МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІННОВАЦІЙНИХ ОСВІТНІХ ТЕХНОЛОГІЙ

КАФЕДРА КРИМІНАЛЬНОГО ПРАВА І ПРОЦЕСУ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_ Лихова С.Я.

«\_\_» \_\_\_\_\_\_\_\_\_ 2020 р.

**ДИПЛОМНА РОБОТА**

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ

«Правознавство»

**Тема: «Основи розслідування злочинів в галузі комп’ютерних технологій»**

Виконавець: Кернична Христина Сергіївна

Керівник: к.ю.н. Григоренко Артем Олегович

**Київ-2020**

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інноваційних освітніх технологій

(Юридичний факультет)

Кафедра кримінального права і процесу

Освітньо-професійна програма «Правознавство»

ЗАТВЕРДЖУЮ

Завідувач кафедри

С.Я. Лихова

«\_\_» \_\_\_\_\_\_\_\_\_ 2020 р.

**ЗАВДАННЯ**

**на виконання дипломної роботи**

Керничної Христини Сергіївни

1. Тема роботи «Основи розслідування злочинів в галузі комп’ютерних технологій» затверджена наказом ректора від «22» листопада 2019 р. № 2701/ст.

2. Термін виконання роботи: з 25 листопада 2019 р. по 29 лютого 2020 року

3. Вихідні дані роботи: монографічна наукова література, нормативно-правові акти, нормативно-правові акти міжнародного характеру, узагальнення судової практики.

4. Зміст пояснювальної записки: аналітичний огляд юридичних джерел з тематики диплому. Дослідження особливостей розслідування злочинів в галузі комп’ютерних технологій на основі аналізу чинного законодавства України, наукової літератури та статистичних даних.

5. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| №  пор | Завдання | Термін виконання | Відмітка про виконання |
| 1 | Вибрати тему дипломної роботи | до 20.11.2019 |  |
| 2 | Затвердити тему і план роботи у наукового керівника | до 26.11.2019 |  |
| 3 | Визначити статистичну,інформаційну базу дослідження скласти бібліографію | до 19.12.2019 |  |
| 4 | Оформити і обговорити з науковим керівником перший розділ роботи | до 14.01.2020 |  |
| 5 | Оформити і обговорити з науковим керівником другий розділ роботи | до 21.01.2020 |  |
| 6 | Оформити і обговорити з науковим керівником третій розділ роботи | до 31.01.2020 |  |
| 7 | Доопрацювати роботу, оформити її кінцевий варіант | до 03.02.2020 |  |
| 8 | Отримати відгук керівника та рецензію | до 11.02.2020 |  |
| 9 | Підготувати доповідь на захист | до 20.02.2020 |  |

6. Консультанти з окремих розділів

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Консультант  (посада, П.І.Б.) | Дата, підпис | |
|  |  | Завдання видав | Завдання прийняв |
| Консультанти з окремих розділів не залучались | | | |

7. Дата видачі завдання: 25.11.2020 р.

Керівник дипломної роботи \_\_\_\_\_\_ к.ю.н. Григоренко Артем Олегович

(підпис)

Завдання прийняв до виконання \_\_\_\_\_\_\_ Кернична Христина Сергіївна

(підпис)

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Основи розслідування злочинів у галузі комп’ютерних технологій»: 87 сторінок, 100 використаних джерел.

КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ; КІБЕРЗЛОЧИН; ІНФРОРМАЦІЯ; ЕОМ; РОЗСЛІДУВАННЯ ЗЛОЧИНІВ; ПРОЦЕСУАЛЬНІ ЗАХОДИ.

**Метою дипломної роботи** є здійснення поглибленого аналізу і подальшого розвитку існуючих теоретичних та практичних напрацювань вітчизняних спеціалістів у галузі розслідування злочинів пов’язаних з комп’ютерними технологіями.

**Об’єкт дослідження** – злочини у галузі комп’ютерних технологій, а також суспільні відносини, що пов’язані з їх вчиненням.

**Предмет дослідження** – механізм вчинення комп’ютерних злочинів, закономірності виникнення слідів та діяльность з їх розслідування.

**Методи дослідження**. Методологічною основою дипломної роботи є сукупність сучасних методів наукового пізнання. Для дослідження історичного розвитку законодавства був використаний метод історичного пізнання. Порівняльний метод надавав можливість дослідити досвід зарубіжних країн у боротьбі з кіберзлочинами. Для вивчення та аналізу судової практики був використаний метод аналізу та розслідування.

**Наукова робота дослідження:** обґрунтовано необхідність вдосконалення чинного законодавства, яке ускладнює ефективно протидіяти правопорушення, вчинені у галузі використання комп’ютерних технологій.

**Практичне значення** одержаних результатів полягає у виробленні пропозицій до чинного законодавства України з метою протидії злочинам у галузі комп’ютерних технологій, а також окремих методів в розробці працівників судових і правових органів.

**Зміст**

**Вступ……………………………………………………………………………………5**

**Розділ 1. Поняття та історіографія розвитку злочинів у галузі комп’ютерних технологій………………………………………………………………………………8**

1.1. Історія виникнення і сучасний стан…………………………….………………...8

1.2. Поняття злочинів у галузі комп’ютерних технологій…………….…………...14

**Розділ 2. Загальна характеристика злочинів в галузі комп’ютерних технологій……………………………………………………………….…………….21**

2.1. Кримінально-правова та криміналістична характеристика у галузі комп’ютерних технологій……………………………………………….……………21

2.2. Класифікація та види злочинів з галузі комп’ютерних технологій……….…..33

**Розділ 3. Особливості розслідування злочинів в галузі комп’ютерних технологій………………………………………………………………………….….51**

3.1. Початковий етап розслідування злочинів у галузі комп’ютерних технологій……………………………………………………………………….……..51

3.2. Особливості проведення окремих слідчих дій злочинів………………………58

**Висновки……………………………………………………………………………...74**

**Список використаних джерел…………………………………………….………..80**

**ВСТУП**

**Актуальність теми.**

Однією з найважливіших функцій держави є забезпечення інформаційної безпеки в Україні, адже уявити сучасне суспільство без використання комп’ютерних програм неможливо, оскільки їх значимість невпинно зростає. На сьогоднішній день стан злочинності вимагає розробки та застосування заходів для запобігання злочинним у сфері комп’ютерних технологій (далі - КТ).

Якщо говорити про Україну, вона суттєво відстає у розвитку від країн-учасниць Конвенції про кіберзлочинність, а саме, внаслідок соціально-економічних проблем. Кібервійни, кібертероризм, кібершпигунство стали звичними, тому злочинність у інформаційній сфері є суттєвою загрозою національній безпеці у сфері економіки.

Зареєстрований масив злочинів у сфері КТ свідчить про суттєве зростання рівня цих злочинів за останні роки і має такі показники:

* у 2013 році було обліковано 595 злочинів;
* у 2014 році – 443, у 2015 році – 598;
* у 2016 році – 865, у 2017 році – 2573;
* у 2018 році – 2301 злочин.

Особливо важливим є питання розробки належного законодавчого рівня захисту як на національному так і на міжнародному рівнях. Тому що нові види злочинної діяльності породжує будь-яка нова технологія, відповідно кожен новий тип злочинів вимагає нових заходів захисту і методів роботи правоохоронних органів.

Стрімкий розвиток інформатизації в Україні несе в собі потенційну можливість використання комп'ютерних технологій з вигодою для злочинця.

Сьогодні одне з найактуальніших питань злочинів у сфері КТ - який вид охорони комп’ютерних програм є найефективнішим та який тип захисту краще.

У наш час економічний розвиток неможливий без розвитку КТ, тому з метою заохочення виробників комп’ютерного програмного забезпечення законодавці повинні забезпечити правовий захист та забезпечити належну безпеку прав власникам та розробникам таких програм. Належний правовий захист принесе користь не тільки виробникам, які отримають не лише моральні права, але й економічні вигоди для створення програм. Крім того, впровадження цих технологій на законних засадах у всіх державних секторах принесе користь для всіх громадян.

Розвиток суспільства та економіки у ХХІ столітті неможливий без розвитку технологій. Надзвичайно важливо дослідити вже існуюче законодавство, судову практику злочинів у галузі КТ.

Отже, потрібно докладати всіх зусиль для створення такого механізму захисту, який би повністю забезпечував захист від комп'ютерної злочинності, та був би ефективним як сьогодні, так і через пару років, враховуючи швидкий розвиток нових технологій.

Разом з тим, с ще багато не врегульованих проблем, які не дають можливості ефективно протидіяти правопорушенням, що вчиняються у сфері використання КТ.

В контексті появи транснаціональної комп'ютерної злочинності і кібертероризму особливо гостро постає питання забезпечення інформаційної безпеки, як однієї з важливих складових національної безпеки держави.

**Мета дослідження** полягає у визначенні особливостей, притаманних кримінально-правовій кваліфікації злочинів у сфері КТ і пошук способів вдосконалення законодавства у цій галузі, а також шляхів, що дадуть можливості для ефективного впровадження цих норм на практиці. Вивчення поняття, види злочинів у сфері КТ та визначення системи її правового захисту на різних етапах розслідування. Також дослідження деяких існуючих проблем та пошуку шляхів для їх вирішення. У цьому дослідженні однією з цілей є аналіз існуючих наукових праць, статей, рефератів у галузі комп’ютерної злочинності.

Для досягнення поставленої мети вирішувалися такі **завдання**:

* визначити поняття та види злочинів у сфері комп’ютерних технологій;
* проаналізувати класифікацію кіберзлочинності за міжнародним та національним законодавством;
* висвітлити кримінально-правову та криміналістичну характеристика;
* визначити початковий етап розслідування злочинів у галузі КТ;
* знайти шляхи вирішення, які допомогли б удосконалити чинне законодавство здійснення злочинів у галузі КТ;

**Об’єкт дослідження** – суспільні відносини, що виникають при здійсненні інформаційних процесів з приводу виробництва, збору, обробки, накопичення, збереження, пошуку, передачі, розповсюдження і споживання комп’ютерної інформації, а так само в інших сферах, де використовуються комп’ютери, комп’ютерні системи і мережі.

