіб, які вчинили злочин (10%).

3. Встановлено факти кримінального заволодіння комп'ютерними даними, для доступу до цієї інформації використано механічне втручання, а інформації про винних немає (10%).

4. Встановлено факти фальсифікації комп'ютерної інформації, і інформація про спосіб доступу та осіб, які вчинили це діяння, відсутня (10%).

5. Встановлені факти знищення інформації в комп’ютерній системі, і немає інформації про спосіб доступу та осіб, які вчинили акт (5%).

6. Визначено факти злочинного впливу на комп'ютерні дані (вилучення, підробка, знищення), а також інформацію про спосіб доступу та осіб, які вчинили злочин (5%).

Основою для розробки стандартних версій можна розглядати мету вчинення «комп’ютерного злочину». Можна виділити наступні основні цілі вчинення «комп’ютерного злочину»:

1) прагнення отримати суттєві вигоди від придбання майна у третіх осіб у вигляді: грошових коштів, інших матеріальних цінностей, конфіденційності інформації;

2) порушення авторських прав;

3) Порушення алгоритму передачі інформації, знищення або погіршення стану комп’ютерних програм та баз даних та їх носіїв інформації.

Виходячи з цього, ми можемо виділити типові слідчі версії «комп'ютерного» інциденту злочину, а саме:

1. «Комп'ютерні злочини» вчиняються з метою отримання матеріальної вигоди:

а) «Кіберзлочинність» - це втручання у викрадення коштів;

б) «комп’ютерний злочин» був скоєний з метою зловживання грошима групою осіб за попередніми змовами або організованою групою із залученням працівника установи; один із випробовуваних має гарні навички роботи з комп’ютером;

в) «комп’ютерний злочин» здійснено з метою викрадення працівника закладу, який має навички роботи з комп’ютерною технікою;

(г) «комп'ютерний злочин» з метою крадіжки вчинили злочинці, один з яких є комп'ютерно грамотним, без втручання персоналу закладу.

2. «Кіберзлочинність» здійснює порушення авторських прав:

а) «Комп'ютерне» порушення було вчинене з метою порушення авторських прав однієї або кількох осіб, які мають вільний доступ до комп'ютерної техніки.

б) «Комп'ютерний злочин» здійснюється з метою порушення авторських прав однієї або кількох осіб, які не мають вільного доступу до комп'ютерної техніки.

3. «Комп'ютерні злочини» вчиняються з метою порушення алгоритму обробки інформації, знищення або пошкодження комп'ютерних програм і баз даних та їх носіїв: (a) «комп'ютерний злочин» вчинено з метою порушення алгоритму обробки, знищення або пошкодження інформації особою, яка має доступ до комп'ютерного обладнання; (b) «комп'ютерний злочин» був скоєний з метою порушення алгоритму обробки, знищення або пошкодження інформації особою, яка не має доступу до комп'ютерного обладнання» [22];

в) Знищення, пошкодження або порушення алгоритму обробки інформації є наслідком несправності або несправності комп'ютеризованої системи і не є "комп'ютерним злочином".

У присутності підозрюваного головним завданням слідства є зафіксувати хід доказів за допомогою власника інформаційної системи, а саме встановити:

а) порушення цілісності (конфіденційності) інформації в системі;

б) розмір шкоди, заподіяної порушенням цілісності (конфіденційності) інформації;

в) причинно-наслідковий зв’язок між діяннями, що становлять метод порушення, та наслідками, що мали місце з деталями методу порушення цілісності (конфіденційності) інформації в системі та характером дій, скоєних підозрюваним;

г) ставлення винного до вчинених дій та наслідків, що виникають в результаті.

Якщо підозрюваний затриманий на місці злочину або відразу після його перевірки, ситуація характеризується такими заходами:

а) особистий обшук ув'язненого;

б) опитування затриманого;

(с) обшук будинку затриманого;

г) дослідження стану комп’ютерів, комп’ютерних мереж та машинних носіїв;

(д) співбесіди з очевидцями та особами, що керують інформаційною системою, включаючи посадових осіб;

е) тимчасове вилучення документів (як правило, за сприяння спеціаліста) документів, включаючи комп’ютерну допомогу, що фіксують стан інформаційної системи на момент вторгнення зловмисника або його програм та наслідки вторгнення.

Водночас мають бути вжиті заходи щодо фіксації стану робочого місця підозрюваного, де він увійшов до інформаційної системи та де можна зберегти сліди його дій.

У разі відсутності підозрюваного повинні бути вжиті заходи щодо пошуку місця, де відбувся злом в інформаційній системі.

З цією метою здійснюється пошук:

Місця входу в інформаційну систему та спосіб входу в систему;

"Шляхи" зловмисника або його програм до "атакованої" системи.

Зазвичай це можуть бути: робоче місце зловмисника у відділі або його будинку, а також інші місця, де встановлено відповідне обладнання.

Розслідуючи комп’ютерну злочинність та проводячи розслідування (обшуки), слід пам’ятати, що всі злочинні операції здійснюються за допомогою комп’ютерів і тому залишають сліди на магнітних носіях (жорстких дисках, компакт-дисках, флеш-картах

тощо). Своєчасне виявлення ІТ-обладнання та інструментів, а також належне їх утилізація визначають ефективність подальших технічних досліджень ІТ, спрямованих на вилучення та консолідацію інформації, що зберігається на магнітних носіях, і тим самим виявлення цих слідів злочинної діяльності.

Під час розслідування кіберзлочинності найбільш обґрунтованими є такі обставини:

Вчинити комп’ютерний злочин;

Місце злочину;

Час злочину;

Надійність засобів захисту комп’ютерної інформації;

спосіб вчинення злочину;

Люди, які вчинили злочин;

Вина та мотиви винного;

Обставини, що впливають на тяжкість злочину, а також обставини, що характеризують особу підозрюваного, пом'якшують і посилюють покарання

Характер та розмір шкоди, заподіяної злочином;

Обставини, що сприяли злочину.

2.2. Проведення окремих слідчих (розшукових) дій під час розслідування комп’ютерних злочинів

Попередній перегляд місця події. Обов’язковими підготовчими заходами, які будуть проведені перед відвідуванням місця, є:

Отримувати інформацію про подію від поінформованої особи (де, коли, з яких причин їм стало відомо про кіберзлочинність, яка вже була скоєна або що відбувається, хто виявив ці сигнали, хто повідомив про подію);

Інформування про подію та виклик працівників відповідних зацікавлених підрозділів (наприклад, СБУ);

Вживати заходів для підтримання ситуації та цілісності комп’ютерної системи та запобігання спробам проникнення в приміщення, що підлягають огляду (відмова у наданні допомоги працівникам відповідної організації, блокуванні та охороні приміщень тощо);

Запрошення для участі в оцінці від експертів, бажано від зовнішніх організацій, та свідків. Враховуючи своєчасність цих злочинів та складність їх розкриття та розслідування, бажано мати заздалегідь складений список фахівців, які можуть надати реальну допомогу у розслідуванні.

Підготовка науково-технічних джерел. Для оперативного контролю носіїв даних для машин портативні комп'ютери повинні бути включені в структуру науково-технічних засобів. За допомогою сучасних технологій ви можете записувати відео, робити знімки та перетворювати їх у цифрову (комп’ютерну) форму, при цьому якість зображення залишається незмінною, тобто не змінюється. не погіршується навіть при кількох копіях. Тому спеціально підібране програмне забезпечення також є важливою частиною науково-технічних ресурсів, необхідних для досліджень.

Після прибуття на сайт є:

Перевірка ефективності блокування та захисту будівель, видалення всіх третіх осіб;

знати кількість кімнат, обладнаних комп’ютерною технікою, їх розташування та розподіл у різних кімнатах;

Опитування осіб, які виявили наслідки кіберзлочинів або працівників комп'ютерної безпеки (якщо це можливо);

Планування рецензування (визначення порядку та порядку власних дій та дій рецензентів).

Перевірку комп'ютерного обладнання слід починати з пошуку відбитків пальців на клавіатурі, ручного маніпулятора (миші), комп'ютерної периферії, кнопок "скидання" та "живлення" на центральному блоці.

Обов’язково запишіть стан свого комп’ютера та периферійних пристроїв (увімкнено чи вимкнено) у звіті про сканування. Вкажіть операційну систему, встановлену на комп’ютерах.