**Предмет дослідження**. Предметом даного дослідження є особливості кримінально-правової кваліфікації злочинів у сфері комп’ютерних технологій.

**Методи дослідження.** Методологічною основою дипломної роботи є сукупність сучасних методів наукового пізнання. Для дослідження історичного розвитку законодавства у галузі розслідування комп’ютерних технологій був використаний метод історичного пізнання. Порівняльний (компаративістський) метод надав можливість дослідити досвід зарубіжних країн у боротьбі з кіберзлочинами. Для вивчення та аналізу судової практики був використаний метод аналізу та узагальнення.

**Теоретична основа.** Дослідженню основ розслідування злочинів в галузі комп’ютерних технологій присвячено безліч наукових публікацій, книг, монографій, статей українських науковців та вчених із США та країн Європейського Союзу. Серед них, зокрема: Д. С. Азаров, Ю. М. Батурин, П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, А. Г. Волевоз, О. В. Демешко, І. В. Європіна, М. В. Карчевський, С. А. Кузьміна, О. В. Мазоліна, К. В. Манжула, В. М.Машкова, С. С. Мірошниченко, А. А. Музика. Питання незаконого втручання в роботу електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж відображена в публікаціях таких вчених як М. В. Рудика, В. П. Шеломенцева, М. П. Бікмурзіна, Т. В. Корнякова, В. В. Кузнецова, Є. В. Лащук, Є. І. Литвинов, Ю. М. Онищенко, П. І. Орлова, С. О. Орлов, О. Е. Радутний, Н. А. Розенфельд, В. С. Романюк, О. В. Смаглюк, Л. В. Сорока, В. С. Цимбалюк, С. В. Шапочка, Н. С. Юзікова, І. О. Юрченко, К. В. Юртаєва та інші.

Крім того, серед науковців, які займаються дослідженнями злочинів в галузі КТ варто виділити С. В. Шапочки «Запобігання шахрайству, що вчиняється з використанням комп’ютерних мереж» (2018 р.), у якій створено власну класифікацію шахрайства, що вчиняється з використанням комп’ютерних мереж, визначаються детермінанти та ступінь його латентності.

**Наукова новизна одержаних результатів.** Незважаючи на те, що на цю тему існує велика різноманітність науково-дослідних робіт, дані досліджень необмежені, особливо з урахуванням швидкого розвитку комп’ютерних технологій та законодавства, що регулює цю сферу.

Ознайомившись та переглянувши велику кількість праць на дану тему, варто зазначити , що праці де здійснюється порівняння комп’ютерних злочинів між законодавством України та ЄС немає. Більшість попередніх досліджень проводилися досить давно, тому враховуючи швидкість розвитку нових технологій, є необхідність дослідити це питання на сьогоднішньому етапі розвитку комп’ютерних технологій, щоб отримати висновок про сучасний стан законодавства у цій галузі.

**Практичне значення.** Це дослідження важливе як для теорії, так і для практичних аспектів протидії комп’ютерним злочинам. Що стосується практичного значення, то в цій роботі досліджено сучасні проблеми комп’ютерної злочинності та представлено ідеї, які можуть допомогти вирішити ці проблеми та удосконалити законодавство у цій сфері. Що стосується значущості теорії, в даному дослідженні проаналізовано сучасну основу теорій, досліджено діючі юридичні документи, а також наукові дослідження, статті, монографії, що може допомогти систематизувати існуючі теоретичні праці та надати можливість детального їх аналізу.

**РОЗДІЛ 1. ПОНЯТТЯ ТА ІСТОРІОГРАФІЯ РОЗВИТКУ ЗЛОЧИНІВ У ГАЛУЗІ КОМП’ЮТЕРНИХ ТЕХНОЛОГІЙ**

**1.1. Історія виникнення і сучасний стан**

Перша історична згадка про злочини в галузі КТ сягає давніх давен, про злочини цієї галузі згадувалося ще в п’ять тисяч шістсот вісімдесятому році до нашої ери у єгипетських літописах про так званих Чорних отруйників, які своїм жертвам згодовували розтерті в порошок рахункові палички так званий сучасний на той час персонального комп'ютера.

Більш наближена до наших часів згадка про таку категорію злочинів виникає коли в Сполучених Штатах Америки у 1945 році була створена перша Електронна обчислювальна машина (далі також «ЕОМ»), яка використовувалась для розшифровування німецьких військових телеграм, а згодом й для іншої діяльності.

Поняття «кіберзлочинність» з’явився в американській доктрині на початку 60-х років, коли були зафіксовані перші випадки злочинів, вчинених з використанням комп’ютерів. Тоді ж з’являються перші «хакери», ними стали студенти Масачусетського технологічного інституту, які практикувалися з програмами нового університетського комп’ютера [1, с. 294]. ЕОМ набули значного застосування, як серед працівників правоохоронних органів так і серед науковців, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [2, с. 17].

В1966 р. було зафіксовано перший випадок використання ЕОМ як засобу при пограбуванні банку в Міннесоті. Альфонсо Конфессоре став першою людиною, що постала перед американським судом у 1969 р. за використання ЕОМ для вчинення податкового злочину на суму 620 тис. доларів.

Подальша історія злочинів в сфері КТ, відмічена такими найбільш впливовими подіями:

* кінець 1970-х років - пограбування Секьюріті пасіфік банку більш ніж на десять мільйонів доларів;
* 1979 рік – розкрадання компютерів у Вільнюсі на суму майже 79 тисяч карбованців;
* 1984 рік - перший в світі комп’ютерний вірус;
* 1985 рік – зірване голосування в конгресі Сполучених штатів за допомогою комп’ютерного вірусу;
* 1986 - 1988 роки – перша поява комп’ютерного вірусу в Союзі Радянських Соціалістичних Республік;
* 1989 рік - блокування американським студентом близько 6 тисяч ЕОМ в Пентагоні;
* 1990 рік - в Голландії відбувся перший міжнародний з’їзд комп’ютерних піратів де демонструвалися можливості необмеженого втручання в системи ЕОМ;
* 1991 рік - викрадення коштів «ЗовнішЕкономБанку» на суму понад 125 тисяч доларів США;
* 1992 рік - умисне порушення роботи реакторів Ігналінської атомної електростанції;
* 1993 рік - шахрайство в Центробанку Росії з використанням КТ на суму майже в 70 мільярдів рублів;
* 1995 рік - спроба громадянина Росії пограбувати Сіті-банк на суму 2 мільйони 800 тисяч доларів [51, с. 133].

Перший злочин із використанням КТ в колишньому СРСР, було зареєстровано у 1979 році у Вільнюсі, ним стало розкрадання, збитки якого складали 78 тисяч крб. Цей злочин було занесено до міжнародного реєстру правопорушень подібного роду і він став своєрідним початком розвитку нового виду злочинів. [3, с. 126].

Проте заходів по протидії злочинам в сфері КТ, як таких ще не існувало. Створення заходів з комп’ютерної безпеки було поставлено на трохи пізніший час, після того, як студент Корнельського університету зміг увійти до комп’ютерних систем американської розвідки, міністерства оборони та відключив в цих системах кілька тисяч комп’ютерів. Це посприяло появі перших заходів протидії злочинам в сфері КТ, зокрема при університеті Карнегі Меллон у Пітсбурзі на кошти Пентагону була створена комп’ютерна група швидкого реагування — CERT (Computer Emergency Response Team), яка займалася реєстрацією великих зломів в сфері КТ і надання допомоги в «латанні» дірок, пророблених злочинцями [4, с. 96].

Перші спеціальні нормативно-правові акти по боротьбі зі злочинами в сфері КТ було прийнято у 1973 році у Швеції та у 1976 році у Сполучених Штатах Америки. Перші закони стосовно комп’ютерних злочинів прийняті у 70-80 роках майже усіма індустріально розвинутими країнами. Серед них Computer Fraud and Abuse Act 1984 року у США, які найбільше страждали від комп’ютерних злочинів. Пізніше і в інших країнах світу були прийняті закони стосовно цієї категорії злочинів. Активно в боротьбу з комп'ютерними злочинами вступили і міждержавні та громадські організації, але вдосконалення чинного законодавства не припиняється і сьогодні, що викликане активним розвитком інформаційних та комп’ютерних технологій [5].

Початок 21 століття характеризується активним впровадженням у світі комп’ютеризованих (автоматичних) інформаційно-технологічних систем у банківській, комерційній, виробничій та інших сферах. Це призводить до того, що головною і водночас невідкладною для вирішення проблемою стає розробка діючої системи захисту від несанкціонованого вторгнення. Зростання обсягів інформації йде паралельно з загостренням проблеми можливості несанкціонованого доступу до неї, цьому водночас активно сприяє розвиток функціонування глобальної комп’ютерної мережі «Internet». Віддаленість об’єкта, широка географія посягання (за сотні тисяч кілометрів від місця вчинення злочинної дії), проблеми з виявлення, доведення вини, а також високий прибуток від вчинення злочину в сфері КТ, зробили його одним з найбільш привабливих для псевдо фахівців злочинного світу.

В Україні у 1994 році були здійснені перші кроки з протидії кіберзлочинам, коли до Кримінального кодексу 1960 року було внесено зміни, якими в ст. 198-1 «Порушення роботи автоматизованих систем» уже передбачалося кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що спричинило перекручування чи знищення інформації або носіїв де ця інформація зберігалася, або розповсюдження програмних і технічних засобів, призначених для незаконного проникнення до автоматизованих систем і здатних спричинити перекручування або знищення інформації чи носіїв такої інформації.

В 2001 році був прийнятий Кримінальний кодекс України (КК України), відповідно до якого ця діяльність вийшла на якісно новий рівень.