При огляді місця події за участю спеціаліста необхідно:

Вивчити журнали подій системи, файли обліку доступу до комп'ютерної системи, файли паролів, списки доступу до маршрутизатора, журнали системи виявлення вторгнень, журнали веб-серверів, DNS-сервери, поштові сервери, сервери баз даних, модеми xDSL;

можливість модифікувати, усунути або мінімізувати систему, що розслідується;

Зафіксувати якомога більше всіх дій кіберзлочинця шляхом створення файлів доказів, виявлення всього встановленого програмного забезпечення та створення файлу з контрольними сумами всіх виявлених та створених речових доказів;

Зареєструйте всі створені файли доказів, розпізнане програмне забезпечення та файли контрольної суми виключно на одному носії, що записується (CD-R, DVD-R).

Запакуйте носії інформації згідно з криміналістичними рекомендаціями.

Вислухати свідків. Готуючись до допиту, слідчий може заручитися допомогою комп’ютерного вченого, пояснення та інструкції якого допоможуть повністю зрозуміти природу злочину, що розслідується, з тим щоб можна було краще встановити обсяг слідчих обставин.

Щоб підготуватися до співбесіди, ви повинні:

виявити характеристики злочину, зокрема питання, що стосуються технічних аспектів підготовки та виконання санкційних планів;

Визначте обставини, які потребують з’ясування. Сюди може входити інформація про жертву, технічні та конструктивні особливості розглянутої комп’ютерної системи, комп’ютерне обладнання, що використовується винним тощо.

формулювати найскладніші запитання;

За необхідності підготуйте докази або інші матеріали, які можна виявити під час допиту, забезпечуючи необхідний рівень захисту; Зверніть особливу увагу на підготовку науково-технічних засобів для фіксації ходу слідчого заходу (розслідування).

Опитуючи свідків, ви завжди повинні зазначити:

якщо когось цікавить комп’ютерна інформація, програмне забезпечення, комп’ютерне обладнання компанії, організації, установи, компанії чи корпорації;

чи є сторонні особи в районі, де зберігається комп’ютерна інформація, чи були випадки, коли працівники працюють з інформацією, що виходить за межі їх компетенції

чи були помилки програмного забезпечення, крадіжки носіїв інформації та окремі обчислювальні пристрої;

якщо є помилки в роботі комп’ютерної техніки, електронних мереж та засобів захисту комп’ютерної інформації;

Хто з працівників працював понаднормово і цікавився інформацією, не пов’язаною з їх безпосередньою діяльністю?

чи не було останніх випадків захисту комп'ютерної інформації;

Як часто програми скануються на віруси? Які результати останніх сканувань?

як часто програмне забезпечення оновлюється, як воно купується;

як купується комп’ютерна техніка, як її ремонтують та модернізують;

як компанія, організація, установа чи компанія використовує інформацію, як її отримують, обробляють та надсилають за каналами зв'язку;

Кожен, хто в іншому випадку є учасником комп’ютерної мережі, до якої підключені комп’ютери компанії, організації, установи чи компанії, має як доступну мережу дозвіл цих користувачів працювати в мережі, працювати з інформацією;

як захищається комп’ютерна інформація, які засоби та методи використовуються для її захисту тощо.

Пошук. Для підготовки до навчання вам знадобиться:

знати, яка комп’ютерна техніка знаходиться в приміщенні, де проводиться обшук, і скільки її;

визначте, чи використовує ваш комп’ютер автономне чи джерело безперебійного живлення, і якими наслідками може призвести до збою живлення;

Запросіть спеціаліста з комп'ютерних систем, оскільки його знання необхідні для підготовки дослідження та швидкого аналізу інформації та кваліфікованого вилучення комп'ютера;

Підготовка відповідного комп'ютерного обладнання для читання та зберігання видаленої інформації;

вивчити особу власника комп’ютера, знати його професійні навички, пов’язані з комп’ютерною технікою;

визначити, коли проводити пошук та які заходи вжити для забезпечення конфіденційності;

Спрогнозуйте тип інформації, яка може знаходитися в комп’ютері, її роль у її швидкому та ефективному отриманні, визначивши, яку інформацію про комп’ютер слід вивчити на місці, а яку видалити для подальшого дослідження.

Перше, що потрібно зробити під час досліджень, - це захист комп’ютерів. Не дозволяйте нікому заходити в кімнату. Пам’ятайте, що зміна або видалення інформації може бути спричинене не лише використанням клавіатури, але й увімкненням та вимкненням комп’ютера. Отже, якщо комп’ютер був увімкнений під час входу, його повинен увімкнути професіонал. Всі роботи на комп’ютері повинен проводити фахівець.