Основні статті Кримінального кодексу України, за якими розслідуються кіберзлочини в Україні сьогодні:

* стаття 176 «Порушення авторського права і суміжних прав»;
* стаття 190 «Шахрайство»;
* стаття 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку»;
* стаття 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
* стаття 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації»;
* стаття 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»;
* стаття 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється»;
* стаття 3631 «Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку».

В Єдиному державному реєстрі судових рішень можна знайти декілька судових рішень винесених за результатами розгляду кримінальних справ, що стосуються вище зазначених статей.

На сьогодні в Україні та світі кожен рік вчиняються десятки тисяч злочинів із застосуванням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технологічних засобів та обладнання.

Кожен день у фізичних та юридичних осіб викрадають персональні дані, кошти з рахунків, збирають конфіденційну та комерційну інформацію, блокують діяльність та інше, але успішність протидії таким злочинним діям, їх виявлення та притягнення винних осіб до відповідальності зараз є достатньо рідкісним явищем, у порівнянні з кількісним обсягом таких правопорушень.

Це очевидно, оскільки кіберпростір – безграничний, а досвідчені хакери мають всі необхідні вміння та навички, щоб бути в ньому нерозпізнаваними. Кібератаки завдають шкоди не лише людям та компаніям, але й державам. Щороку у світі проходять тисячі заходів різних рівнів, щодо пошуку шляхів вирішення актуальних питань кібербезпеки. В мовлені країн постійно з’являються нові поняття: кіберрозвідка, кіберпростір, кібертероризм, об’єкт критичної інфраструктури, кібершпигунство тощо. Кібербезпека та боротьба з кіберзлочинами у 21 ст. – це одне з більш важливих тем, яка потребує глибокого вивчення, розробок та застосування високотехнологічних вирішень з метою запобігання та протидії злочинів в сфері КТ.

Шкода, яку завдає державам і окремим особах злочини в сфері комп’ютерних технологій, є дуже значна. На сімдесят третій сесії Генеральної асамблеї ООН генесекретар Антониу Гуттереш оцінив щорічні збитки від кіберзлочинів у світі в розмірі півтора трільйони доларів. Передбачення експертів з кібербезпеки в загальному не зовсім втішні. На майбутнє передбачається тенденція, що кількість злочинів та збитків завданих ними, лише зростатиме, оскільки зазвичай правопорушники йдуть на крок попереду методів, які державні органи та приватні особи застосовують, щодо запобігання і їх розкриттю.

Україна, як і решта країн, щодня зіштовхується з викликами у сфері кібербезпеки, лише за останні декілька років державні органи неодноразово були атаковані з кіберпростору. Однією з таких атак був 27 червня 2017 року різновиду вірусу Petya, який призвів до порушення роботи державних підприємств, установ, медіа, банків, та інших. Внаслідок чого було заблокована діяльність таких підприємств, як аеропорт «Бориспіль», «Укртелеком», ЧАЕС, «Укрпошта», «Укрзалізниця», «Ощадбанк», та багато інших великих організацій. Були також постраждалими інформаційні системи Міністерства інфраструктури, Кабінету міністрів, Київської міської державної адміністрації, сайт Львівської міської ради, кіберполіції та служби спецзв’язку України.

В Україні на законодавчому рівні приймаються відповідні нормативні акти, що покликані регулювати відносини у цій сфері. Станом на початок 2019 року до правової основи кібербезпеки України включені такі законодавчі акти, як: Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про основи національної безпеки України» та інші, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

В Україні напрямок, щодо кібербезпеки покладається на кілька державних органів, таких як Державна служба спеціального зв’язку та захисту інформації України, Національна поліція, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, НБУ. В кожному із вище зазначених органів є своя структура, яка складається з низки підрозділів.

За інформацією голови Департаменту кіберполіції, щорічно кількість злочинів в сфері КТ зростає в середньому на дві з половиною тисячі. Відповідно до звіту, що міститься на сайті правоохоронних органів, у 2019 році працівники Департаменту кіберполіції брали участь у розслідувані більше одинадцяти тисяч кримінальних проваджень, вчинених у сфері КТ.

Але, незважаючи на велику кількість кримінальних проваджень, Департамент кіберполіції не озвучує реальних результатів таких розслідувань. Зазначивши у звіті, що кількість встановлених правопорушників у кількості вісімсот осіб, відсутня будь-яка інформації про реальну кількість вироків щодо цих осіб та притягнення їх до відповідальності.

Отже, стрімкий розвиток технологій та наукові відкриття в галузі комп’ютерних технологій мають свої позитивні і негативні наслідки. Зокрема позитив – це створення першого комп’ютера (електронно обчислювальної машини), його активне застосування в сферах оборони, фінансовому ринку, комерційній сфері і т.д., що призводить до виникнення нового виду злочину, які вчиняються за допомогою цих же комп’ютерних технологій, що потребує швидкого реагування на державному рівні відповідних органів, з метою їх запобігання, виявлення, розслідування та ліквідації таких злочинних наслідків.

**1.2. Поняття злочинів у галузі комп’ютерних технологій**

Для аналізу чинного законодавства злочинів у галузі КТ та для виявлення основних проблем у цій галузі необхідно визначити, що розуміється під поняттям комп'ютерні злочини у правовому сенсі.

Конвенція про кіберзлочинність від 23 листопада 2001 року (далі - Конвенція) є відправною точкою для визначення понять, якими керує законодавець у сфері протидії комп’ютерним злочинам. Сьогодні вона ратифікована вісімнадцятими державами та підписана двадцяти п’ятьма країнами, серед яких є і Україна від 7 вересня 2005 року [6]. Терміни, які вживаються в Конвенції, на жаль, так і не знайшли свого закріплення у вітчизняному законодавстві. Також варто виділити, що у тексті Конвенції не міститься визначення поняття «кіберзлочин» та суміжних з ним понять.[7, с. 4].

У «Доктрині інформаційної безпеки України» використовувались категорії «комп’ютерна злочинність» та «комп’ютерний тероризм» [8, ст. 1783]. Стратегія національної безпеки, затверджена Указом Президента України від 8 червня 2012 року № 389/2012, містить терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [9].

Законом України (далі - ЗУ) «Про основні засади забезпечення кібербезпеки України» зазначено поняття - кіберзлочин. Кіберзлочин - є суспільно небезпечним винним діянням у кіберпросторі та/або з його використанням, відповідальність за яке передбачена ЗУ про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [10, ст. 1].

На мою думку, визначення термінології на дану тему мав би вирішити ЗУ «Про кібернетичну безпеку України», проект якого було зареєстровано ще 4 червня 2013 року, що так і не був прийнятий. Пізніше Указом Президента України від 1 травня 2014 року № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» одне з головних задач, що були поставлені, це розробити проекти Стратегії кібернетичної безпеки України і ЗУ «Про кібернетичну безпеку України», другорядні задачі, це привести національне законодавство у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [11, с. 416]. Стратегія кібернетичної безпеки України було затверджено Указом Президента України від 15 березня 2016 року № 96/2016 [12].

Кіберзлочини - це злочини, що вчиняються в процесі обробки інформації за допомогою ЕОМ або через комп’ютерні системи, суспільні відносини є об’єктом посягання у сфері обігу електронної інформації та інших суспільних відносин, у яких кваліфікуючою ознакою вчинення злочину виступає комп’ютер (наприклад, комп’ютерне шахрайство, або кібертероризм) [11, с. 417].

О. К. Копатін та Є. Д. Скулишин надають декілька визначень поняттю «кіберзлочин»:

Кіберзлочин – злочин, пов’язаний із використанням кібернетичних комп’ютерних систем, та злочин у кіберпросторі. Поняття комп’ютерного злочину, що пов’язане з використанням будь-якої комп’ютерної техніки, є більш широким на відміну від поняття кіберзлочин, пов’язаним із функціонуванням саме кібернетичних комп’ютерних систем. Несанкціоноване отримання прав керування кібернетичних комп’ютерних мереж можна віднести до протиправного використання (наприклад, використання шкідливого програмного забезпечення, спотворення інформації про стан об’єкта в каналі зворотного зв’язку, спотворення керуючого сигналу в каналі прямого зв’язку тощо), її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), також якщо створювати та використовувати в злочинних цілях будь яку кібернетичну комп’ютерну систему проти інших в злочинних цілях (наприклад, створення мережі зомбованих комп’ютерів для здійснення атак на веб-сайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо). [7, с. 6; 13, с. 85-86].

Кіберзлочин – можна віднести до найбільш небезпечного кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [14, с. 85-86].

Отже, вчені чітко відмежували кіберзлочин та злочин, що вчиняється з використанням комп’ютерної техніки, де може й не бути кіберпростору.

Чітке поняття «комп’ютерні злочини» можна сформулювати, визначивши суспільні відносини, яким завдається шкода в результаті вчинення комп’ютерних злочинів. Тобто «комп’ютерні злочини» як суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є ЕОМ, автоматизовані системи, комп’ютерні мережі або мережі електрозв’язку [7, с. 8].

У такий спосіб, науковці визначають «комп’ютерні злочини», як сукупність кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), передбачених чинним законодавством, що посягають на право захисту від незаконного поширення і використання інформації, шкідливих наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов’язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію. Зробивши висновки, можна сказати, що комп’ютерні злочини слід вважати злочинами, які вчиняються за допомогою або через комп’ютерні системи чи пов’язані саме з комп’ютерними системами, іншими словами із сукупністю пристроїв, із яких один чи більше у схожості до певної програми виконують автоматичну обробку даних.

Зважаючи на актуальність різних міркувань на визначення злочинів даної категорії, можна вважати, за потрібне ознайомитись з похідними поняттями від кіберзлочинності.

Кіберправопорушення є суспільно небезпечним діянням, яке здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки знищення) інформації, представленої у вигляді комп’ютерних даних, і тягне за собою юридичну відповідальність. Комп’ютерний злочин можна віднести по його ознакам до правопорушення, який відокремлюються в теорії права та виділяється факультативною частиною юридичного складу, у якому кіберпростір виступає як засіб або мета здійснення незаконних дій [13, с. 87]. На думку В.М. Болгова, вислів «кримінальні правопорушення, що вчиняються з використанням інформаційних технологій», дуже не практичні для вживання у повсякденному спілкуванні, саме через це вчений визнає раціональним термін не довгий «кіберзлочини», тим паче, інформація та тісно пов’язані з нею технології її обробки, тобто інформаційні технології є об’єктом цієї категорії правопорушень

Кіберпроступки - кіберправопорушення, які не несуть суттєвої небезпеки у суспільстві, за які законодавством передбачена юридична відповідальність (крім кримінальної).

Кіберпростір (кібернетичний простір) серед науковців має декілька визначень:

* штучно створене цифрове середовище перебування інформаційних об’єктів у цифровій формі, які створені через діяльність кібернетичних комп’ютерних систем керування й обробки даних і надає користувачам доступ до рахункових і інформаційних систем, створення цифрових інформаційних продуктів, передача електронних повідомлень та здатність за допомогою електронних цифрових об’єктів в режимі реального часу розпочинати роботу з спільного користування рахункових та інформаційних системи, до прикладу надання послуг, здійснення електронної комерції;
* середовище в якому створене інформаційно-комунікаційними системами де здійснюється процес зміни, формування, зберігання, передачі та видалення даних, що представлена у вигляді електронних комп’ютерних даних [13, с. 87-88].

Також зі сторони Верховного Суду США надійшло цікаве визначення кіберпростору, а саме: «Унікальний носій, що не знаходиться на визначеному місці, але через Internet загальнодоступний кожному в будь-якій точці Землі» [15, с. 152]. Internet є Інституціональним втіленням кіберпростору, якраз він становить собою масштабну інформаційну систему, що утворюються з інформаційних систем і не забороняє споживачу виконувати обмін інформацією з комп’ютерами, саме у такій системі.

Відповідно до ЗУ «Про основні засади забезпечення кібербезпеки України», кіберпростір є віртуальним простором (середовищем), що наділяє можливостями для виконання комунікацій та реалізації суспільних відносин, створений у підсумку функціонування схожих комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Internet та/або інших маштабних мереж передачі даних [15, ст. 1].

Причини появи злочинності у галузі використання ЕОМ ефективно розглядати у сукупності підстав залежно від зв’язків, що їх спричиняють. В першу чергу це правові підстав, а саме:

* правове регулювання злочинів у сфері комп’ютерних технологій в Україні далеке від ідеальності. Відсутність окремого нормативно-правового регулювання в межах міжнародного права є однією з підстав створення кібернетичної злочинності, оскільки місцевим законодавством окремої держави усіх проблем охорони КТ вирішити не реально. З’являється потреба застосовування єдиного підходу, сталої моделі поведінки, яка можлива лише у разі спорідненості чи тотожності їхнього національного кримінального законодавства чи окремих угод щодо переслідування злочинців [16, с. 93].
* відсутня законодавча урегульованість решти суспільних відносин, які є одним з принципових умов існування соціально-економічних причин злочинності у сфері КТ;
* інформаційні відносини в Україні перебувають на етапі створення, нормативні акти про інформаційні відносини регулюють в більшості загальні питання, тому нажаль деякі галузі регулюються в потрібній мірі, такі як захист державної та інших видів таємниць.

Кібербезпека під загрозою у випадку реалізації таких чинників, зокрема, як:

* відмінність інфраструктури електронних комунікацій держави, критерій її розвитку та підтримка сучасним вимогам;
* обмежений рівень підтримки критичної інфраструктури, державних електронних інформаційних ресурсів і інформації, вимога щодо захисту якої встановлена законом, а саме від кібернетичних загроз;
* не структурованість способів кіберзахисту основної інфраструктури;
* малий розвиток організаційно-технічної інфраструктури сприяння кібербезпеці та кіберзахисту основної інфраструктури та національних цифрових інформаційних ресурсів;
* мала ефективність суб’єктів сфери безпеки і оборони України у протидії кібернетичним загрозам воєнного, кримінального, терористичного та іншого змісту;
* обмежений рівень взаємодії, координації, інформаційного обміну між суб'єктами здійснення безпеки кібербезпеки [12, п. 2].

За В.М. Бутузовим певні злочини у сфері високих інформаційних технологій відносять до комп’ютерних, а саме:

* комп’ютерна техніка – знаряддя вчинення злочину;
* кіберпростір (середовище комп’ютерних систем та мереж) – незвичне середовище вчинення злочинів. Також об’єктом є суспільні відносини у галузі автоматизованої обробки інформації [7, с. 5; 11, с. 415].

Отже, з розвитком комп’ютерних технологій, зокрема саме злочинів в цій сфері, зростання способів, методів, технологій та суб’єктів їх вчинення, призводить до виникнення потреби їх розмежування та появи нових понять, які б їх чітко розмежовували та характеризували. Такі поняття потребують нормативного їх закріплення на законодавчому рівні, що в свою чергу призводить до частих змін та коригувань у законодавстві, або появи в корні нових нормативно-правових актів, які в подальшому будуть застосовуватися державними органами по боротьбі із злочинами в сфері комп’ютерних технологій. Правильне розуміння, застосування та трактування таких понять, матиме вплив на процес від їх попередження до ліквідації їх наслідків.

**РОЗДІЛ 2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ В ГАЛУЗІ КОМП’ЮТЕРНИХ ТЕХНОЛОГІЙ**

**2.1. Кримінально-правова та криміналістична характеристика злочинів у галузі комп’ютерних технологій**

Без сучасних інформаційних технологій неможливо уявити наш світ, люди щоденно використовують КТ та новітні засоби комунікації. Сьогодні комп’ютери впроваджуються в різноманітні сфери життя усіх людей. Велика кількість організацій та установ взяли за практику використовувати у своїй господарській діяльності, укладання грошових контрактів у спосіб електронного документообігу. Ця взаємодія організацій в більшій мірі залежить від технічних можливостей КТ, що ними використовується.

За звітами ФБР, протягом останніх років в Західній Європі, США, Австралії, в країнах СНД та Японії прослідковується зростання злочинних дій в сфері КТ, що являє погрозу як окремим організаціям та установам, так й економіці кожної країни та суспільства в цілому.

Нові інформаційні технології все ширше впроваджуються в практику правоохоронних органів. Так, в МВС України функціонує значна кількість автоматизованих систем оперативно-розшукового і профілактичного призначення, де обробляються величезні масиви інформації, в тому числі таємної чи призначеної для службового користування. Тому проблема захисту інформації, що зберігається та обробляється в комп’ютерних системах МВС від несанкціонованого доступу, її підробки, проникнення комп’ютерних вірусів і т. ін. сьогодні є особливо актуальною.

Глобальні інформаційні мережі не тільки стрімко криміналізуються, але і стають своєрідним джерелом інформації для злочинців, також часто являє собою зручним місцем для спілкуванням між собою та для створення злочинних груп. Тому питання протидії злочинам в сфері використання нових КТ на даний момент набуває потреби глибокого дослідження та особливої уваги [17, c. 28].

Незаконність в галузі КТ – це суспільно небезпечна діяльність чи бездіяльність, що вчиняється за допомогою КТ для вчинення матеріальної або соціальної шкоди підприємств, громадян, , відомств, організацій, громадських формувань та інтересам держави, а також особистим правам. В такому випадку комп’ютерні технології можуть використовуватися як об’єкт, або як засіб вчинення злочинів [7, c. 8].

Криміналістичні ознаки злочинності в галузі КТ відрізняється від загально розповсюджених злочинних посягань в криміналістиці. Для початку, до даних ознак мають включатися вагома інформація в криміналістиці про злочинця, чим він керувався та що його спонукало до злочинної поведінки, та ще потрібно вказати інформацію про потерпілу сторону.

Зазвичай здійснення злочину у галузі комп’ютерних технологій є вигода. За час розвитку комп’ютерних технологій злочини керуються також мотивами у політичній сфері (шпіонаж, тероризм), через дослідження у різних сферах (професіонали-програмісти, студенти), з метою помсти та із хуліганських мотивів.

Можна розділити на 5 категорій осіб, які скоюють злочини в галузі комп’ютерних технологій.

Перша категорія – це порушники правил користування ЕОМ. В дану категорію можна занести: недозволене використання комп’ютерів, розмноження вірусів і т.п.

Друга категорія – в народі називають "хакери", тобто одержимі програмісти. Це професіонали своєї справи, в них сильна технічна підготовка, ці особи вчиняючи протиправну дію, зазвичай економічної вигоди це не стосується. Для хакерів немає різниці до самоствердження, помсти за образу, бажання пошуткувати і т. п.

Схожа до зазначеної вище групи, є третя група осіб, це злочинці, які потерпають від сучасного різновиду психічних розладів, їх називають – інформаційними хворобами, а ще комп’ютерними фобіями. Доцільно зазначити, що під час розкриття та розслідуванню правопорушень в випадках психічного захворювання в обов’язковому порядку застосовуєтьсч судово-психіатрична експертиза щоб визначити осудності особи в момент скоєння злочину. Скоєнні злочини третьою групою осіб зазвичай тягнуть за собою фізичне пошкодження або знищення приладів комп’ютерної техніки без присутності злочинного умислу, з частковою чи повною втратою контролю над своїми діями [18, c. 145-146].

До вищого рівня злочинного світу відносяться так звані респектабельні злочинці: скарбники, бухгалтери, віце-президенти корпорацій, адвокати і т. п. Для них притаманне нелегальне застосування комп’ютера для того щоб змоделювати передбачені злочини, містифікація інформації, фальсифікація інформації та комп’ютерний шантаж і т. п. Такі злочинні дії для того, щоб отримати майнову вигоду чи з метою покрити інші злочини.