Щоб перевірити обладнання комп'ютера, виконайте такі дії:

1) Перевірте, чи комп'ютери в кімнаті підключені до локальної мережі.

2) визначити, чи підключений комп’ютер до обладнання чи комп’ютерів поза приміщеннями, де проводиться пошук;

3) перевірити, чи підключений комп'ютер до модему;

4) Визначте, чи і які програми працюють на комп’ютері. Для цього вивчіть зображення на екрані та опишіть його якомога детальніше в протоколі. Якщо виявиться, що під час операцій трасування (розслідування) на комп'ютері, що запускає програму, необхідно вжити заходів для припинення її роботи;

5) Визначте, чи є на комп’ютері якась інформація, яка може допомогти у розслідуванні. Це може побачити лише професіонал, вивчивши інформацію на жорсткому диску.

Для розслідування кіберзлочинів потрібен не лише висококваліфікований фахівець з комп’ютерних систем, а й вся робоча група з розслідування. На додаток до спеціальних дій з комп’ютером, такий пошук вимагає чіткої організації пошукової діяльності для виявлення кеш-пам’яток, які можуть містити загальні документи та предмети. Системний блок комп'ютера також може бути кешем. Він має ряд структурних особливостей, що полегшують його зберігання. По-перше, в процесорі багато вільного місця. По-друге, завдяки модульній структурі центрального комп'ютерного блоку його дуже зручно та

швидко розбирати та збирати, як правило, без додаткового обладнання. Це полегшує безслідний доступ до комп'ютерних компонентів. По-третє, комп'ютер використовує електронні схеми низької напруги, які не загрожують життю. Таким чином ви можете відкрити корпус, не відключаючи його від електромережі. По-четверте, материнська плата кріпиться до стінки корпусу, між якими є досить великий простір, що дуже зручно для зберігання документів. Доступ до такого кешу для фахівця простий.

Більшість інформації, що зберігається та обробляється комп’ютером, все ще може бути скопійована на знімні носії - лазерні диски, флеш-карти тощо. Інформаційні носії інформації можуть бути вилучені, а документи про кримінальні справи можуть бути додані як докази.

Через неможливість швидкого аналізу великої кількості інформації на комп’ютері її потрібно видалити для подальшого розслідування. Ви можете скопіювати інформацію на жорсткий диск ПК дослідницької групи. Якщо у вас немає переносного ПК у робочій групі, просто вийміть жорсткий диск розпізнаного комп'ютера або весь центральний процесор комп'ютера.

Допит підозрюваного. Щоразу, коли ви допитуєте людину як підозрюваного, ви повинні відповісти принаймні на такі запитання:

1. Де і ким (у якій позиції) працює підозрюваний?

2. До яких комп’ютерних даних він має доступ? Які інформаційні операції він може виконувати? Яка категорія його доступу до інформації?

3. Чи може підозрюваний працювати на комп’ютері? Може бути?

4. Які ідентифікаційні коди та паролі йому присвоюються (також при роботі в комп’ютерній мережі)?

5. До яких типів програмного забезпечення має доступ підозрюваний?

6. З якого джерела або від кого підозрюваний конкретно дізнався зміст інформації, до якої він отримав незаконний доступ?

7. Як підозрюваний потрапив у комп'ютерну систему (мережу)?

8. Де підозрюваний знайшов пароль (код) для доступу до інформації?

9. Чи є обмеження доступу до будинків, де встановлено комп'ютерне обладнання?

10. Чи знає він робочий процес з інформацією та інструкціями щодо робочого процесу?

11. Чи отримував підозрюваний пропозиції від незнайомців щодо передачі комп'ютерних даних чи програмного забезпечення?

Провести судово-медичне розслідування. Для допомоги у прийнятті рішень щодо технічного огляду ІТ-обладнання задаються такі запитання:

1. Яка комп'ютерна модель представлена для дослідження, якими технічними властивостями та периферійними параметрами вона володіє?

2. Чи справний комп'ютер? Чи можна змусити його працювати? Якщо ні, то в чому причини?

3. Чи відповідає подана документація цьому технічному та периферійному обладнанню?

4. Які умови складання комп'ютера та його компонентів: складання торгової марки, складання компонентів від іншої компанії чи ручне складання?

5. Чи певна периферія комп'ютера несправна?

6. Чи адаптований комп'ютер для конкретних користувачів (лівшів, людей із вадами зору тощо)?