П’ята вища категорія – це злочинці, які діють у сфері комп’ютерного шпигунства. Такі особи також є професіонали – підготовлені фахівці. В політичній, економічній, технічній та інших галузях їхня основна мита – це придбання вагомих стратегічних фактів про суперника.

Юридична особа зазвичай відіграє роль потерпілої сторони від комп’ютерних злочинів.

Можна поділи три види потерпілих від таких злочинів:

* власники комп’ютерної системи;
* клієнти, які користуються їх послугами;
* інші особи [19, c.54].

Потрібно зазначити, що коли злочинці першої групи скоюють злочин, то потерпіла сторона, зазвичай, неохоче повідомляє в правоохоронні органи про факт вчинення злочину або взагалі цього не робить. Це, зокрема, можна віднести до основних факторів, яким можна пояснити високий рівень латентності цих злочинів.

Статистика комп’ютерних злочинів показує, що зареєстровані такі правопорушення можна виявити таким чином:

* 31% в результаті постійних перевірок доступу до даних службами інформаційної безпеки;
* 28% через агентурні роботи, а також за допомогою організації оперативних заходів по перевіркам заяв громадян;
* 19% випадково;
* 13% під час проведення бухгалтерських ревізій;
* 10% в ході розслідування інших видів злочинів.

Щоб вирішити питання потерпілої сторони про звернення до правоохоронних органів по факту вчинення злочину впливають різні фактори, а саме:

* відсутня компетентність працівників правоохоронних органів у питаннях зазначеної сфери;
* велика кількість організацій стримується вирішення конфлікту власними силами, що зазвичай закінчується використанням заходів, що можуть включати рецидив;
* втрата значної кількості клієнтів, що є результатом страху втратити власний авторитет;
* під час судового розгляду викриття системи безпеки організації, що є шкодою для неї;
* страх імовірності розкриття під час розслідування злочину незаконної техніки виконання різних фінансово-економічних операцій;
* не висока юридична грамотність не малої кількості посадових осіб у питаннях, що розглядаються і т. п.

Злочинці мають можливість використовувати способи КТ як прилад посягання на другі об’єкти, можна навести приклад, як спосіб впливати на керівництво за для кар’єрного росту. Як приклад з історії можна зазначити судовий розгляд по справі знаменитого Роберта Теппена Моріса про впровадження програми – черв’яка у мережу Internet у тисяча дев’ятсот вісімдесят восьмому році. Майнової шкоди програма черв’як не завдала, так як дані не були викрадені чи зруйновані. Проте технічні відділи втратили мільйони, а саме за час, на який було потрачено щоб виявити програму Моріса, тому що будь яка інша робота не виконувалася, а ще додатково був витрачений час на відновлення та перевірку функціональність систем. Під час судового процесу обвинувачений Моріс не заперечував впровадження програми, але заявив, що це було зроблено без злого умислу, наслідком чого було застосовано умовне позбавлення волі. І таких випадків велика кількість, коли застосовувалося умовне покарання [20, c. 22].

На рахунок злочинів, що вчиняються в галузі КТ, особливу увагу привертають сліди, тому що саме вони показують, яким способом особа потрапила та зникла з місця події, які знання використала, використала своє службове становище, подолала перешкоди, виконла поставлену злочинну ціль, до яких навиків та фізичних зусиль вдалася, чи намагалася скрити сліди злочинних дій. Велике значення мають також сліди, що розказують про характер зв’язку злочинця з предметом злочинного посягання і т. п.

Проте, спосіб вчинення злочину в кримінально-правовій характеристиці надано у загальному вигляді, можна навести приклад, проникнення у приміщення, спосіб відкритого або таємного розкрадання. Для кримінально-правової характеристики не відіграє велику роль конкретні способи проникнення, прийоми таємного розкрадання, засоби, що використовуються при цьому, джерела їх отримання. Таким чином використовується криміналістична характеристика способу вчинення злочину [18, c.121].

Коли за базу класифікації покласти метод, який використовувався особою, що вчинила злочин для отримання доступу до засобів комп’ютерної техніки, можна виділити такі п’ять основних груп:

* вилучення засобів комп’ютерної техніки;
* перехоплення інформації;
* несанкціонований доступ;
* маніпулювання даними та керуючими командами;

комплексні методи.

Важливим фактом для розслідування злочинів у галузі КТ є спосіб вчинення злочину, тому що є обов’язковою часткою об’єктивної сторони злочину та відноситься до його кримінально-правової характеристики і служить й кваліфікуючою обставиною.

Вилучення засобів комп’ютерної техніки, тобто першою групою засобів скоєння злочинів у сфері комп’ютерних технологій, можна виділити, що предметом злочинного посягання постійно виступають засоби КТ. А що не відноситься до комп’ютерної техніки, тобто інші інструменти та технічні засоби, що використовуються або взагалі без їхнього використання відносяться до знаряддя скоєння злочину.

До другої групи, а саме перехоплення інформації, характерною рисою є способи, які злочинці використовують: аудіовізуального та електромагнітного перехоплення інформації. В цій та наступних групах, які зазначені, засоби КТ виступають предметом та знаряддям скоєння злочину.

Перехоплення інформації поділяють на безпосереднє-активне, електромагнітне-пасивне, аудіоперехоплення, відеоперехоплення, а також “прибирання сміття”, так називають спосіб.

Якщо говорити про безпосереднє перехоплення, воно вчиняється за допомогою прямого підключення до комп’ютерної системи чи мережі, телекомунікаційного обладнання комп’ютера. Можна навести приклад: до телефонної лінії каналу зв’язку, який використовують щоб передати комп’ютерні дані.

Через підключення до кабелю або перехвату мікроволн від супутника та наземних радіостанцій злочинці отримують пароль та всю засекречену інформацію з телекомунікаційних систем, це можна віднести до способу скоєння злочину.

Другий спосіб скоєння злочину, це електромагнітне, до його характерної ознаки можна віднести роботу електронних пристроїв (принтери, дисплеї), які супроводжується електромагнітним випромінюванням.

Через це, сигнали з електронно-лучової трубки дисплея можна аналізувати, записувати та приймати на велику відстань, приблизно 1000 метрів за допомогою стандартного телевізійного та відтворюючого устаткування, що може знаходитися, наприклад, у автомобілі.

Аудіоперехоплення – цей вид перехоплення є дуже небезпечний і на жаль часто застосовується злочинцями, тому секретні дані залишити в безпеці складає труднощі. Злочинці використовують підслуховуючий пристрій, щоб здійснити злочин (наприклад “таблетки”, “клопа”, “жучка”). Вони через обман проникають у приміщення та встановлюють різні пристрої в апаратуру засобів обробки інформації. Також в сучасному світі винайшли спосіб без прямого проникнення злочинця в будівлю, для цього їм потрібні спеціальні акустичні та вібраційні датчики.

Відеоперехоплення – це спосіб злочинці застосовують для отримання секретних даних, для цього їм потрібні різні сучасні відеооптичні техніки. Можна навести приклад відеооптичної техніки, а саме відео-фотоапаратура з підходящими оптичними насадками, бінокль, підзорна труба, пристрій нічного бачення.

Прибирання сміття – злочинці використовують недбалість користувачів комп’ютерів, та використовують інформацію яку вони залишили після роботи з технікою, тобто вони користуються технічними відходами. Можна розділити на форми використання способу: фізичній та електронній.

Третя група скоєння злочину у сфері комп’ютерних технологій характеризується діями особи, що вчинила злочин, ці дії націлені на отримання незаконного доступу до засобів КТ, а саме:

“За дурнем” – серед злочинців цей спосіб відомий, вони часто його використовують для проникнення на заборонену територію.

Наприклад: злочинець, спочатку очікує працівника біля дверей державної установи, а потім проникає в будівлю разом з співробітником, злочинець в цей час тримає зі собою предмети, які пов’язані з комп’ютерною технікою.

“За хвіст” – такий спосіб заволодіння даними супроводжується фізичним під’єднанням зловмисника до мережі законного користувача, після чого очікує моменту, а саме спец сигналу, завершення, спрямовує його на себе, а потім, лише коли законний користувач завершує роботу, виконує вхід до системи.

“Комп’ютерний абордаж” – злочинець використовує номер абонента комп’ютерної системи, заздалегідь його організувавши, для цього способу може використовувати звичайний телефонний апарат, після чого злочинець підбирає пароль до комп’ютера. Є 2 варіанти дізнатися пароль: власноруч або за допомогою програм, що спеціалізуються на зломі.

“Неспішний вибір” та “пролом”. При повільному виборі відбувається відшукування вразливих точок у безпеці комп’ютерної системи, у наступному способі виявляються “проломи” у комп’ютерних системах, це частіше всього слабкі місця у системному забезпеченні, який з часом можна застосовувати у злочинних цілях.

“Маскарад” – для того щоб захистити комп’ютерну систему користувачі встановлюють автентифікацію користувача, наприклад, відбитки пальців, розпізнавання голосу. На жаль, не всі користувачі користуються даною функцією, через що злочинна особа має можливість обманути систему і проникнути в комп’ютер в ролі законного користувача.

“Містифікація” – інколи користувач ПК від’єднується до чиєїсь системи, будучи занадто впевненим в тому, що працює з потрібним йому абонентом. Таким фактом користується правопорушник, створюючи правдоподібні відповіді на питання власника інформаційної системи, до якої відбулося під’єднання та підтримуючи таку помилку протягом деякого часу, він отримує потрібну інформацію, таку як, паролі доступу чи відзив на пароль.

“Аварійний” – правопорушником враховується такий факт, що у будь-якому комп’ютерному центрі є спеціальна налаштовувана програма, що дає змогу обійти ступені захисту даних.

“Склад без стін” – заборонений доступ до комп’ютерної мережі в цьому разі здійснюється правопорушником шляхом використання комп’ютерної поломки, в результаті якої з’являється часткове або повне порушення правильного та безпечного режиму роботи програм захисту інформації.

Четвертої група скоєння злочинів можна описати діями злочинця шляхом маніпулювання даними та працівниками, що стоять вище кар’єрній сходинці. Найбільш відомий метод серед злочинців - “підміна даних або коду”. В такому випадку злочинці змінюють або вводять нові дані або коди [21, с.67].

Також в комп’ютерному злочинному світі часто використовують комп’ютерне шпигунство: у господарській діяльності компаній, що на пряму стосується сфери поточних рахунків, фінансових звітів та інформація про клієнтів, що містяться у комп’ютерах.

Злочинці з сфері шпигунства в сучасному світі мають нову мету – комп’ютерні прогарами і "дефекти конструкцій".

Наприклад: злочинець копіює та переписує на дискету секретну інформацію компанії, програми та файли, шляхом перевірки файлів у комп’ютері та аналізу цих файлів, на цю дію йому не потрібно багато часу.

Щоб захистити дані від злочинного посягання, потрібно дотримуватися основних завдань:

* перевірка цілісності інформації;
* виключення несанкціонованого доступу до ресурсів ПЕОМ, до програм і даних, що зберігаються в ній;
* виключення несанкціонованого використання програм, що зберігаються в ЕОМ (тобто, захист програм від копіювання) [21, c. 15].

Комп’ютерні злочини також можна передбачити, але для цього потрібно використовувати різноманітні способи захисту інформації, в саме: технічні, програмні, криптографічні та правові.

Під технічним захистом даних мається на увазі різні апаратні методи, як приклад можна навести: екранування приміщень де встановлені ПК, установка генераторів шумів та інше. Також, варто відзначити, що захистити дані від незаконного втручання тільки технічними засобами майже неможливо.

Програмний метод захисту інформації – це спеціальні системні програми, що перешкоджає несанкціонованому суб’єкту отримати інформацією, що зберігається у системі. Цей видом безпеки може бути, наприклад, застосування групи паролів.

Під криптографічним способом збереження інформації мається на увазі попереднє їх шифрування до моменту введення у ЕОМ.

По проведеній статистиці можна зазначити, що компанії та організації використовують комбіновані способи захисту інформації від незаконного втручання.

Більшість людей в сучасному світі користуються антивірусними програмами, щоб у комп’ютері, яким вони користуються передчасно виявити та очистити від занесеного вірусу.

Правовий захист інформації – це сукупність адміністративно-правових і кримінально-правових норм, що визначають відповідальність за незаконне використання інформації або програмних засобів [22, c.31].

Мережа Internet також є актуальна для злочинців. Спеціалісти розробили особливі засоби захисту в мережі. Наприклад: захист портів, що являють собою комп’ютери, які сторожать входи до головного комп’ютера. До них входить мікропроцесор, що здійснює ідентифікацію користувача та приймає рішення про надання доступу до системи та пристроїв пам’яті, який зберігає коди користувачів, що мають право на доступ.

Способи захисту портів, якими користуються на сьогодні, можуть здійснювати таступні захисні функції: “камуфляж”, “дзвінок назустріч”, “звірка коду”, та інші.

Сьогодні з метою захистити комп’ютерні системи і мережу Inernet, використовують електронні ключі, їх можна описати як прилад з пам’яттю, створений на особливому чипі.

Ключ має два входи, одним підключається з паралельним портом ПК, інший використовується для підключення периферії. Ключ не має власних джерел живлення та зберігає записану в нього інформацію при від’єднанні від ПК. Ключ має до ста тисяч циклів перезапису еерrom – пам’яті й термін зберігання інформації не менше десяти років. До пристроїв такого виду належать електронні ключі HASP компанії Fladdin [23, c.29-40].

Для того щоб при запуску захищена програма функціонувала, вона має знайти “свій” ключ, в тому випадку, якщо ключ не був виявлений, програма повідомляє про помилку та не продовжує свою роботу. Якщо особа бажає перенести програму та зробити резервну копію, для цього потрібно лише перенести з собою електронний ключ. В захисному процесі застосовуються потужні антивідладочні чи антитрасировочні алгоритми з кодуванням інформації, такий реалізований захист від вірусів.

Система захисту персональної електронно-обчислювальної машини від незаконного входу “Barrier-III”, “Barrier-IV” являє собою додаткову спец програму яка працює в парі з основною операційною системою і забезпечує можливостю розмежування доступу окремим особам.

Система дає можливість створити спеціальне робоче місце з програмним середовищем що має межі та невеликою кількістю користувачами, що мають різні повноваження щодо доступу до файлів, програм, каталогів, дисків. Система “Barrier-III” виконує такі функції:

* захист персональної електронно-обчислювальної машини від незаконного запуску операційної системи з жорсткого диску;
* захист від найбільшого спільного дільника даних, які записані на жорстких дисках при завантаженні операційної системи з системної дискети;
* ідентифікація та верифікація користувача;
* розподіл меж доступу між користувачами місць зберігання даних;
* нагляд за відсутністю пошкоджень системних програм;
* розподіл доступу до баз даних, програмних продуктів;
* крипто захист даних, на жорстких дисках (Державний стандарт 28147-89) [24, c.135].

Програмні системи криптографічного захисту даних “Postcrypt”. Існує для вирішення таких питань криптографічного захисту даних в комп’ютерних мережах та системах:

* аутентифікація, контроль цілісності, повідомлення;
* аутентифікація автора повідомлення за допомогою вироблення та перевірки електронного цифрового підпису (ЕЦП);
* ідентифікація автора повідомлення;
* зашифровка повідомлення.

Процес кешування повідомлень здійснюється відповідно до стандартів ДЕСТ Р34.11-94. Створення та перевірка ЕЦП здійснюється відповідно до стандартів ДЕСТ Р34.10.-94. Розподіл кодів шифрування здійснюється за схемою Диффі-Хеллмана. Контроль цілісності та шифрування виконується відповідно до стандартів ДЕСТ 28147-89.

Методи захисту інформації у комп’ютерній мережі “Secret Net”, надає власнику можливість централізованого і узагальненого керування доступом до даних на всіх комп’ютерних станціях мережі з будь-якого місця. “Secret Net” чітко захищає комп’ютерну мережу від вірусних атак, та підтримує різного роду крипто засоби, які сертифіковані Державною технічною комісією по третьому класу захищеності.

Система телекомунікаційного передачі даних між банком і його клієнтами “Fast pay”. Конфіденційність в системі забезпечується:

* групою кодів доступу, які самостійно міняються кожним користувачем окремо;
* відмінностями у правах доступу користувачів до інформації;
* використання ЕЦП з використанням алгоритмів гарантованих ДЕСТ 34.10-94;
* шифрування та криптуванням даних, що передається та зберігаються;
* веденням історії відправлених та отриманих з банку даних, а також допущених у системі критичних операцій [24, c.176].

Системи контролю доступу. Проблема розподілу людей на “своїх” та “чужих” здавна вирішувалася, зокрема, наділенням особи, якій дозволено доступ до певного приміщення чи обладнання якимись знаками відмінності, що виділяють її серед інших (спеціальна монета, перстень, ключ, перепустка, магнітна картка і т. ін.). Їй довірявся шифр, пароль. Проте, при такому підході не існує повної певності у відповідності носія інформації особі, що пред'явила його. Так, перепустка чи посвідчення можна підробити, пластикову картку - викрасти, пароль - підслухати.

Новим напрямом в організації систем розмежування доступу є системи, що базуються на біометричних методах, за допомогою яких можна по відбиткам пальців рук, малюнку радужної оболонки ока, за формою руки, голосу, підпису ідентифікувати особу.

У приладі “Handkey”, розробленому компанією “Avan”, як вхідний параметр використовується трьохмірне зображення руки в інфрачервоному діапазоні. Для ідентифікації використовуються параметри від сканованої руки, тобто рука людини є її унікальним “посвідченням” (прилад “Handkey” розсекречено урядом США у 1991 році) [25, c.113-116].

Отже, у зв’язку з широким переліком сфер застосування комп’ютерних технологій в повсякденній діяльності, а в деяких із них, неможливість діяльності без таких технологій, виникає ризик втрати важливої інформації, тому що досить часто комп’ютер використовується як "безпечний склад" для збереження інформації. Так, багато користувачів зберігають свої важливі службові та комерційні таємниці в комп’ютерах у вигляді банків даних. При цьому більшість з них навіть не ознайомлені з необхідністю прийняття заходів щодо захисту комп’ютерної інформації, що може лише сприяти злочинному втручанню. Тому важливим моментом є знання та спеціалізація окремих осіб на будь-якому рівні (державному, комерційному, особистому), з питання визначення сутності можливого вчинення злочину, що збільшує шанси користувача не стати його жертвою.

**2.2. Класифікація та види злочинів з галузі комп’ютерних технологій**

В законодавстві України, кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі ( п.5 ч.1 ст.1 Закону України «Про основні засади забезпечення кібербезпеки України») [10]. У загальному розумінні, кібербезпека є реалізацією методів захисту мереж, програм та систем від кібер атак.

Відповідно до Конвенції про кіберзлочинність, яка є невід’ємною складовою національного законодавства України з 11 жовтня 2005 року, кіберзлочини умовно діляться на 4 види.

До першого виду відносяться злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем. До цього виду злочинів відносять всі злочини, направлені проти комп’ютерних систем і даних (наприклад, умисне завдання шкоди, руйнування, погіршення, зміни або приховування комп’ютерних даних; умисне втручання до комп’ютерної системи або її окремих частин; умисне вчинення, без наявного права, створення, продаж, придбання для застосування, поширення або надання для використання іншим чином пристроїв, в тому числі комп’ютерних програм).