Наступні проблеми можна вирішити при дослідженні даних та програмного забезпечення:

Який тип операційної системи використовує ваш комп’ютер? Яка його версія?

Яке програмне забезпечення працює на цьому комп’ютері? Вони є ліцензійними чи "незаконними" копіями, або власними оригінальними зразками? Коли ви встановили ці програми?

Для чого використовуються програмні продукти? Для яких програм вони призначені? Які методи введення та виведення використовуються? Чи відповідають результати програм необхідним заходам?

Які методи програмного забезпечення для захисту інформації (паролі, ідентифікатори, програми безпеки тощо) використовуються?

Чи були зроблені спроби відновити пароль чи інші спроби незаконно порушити роботу комп’ютерів (комп’ютерів), комп’ютерних систем та мереж?

Яку інформацію містять приховані файли?

Чи видалені (знищені) файли на пропонованому магнітному носії? Якщо так, то які їх імена, розміри та дати створення, строк позовної давності для знищення?

Чи можу я відновити раніше видалені файли та який їх вміст?

Чи змінився вміст файлів (будь ласка, вкажіть), якщо так, що сталося?

У якому вигляді знаходиться інформація про результати роботи антивірусних програм, програм для перевірки контрольних сум збережених файлів? Який зміст цієї інформації?

ВИСНОВКИ

Проведене дослідження дає можливість зробити наступні висновки:

1. Процедура (правила) доступу до комп’ютерної інформації – це сукупність конкретних правил, встановлених власником (користувачем) комп’ютерної інформації, правил доступу до комп’ютерної інформації або їх використання (цитування, копіювання) та обробки (модифікація), видалення, знищення).

2. Безпосереднім об'єктом злочину "Навмисне розповсюдження шкідливих комп'ютерних програм" є право власника (користувача) на безпеку програмного та апаратного забезпечення комп'ютерних систем,що гарантує цілісність комп'ютерної інформації, її засоби масової інформації та належне функціонування комп’ютерних систем.

3. Іншим суб’єктам злочину, передбаченого ст. 361 Кримінального кодексу України, включають комп’ютери, їх системи, комп’ютерні мережі, комп’ютерну інформацію, носії для такої інформації та засоби програмного забезпечення та математичного захисту комп’ютерної інформації. Комп’ютер - це сукупність апаратного та програмного забезпечення, призначеного для автоматичної обробки інформації, частково керованої оператором.

4. Предметом злочину «Несанкціонований доступ до комп’ютерної інформації» є комп’ютерна інформація.

5. Жертвами незаконного втручання у функціонування комп'ютерних систем повинні бути особи, які зазнали матеріальної або моральної шкоди внаслідок несанкціонованого доступу до комп'ютерної інформації, що належить їм як власнику чи користувачеві, або від навмисне розповсюдження комп'ютерних матеріалів, що належать їм, на однакових правах. комп’ютерна система або комп’ютерний носій шкідливих комп’ютерних програм.

6. З об'єктивної точки зору юридичний склад злочину «Несанкціонований доступ до комп’ютерної інформації» вчиненням можна охарактеризувати характеризується як скоєння будь-якого активного акту несанкціонованого доступу до комп'ютерної інформації, виникненням одного з інші соціально небезпечні наслідки у вигляді витоку, спотворення або знищення комп'ютерної інформації та причинного зв'язку між діями та наслідками. Склад цього злочину важливий. Злочин вважається закінченим з моменту настання одного із соціально небезпечних наслідків.

7. Об'єктивний аспект правового складу правопорушення "Навмисне розповсюдження шкідливих комп'ютерних програм" відноситься до активних актів навмисного розповсюдження комп'ютерних вірусів або іншого шкідливого програмного забезпечення, що може спотворити або знищити комп'ютерну інформацію або її дані. опори. Іншими словами, злочин є формальним і вважається закінченим з моменту розповсюдження комп’ютерного вірусу або іншого шкідливого програмного забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації //Юридична Україна. – 2004. – № 7 (19). – С.64 – 68.

2. Азаров Д. Порушення роботи автоматизованих систем – злочин в сфері комп'ютерної інформації //Право України. – 2001. – № 12. – С.72 – 74.

3. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. канд. юрид. наук. – К., 2002. – 18 с.

4. Антонов С. Компьютерные преступления в банковской сфере //Юридическая практика. – 1997. – № 8. – С. 7 – 9.