До наступного виду злочинів належать протиправні діяння, пов’язані з комп’ютерами. Такі правопорушення охарактеризуються умисними діями, що має наслідок втрати майна іншою особою шляхом будь-якого застосування, зміни, знищення чи приховування комп’ютерних баз даних або будь-якого втручання у роботу комп’ютерної системи, з шахрайською метою заволодіння, не маючи на це прав, економічними перевагами для себе чи третьої особи.

Третій вид кіберзлочинів включає вчинки, пов’язані з інформацією (контентом), що являє собою здійснення навмисних протиправних дій зі створення, розповсюдження або надання доступу до контенту з дитячої порнографії, та володіння таким контентом.

Останнім, четвертим видом є навмисне діяння, пов’язане з порушенням авторських та суміжних прав, відповідно до умов Угоди про торговельні аспекти прав інтелектуальної власності, Бернської Конвенції про захист літературних і художніх творів та Угоди ВОІВ про авторське право, а також законодавства України [26].

Існують ще інші класифікації кіберзлочинів, але класифікація, що застосовується конвенцією є найбільш популярною.

У пункті 14 Доповіді Комітету ІІ Десятого Конгресу ООН 2000 року із запобігання злочинності та поводження з правопорушниками зазначено, що існує дві категорії злочинів:

* кіберзлочини у вужчому розумінні (комп’ютерні злочини) - будь-яка протиправна дія, вчинена шляхом електронних операцій, завданням яких є проходження захисту комп’ютерних систем і оброблюваної ними інформації;
* кіберзлочини в ширшому значені (правопорушення, пов’язані із застосуванням комп’ютерів) - незаконне діяння, що здійснюється за допомогою або у взаємодії з комп’ютерною системою або мережею, в тому числі такі злочини, як пропонування, незаконне зберігання або розповсюдження даних через комп’ютерні системи або мережі [27, с. 338].

Кримінальну караність за злочини в сфері КТ, як у вузькому так і широкому значені регулює Конвенція про кіберзлочинність. Кримінальне законодавство окремих держав, застосовує карну відповідальність за злочини в сфері комп’ютерних технологій лише в вузькому значені, що підтверджується на прикладі нашого національного законодавства [28, с. 129].

В Особливій частині Кримінального кодексу наявний Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку». Жодна із шести статей в цьому розділі не має норми, за якою можна було б притягнути до відповідальності особу, що здійснила, наприклад, шахрайство у виді незаконних дій з використанням електронно-обчислювальної техніки (частина 3 статті 190 Кримінального Кодексі України), або окремі суспільно- небезпечні дії, передбачені статтею 200 Кримінального Кодексі України [29, с. 134].

Використання комп’ютерів для здійснення названих дій є лише певним шляхом вчинення злочину, який в більшості не входить до обов’язкових характеристик об’єктивної сторони складу злочину. За присутності деяких фактичних обставин ці правопорушення можуть кваліфікуватись за сукупністю з злочинами, передбаченими Розділом XVI Особливої частини Кримінального Кодексу України [30, с. 435].

Потрібно також відзначити, що у зв’язку із застосуванням комп’ютерних технологій чимала кількість простих злочинів відноситься до категорії злочинів в сфері КТ, до того ж, методи їх здійснення значно полегшилися, а території їх вчинення зросли в рази. [28, с. 129].

За характером, їх відносно можна розділити на 2-ві основні групи, це економічні та воєнно-політичні.

До воєнно-політичних слід відносити кібер війни, щодо комп’ютеризацією ракетного ядерного забезпечення кожної держави.

В групу економічних злочинів входить нелегальне інформаційне брокерство (вторгнення у комп’ютерні системи з метою продажу інформації, як особам у яких її було викрадено, або конкурентам); комерційне шпигунство; комп’ютерне піратство.

Європейський комітет з проблем злочинності у 1990р. написав низку рекомендацій для виокремлення у Європі злочинів, пов’язаних з комп’ютерними технологіями, і виніс їх до так званого «мінімального списку» та «необов’язкового списку» комп’ютерних правопорушень, які були віднесені на включення до законодавства країн Європи. [31, с. 167]

До Мінімального списку віднесені наступні види злочинів:

* знищення комп’ютерної інформації, знищення комп’ютерних програм, комп’ютерне шахрайство, комп’ютерний саботаж, комп’ютерний підлог, незаконний доступ до комп’ютерних мереж;
* незаконне виробництво типографічних копій;
* незаконне копіювання захищених комп’ютерних програм.

Необов’язковий перелік містить в собі наступні види злочинних діянь:

* незаконне використання комп’ютера;
* комп’ютерне шпигунство;
* зміни до інформації чи комп’ютерних програм;
* незаконне використання захищених комп’ютерних програм [32, с.265-266].

З практичної сторони залишаються не врегульованими чимала кількість правових запитань у сфері КТ, зокрема, визначення місця вчинення правопорушення, вчиненого за допомогою Інтернет мережі.

Законодавство якої країни слід використовувати, якщо особа, що вчинила правопорушення і об’єкт посягання знаходяться у різних місцях, навіть континентах?

Як буде вирішене питання щодо меж можливого та обов’язкового застосування кримінального права держави до злочинів в сфері комп’ютерних технологій, вчинених поза її територіальними межами? [28, с. 130]

Діючий Закон України «Про міжнародне приватне право» [33] роз’яснює деякі суперечливі одна одній норми, які мають місце у міжнародній діяльності країн, але контроль кібер-злочинів не зачіпається зовсім ніяк.

ЗУ «Про основні засади забезпечення кібербезпеки України» в ст. 14 зазначається, що Україна відповідно до ратифікованих нею міжнародних договорів здійснює співпрацю у сфері кібербезпеки з іншими державами, їх правоохоронними органами і спецслужбами, також з міжнародними організаціями, що боряться з міжнародною кіберзлочинністю [10, ст. 14].

Україна відповідно до міжнародних договорів, ратифікованих Верховною Радою України (ВРУ), також бере активну участь у загальних заходах із підтримання та встановлення кібербезпеки з дотриманням вимоги Закону України «Про порядок направлення підрозділів Збройних Сил України до інших держав» [34] та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України» [35].

Відповідно до вище зазначених норм, інформація, яка пов’язана із боротьбою з міжнародною кіберзлочинністю, Україна зобовязується надати іншій державі на підставі її запиту із дотриманням вимог чинного законодавства України та її міжнародно-правових обов’язків. Також така інформація може бути надіслана без будь-якого запиту іншої країни, якщо це не блокує чи заважає здійсненню досудового розслідування чи уже судового розгляду справи і може допомогти відповідним органам іноземної держави у ліквідації кібератаки, своєчасному виявленні і припиненні кіберзлочину, але якщо норми законодавства країн, між якими стався злочин, суперечать одна одній відповідальність за правопорушення може і не настати, оскільки причин для надання інформації в однієї із держав може не бути, за умови, що в цієї країни відсутні норми до яких це діяння внесене як злочинне.

Юртаєва К.В. зазначає, що найбільшою проблемою, яка характеризує Інтернет з точки зору політики юрисдикції є те, що він не має межі між внутрішньодержавною і міжнародною передачею інформації. Інтернет створений та являє собою поза територіальний засіб спілкування та обміну даними, що не має централізованого управління.

Кожна особа і її комп’ютер діють незалежно та формують одну транснаціональну мережу, яка поширюється за межі географії державних територій. Інтернет-адреси, які підтримуються інтернет мережею є розмитими і навіть адреси сайтів, що мають URL-індикатори держави походження, наприклад, «pl» або «ua» не обов’язково мають бути точними.

Інтернет-адреси є довільними та можуть бути незмінними, у той час, як сервери рухаються фізично. Така особливість мережі Інтернету ставить науку і практику перед потребою винайдення кардинально нових методів по протидії злочинам міжнародного характеру із застосуванням КТ та впровадження політики юрисдикції щодо таких злочинних дій [28, с. 130].

Найбільш розповсюдженими є кілька головних напрямів вирішення проблеми наступного регулювання відносин в мережі Інтернет та кримінальної караності за правопорушення міжнародного змісту за використанням КТ.

Перший напрямок рекомендує пристосуватися до правопорушень, що відбуваються за участю новітніх інформаційних технологій.

Щодо другого, то запропоновано розглянути мережу Інтернет, як незалежний кіберпростір та винаходити кардинально нові правила впровадження кримінальної юрисдикції щодо правопорушень, що в ньому здійснюються. [29, с. 135-136]

Ті, хто підтримує перший напрямок вважають, що сучасні Інтернет-технології за замовчуванням не міняють правову природу кримінальної територіальності і може бути використана до злочинів в сфері КТ міжнародного характеру. [28, с. 130]

Поширену структуру кримінальної юрисдикції, щодо регульованих злочинних дій регулює Конвенція про кіберзлочинність та допускає місцевий та національний принципи кримінальної юрисдикції. У частині 1 статті 22, кожен із учасників, здійснює такі законодавчі та інші міри, які на їх думку є необхідними для встановлення контролю щодо будь-якого кримінального проступку, визначеного Конвенцією, якщо він вчинений: на її території; на борту судна, яке плаває під прапором такого учасника; на борту літака, що зареєстрований відповідно до законодавства такого учасника; якщо одним з виконавців злочину є громадянин країни учасника де таке діяння карається кримінальним законодавством у місці його здійснення, або злочин вчинено за межами територіальної юрисдикції будь-якої країни.

Сама ж Конвенція не роз’яснює запитання, які ж кіберзлочини варто вважати здійсненими на території даної країни, та визначення «місце вчинення злочину» і залишає це на розсуд суду держави де вчинився такий кримінальний проступок.

Звертаючи увагу на особливості злочинів в сфері комп’ютерних технологій, якщо, наприклад, місце розташування злочинця можна відшукати за ip-адресою, то те що відноситься до постраждалої сторони, якій завдано шкідливі наслідки, можна лише дізнатися після настання для неї таких наслідків. Важкою є випадок, коли комп’ютерний вірус завдає шкоди інтересам 2-ом або більше країнам.