5. Архів Дарницького районного суду м. Києва: Кримінальна справа № 1-503, вирок від 16.01.2001 р.

6. Ахтирська Н. Про удосконалення кримінального законодавства України в сфері боротьби з кіберзлочинністю //htth://www.crime-research.org

7. Баранов О. Кримінологічні проблеми комп'ютерної злочинності //Інформаційні технології та захист інформації: Зб. наук. праць. – Запоріжжя: Юридичний інститут МВС України, 1998. – Вип. 2. – С.64 – 69.

8. Баранов О. Уголовная ответственность за компьютерные преступления //Безопасность информации. – 1996. – № 2. – С.4 – 9.

9. Баранов О. Цифрове законодавство //Дзеркало тижня. – 2002. – № 0. – 7 черв.

10. Батурин Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991. – 271 с.

11. Бачило И.Л., Семилетов С.И. Основные направления организационно-правового регулирования использования глобальных

сетей, включая Интернет /Информационное право: информационная культура и информационная безопасность. Материалы Всероссийской научно-практической конференции Санкт-Петербургского гуманитарного университета профсоюзов, 17 – 19 октября 2002 г. – С.90 – 100.

12. Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження /Вертузаєв М.С., Голубєв В.О., Котляревський О.І., Юрченко О.М.; Під заг. ред. О.П.Снігірьова. – Запорізький юридичний інститут МВС України, Національна академія внутрішніх справ України. – Запоріжжя : ПВКФ "Павел", 1998. – 315 с.

13. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навч. посіб. – К.: Українська академія внутрішніх справ, 1994. – 72 с.

14. Бурчак Ф.Г. Квалификация преступлений. Изд. 2-е, доп. – Киев.: Изд-во полит. лит-ры Украины, 1985. – 119 с.

15. Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України . – 1998. - № 1. – С. 101 – 103.

16. Гавловський В.Д., Романюк В.С. Проблеми організації боротьби з правопорушеннями, що вчиняються з використанням сучасних інформаційних технологій //Публікації Центру дослідження проблем комп'ютерної злочинності. – www/crime-recearch.org/library/Gav-Rom-Cim.htm

17. Гавловський В.Д., Цимбалюк В.С. Кіберзлочинність як чинник державної інформаційної політики України //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвід. наук.-дослід. центр. – 2002. – № 5. – С. 106 – 116.

18. Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України //Юридичний журнал. – 2004. – № 1 (19). – С. 132 – 134.

19. Голубєв В. Комп'ютерна злочинність //Юридичний вісник України. – 2002. – № 6 (9). – С. 1 – 4.

20. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю //Право України. – 2002. – № 5. – С. 121 – 126.

21. Гуцалюк М. Протидія комп'ютерній злочинності //Право України. – 2003. – № 6. – С.114 – 117.

22. Гуцалюк М. Протидія міжнародній комп'ютерній злочинності //Вісник прокуратури. – 2003. – № 9 (27). – С.60 – 64.

23. Гуцалюк М. Хроніка вірусної атаки на Укртелеком //htth://www.ukrtel.net

24. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. – К.: Держстандарт України, 1994.

25. Духов В.Е. Экономическая разведка и безопасность бизнеса. – Киев: ИМСО МО Украины, НВФ "Студцентр" , 1997.

26. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): Автореф. дисс. д-ра юрид. наук, – Институт государства и права им. В.М.Корецкого. – Киев, 1992. – 23 с.

27. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине //Международный научно-практический правовой журнал "Закон и жизнь". – 2004. – № 7 (152). – С.29 – 32.

28. Колесник В.А. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

29. Комиссаров В.И. Теоретические проблемы следственной тактики. – Саратов: Изд-во Сарат. гос. ун-та, 1987. – 129 с.

30. Кримінальний кодекс України. *Відомості Верховної Ради України (ВВР)*, 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2491 (дата звернення: 1.09.2020 р.).

31. Кримінальний процесуальний кодекс України. *Відомості Верховної Ради України (ВВР)*, 2013, № 9-10, № 11-12, № 13, ст. 88. URL:

https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 1.09.2020 р.).

32. Кудрявцев В.Н. Общая теория квалификации преступлений. – 2-е изд., перераб. и дополн. – М.: Юристъ, 2001. – 304 с.

33. Курс Советского уголовного права: В 5 т. – Л.: Изд-во Ленинград. ун-та., 1968. – Т. 1. – 645 с.

34. Курс уголовного права. Общая часть. Т. 1: Учение о преступлении: Учеб. для вузов / Под ред. Н.Ф.Кузнецовой, И.М.Тяжковой. – М.: Зерцало, 1999. – 592 с.

35. Левиашвили М.Ш. Объект уголовно-правовой охраны и его значение для классификации преступлений //Уголовно-правовые исследования: Сб., посвящ. 80-летию со дня рожд. Т.В.Церетели. – Тбилиси: Мецниереба, 1987. – С.94 – 103.

36. Мінченко А.В. Правова інформатика. Інформатика в історичному аспекті: Навч. посіб. – К.: Арістей, 2003. – 296 с.

37. Мотлях О.І. Захист інформації у комп'ютерних системах: актуальність та новизна підходів //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2001. – № 1(10). – С. 57 – 62.

38. Мотлях О.І. Інформаційна безпека: пріоритетні напрями, шляхи розвитку та вдосконалення //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2000. – № 1 (5). – С. 40 – 45.

39. Науково-практичний коментар до Кримінального кодексу України. /За заг. ред. М.О.Потебенька, В.Г.Гончаренка. – К.: Форум, 2001. У 2-х ч. Особл. част. – 942 с.

40. Науково-практичний коментар до Кримінального кодексу України: За станом законодавства і Постанов Пленуму Верховного суду України на 1 грудня 2001 р. /За ред. С.С. Яценка. – К., 2002. – 936 с.

41. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001р. / За ред. М.І.Мельника, М.І.Хавронюка. – К., 2001. – 1104 с.

42. Овчинский В.С. Интерпол в вопросах и ответах. – М.: ИНФРА – М., 2001. – С. 135 – 136.

43. Про авторське право і суміжні права : Закон України від 23.12.1993 р. *Відомості Верховної Ради України (ВВР)*. 1994. № 13. Ст.64.

44. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України 5.07.1994 р. *Відомості Верховної Ради України* (ВВР), 1994, № 31, ст.286.

45. Про інформацію : Закон україни від 2.10.1992 р. *Відомості Верховної Ради України (ВВР)*. 1992. № 48. ст.650.

46. Про науково-технічну інформацію : Закон України від 25.06.1993 р. *Відомості Верховної Ради України (ВВР)*, 1993, № 33, ст.345.

47. Про Національну програму інформатизації : Закон України від 1.01.2001 р. *Відомості Верховної Ради України (ВВР)*, 1998, № 27-28, ст.181.

48. Про Положення про технічний захист інформації в Україні : Указ Президента України від 7.09.1999 р. *Офіційний вісник України* від 15.10.1999. № 39, стор. 28, код акта 11180/1999 р.

49. Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / http:// mndc. naian. kiev. ua

50. Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / http:// mndc. naian. kiev. ua

51. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю. Автореф. дис… канд. юрид. наук: Нац. юрид. академія. – Харків, 2002. – 21 с.

52. Розенфельд Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів) //Вісник прокуратури. – 2002. – № 4(16). – С.23 – 27.

53. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Дисс. канд. юрид. наук. – К., 2003. – 200 с.

54. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Дисс. канд. юрид. наук. – К., 2003. – 200 с.

55. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1982. – 1600 с.

56. Старченко Ю.О. Окремі аспекти протидії "хакерській" діяльності в Україні //Інформаційний бюлетень. – 2000. – № 2. – С. 40 – 41.

57. Старченко Ю.О. Окремі аспекти протидії "хакерській" діяльності в Україні //Інформаційний бюлетень. – 2000. – № 2. – С. 40 – 41.

58. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков: Вища школа, 1998. – 196 с.

59. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков: Вища школа, 1998. – 196 с.

60. Тищенко Є.Ф., Селюк А.В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

61. Тищенко Є.Ф., Селюк А.В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

62. Уголовное право. Общая часть /Отв. ред. И.Я.Козаченко, З.А.Незнамова. – М.: Издательская группа ИНФРА-НОРМА, 1997. – 516 с.

63. Янішевський Д.О. Встановлення відповідальності за "комп'ютерні злочини" //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвідомчий науково-дослідний центр. – 2002. – № 5. – С.117 – 123.

64. Янішевський Д.О. Встановлення відповідальності за “комп’ютерні злочини” //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвідомчий науково-дослідний центр. – 2002. – № 5. – С.117 – 123.