Міжнародна практика зазначає, що єдиного способу для вирішення цих ситуацій на державному рівні ще досі не знайшли, кардинально протилежне роз’яснення місця вчинення злочину, що стосується з комп’ютерних технологій та відсутність конкретного правового врегулювання на міжнародному рівні можуть мати наслідок з одного боку - конфліктів кримінальних доктрин різних країн, коли декілька країн претендують на застосування нормативно правових актів про кримінальну караність щодо одного і того ж кримінального правопорушення, а з другої сторони до негативних суперечок кримінальних юрисдикцій, коли ні одна зі сторін яка задіяна у злочинній дії не бажає розпочинати переслідування вчиненого кримінального правопорушення зі своїх внутрішніх поглядів.

В світовій практиці, питання кримінальної юрисдикції стоїть залежним від наявного розподілу кіберзлочинів за колом об’єктів вчинення:

* проступки, які направлені та посягають на широке коло об’єктів, до прикладу - поширення комп’ютерних вірусів або порнографії;
* проступки, що направлені та завдають збитків конкретним об’єктам, до прикладу, можна віднести - банкам, електронним скринькам особи. [28, с. 131].

Відповідно до норм Конвенції, об’єктом злочинів в сфері КТ, є значне коло суспільних відносин, що регулюються нормами права. Такі відносини беруть свій початок при вчинені інформаційних процесів щодо створення, концентрації, аналізу, нагромадження, зберігання, відшукування, обміном, та використання комп’ютерних даних, та інші сфери людської діяльності де використовуються комп’ютери та комп’ютерні технології, серед яких виокремлюють відносини, які виникають щодо забезпечення цілісність комп’ютерних даних та їх систем, конфіденційність, легального використання комп’ютерів і комп’ютерних даних, авторського права. [32, с. 267]

Щодо застосування нормативно-правових актів країною щодо кримінальної відповідальності кіберзлочини, які направлені на конкретні об’єкти, частіше всього вирішується за принципами об’єктивної територіальності. Перебуваючи злочинця в одній державі, він спрямовує свої незаконні дії на територію іншої держави, з використанням новітніх комп’ютерних технологій. Правоохоронні органи держави з якої діє злочинець можуть навіть не здогадуватися про вчинені ним кримінальні правопорушення, а встановити їх лише після настання суспільно небезпечних наслідків в іншій державі, в цих ситуаціях кримінальне розслідування та переслідування правопорушника є неможливим без допомоги та співпраці з державою де настали ті небезпечні наслідки. В цьому випадку злочинець може притягуватися до кримінальної відповідальності державою у якій він перебуває, або може бути переданий країні, яка постраждала від його злочинних дій, за умов якщо є укладені між цими державами міжнародні договори, які передбачають у своїх нормах процедуру екстрадиції злочинця, але потрібно зазначити, що процес екстрадиції є досить складним і є частіше винятком, а ніж правилом для вирішення проблеми. [28, с. 131]

Повертаючись до Європейської конвенції про видачу правопорушників, сторони в договорі мають обов’язок передавати одна одній правопорушників, які переслідуються правоохоронними органами сторони, що надає такий запит, за вчинене злочинне діяння або які переслідуються такими державними органами за для виконання існуючого вироку. [36, ст. 1]

Варто зазначити, що Україна не ратифікувала дію конвенції [6], тому дії кіберзлочинців, де Україна може бути задіяна як сторона, не регулюються нормами Конвенції.

Світова практика показує разові випадки, де потерпіла сторона вирішує питання про притягнення правопорушника до відповідальності без здійснення відповідного запиту до держави де він знаходиться. Існує проблематика застосування кримінальної юрисдикції держави до злочинів в сфері КТ, які впливають на широке коло предметів посягання та порушують суспільний порядок у декількох державах. Притягнення злочинці до покарання та відповідальності можливе лише у разі наявності правилами екстериторіальності, але із правилом, за умови наявності в державі кримінальної заборони кіберзлочинів. [28, с. 132]

Конвенція про кіберзлочинність встановлює головні, що враховуються у нормативно-правових актах держав, що приєдналися до неї: 1) вчинення дій, потрібних для негайного збереження комп’ютерної інформації (частина перша статті 16 Конвенції); 2) зберігання провайдерами інформації про трафік інформації у строки до 90(дев’яносто) днів з можливістю за потреби наступного продовження такого строку (частина друга статті 16 Конвенції); 3) обов’язок збереження секретності отриманої інформації під час проведення розслідування (частина три статті 16 Конвенції) [26].

У зв’язку з бажанням України до європейської та євроатлантичної інтеграції, для підняття рівня ефективності боротьби з кіберзлочинністю потрібний обов’язковий міждержавний обмін даними із запобігання таким злочинам із врахуванням практики держав, що не ратифікували конвенції про кіберзлочинність у своїй країні.

Широкої практики зазнало створення спецпідрозділів поліції у сфері запобігання кіберзлочинам, такими прикладами є Австралія, Бельгія, Білорусія, Великобританія, Данія, Естонія, Індія, Канада, Малайзія, Нідерланди, Німеччина, Норвегія, Польща, США, Україна, Швейцарія, Швеція та інші.

До основних функцій таких спецпідрозділів належать: 1) збір, структурування та комплексний аналіз даних про злочине в сфері КТ; 2) підвищення кваліфікації працівників поліції 3) розслідування злочинів, надання будь-якої підтримки іншим органам; 4) аналіз та перевірка кіберпростору за для виявлення злочинів, вірусів або шкідливих програм; 5) робота з особами для профілактики кіберзлочинів із використанням ЗМІ; 6) вчинення оперативно-розшукових та розвідувальних дій за для фіксації злочинної діяльності; [36, с. 193].

Держава, що межує з Україною - Польща, повз яку теж курсують інформаційні мережі злочинів в сфері комп’ютерних технологій, протидіє ним за участю кібервійськ, лави яких постійно збільшуються. Створення такого виду військ є реальним завдяки фінансової підтримки зі сторони держави, близько 460 мільйонів євро йде із бюджету на ці потреби. Індія взяла за практику залучення до боротьби зі злочинами в сфері КТ так званих хакерів. Існує теорія, що кіберзлочинці, під час перебування у місцях позбавлення волі під контролем кіберполіції будуть науковим проривом, а саме під час поглибленого дослідження їхньої діяльності.

У США діє підрозділ секретної служби, що співпрацює зі службами та правоохоронними органами штатів і приватним сектором, шляхом встановлення та протидії кіберзлочинам. Також слід відзначити дії Канади зі злочинами в сфері КТ. Спецподрозділ Королівської канадської кінної поліції, беручи до уваги дані інформцентру та взаємодіючий з іншими державами, здійснює розслідування та розкриття злочинів в сфері комп’ютерних технологій.

Швидкість встановлення міждержавних відносин, щодо питання співпраці у протидії зі злочинністю весь час потребує застосування або стандартних дій з переслідування злочинця у разі наявності тотожних норм кримінального законодавства сторін договору, або встановлення світового стандарту відповідної незаконної діяльності міжнародно-правовими механізмами. У кримінальному законодавстві в загальному склад злочину являє собою протизаконну діяльність і являє собою угрупування визначених карним законом ознак, що визначають окреме діяння як злочин. Щоб було досягнуто відповідна співпраця країн то незаконна діяльність окремої особи охарактеризується як факт і в більшості існуючих випадків криміналізується усіма учасниками договору.

Тому можна впевнено вказати, що як міжнародно-правовий феномен - злочин міжнародного характеру, це певний стандарт суспільно небезпечної поведінки особи, який регулюється положеннями міжнародного права і прийнятий країнами, які беруть участь у міжнаціональному співробітництві щодо питань боротьби проти злочинності [16, с. 94].

Враховуючи вище зазначене можна дійти висновку, що теперішній час державами до кіберзлочинів застосовуються звичаєві принципи кримінальної територіальності, які базуються на ідеології географічної територіальності. Враховуючи технології сучасних комп’ютерних систем, вони існують за межами територіального суверенітету, а наявні принципи кримінальної юрисдикції переходять до графи неефективних та сприяють появі чималої кількості юридичних питань.

Але з тим, право на існування є і у інших підходів що регулюють цивільно-правові відносини в мережі Інтернет, як вихід є пропозиція вважати місцем вчинення злочину не територію окремої держави або іншу географічну точку, а зокрема сам кіберпростір [28, с. 132].

За існуючими прогнозами в найближчому майбутньому можлива тенденція швидкого зростання кількості кіберзлочинів, і що найперше це особливо небезпечних таких як «кібершпигунство», «кібертероризм», «кібервійни» [28, с. 135]. Передбачення такого шляху розвитку подій потребує здійснення пошуку і запровадження діючих засобів протидії, які повинні ґрунтуватися на винаходи в сфері кримінального права і криміналістики, на наукових дослідженнях світової та окремої держави практики [32, с. 269].

Для нашої держави, мережа інтернет може бути територією здійснення бойових дій, тому проблематика протидії несанкціонованого доступу є надзвичайно важливою та актуальною. Важливим кроком буде розширення правової та законодавчої обізнаності спеціалістів і посадових осіб, зацікавлених у протидії злочинам в сфері комп’ютерних технологій. З цього слідує значний рівень залежності України від закордонних комп’ютерів та інформаційних систем, які на сьогоднішній момент створюють додаткові ризики організованих хакерських атак, які здатні нанести значну шкоду владній, банківському сектору, енергетиці, транспортній та іншим інформаційно-комунікаційним мережам, законодавче реагування на питання посилення комп’ютерних правопорушень є важливим моментом. Приводом для цього можуть бути також взятий Україною курс на інтеграцію до світової співдружності, та відповідно до Програми інтеграції України до ЄС [37, с. 230].

Кібербезпека внесена до сфери національної безпеки. ЗУ «Про основні засади забезпечення кібербезпеки України» визначає способи досягнення кібернетичної безпеки, об’єкти та суб’єкти кібернетичної безпеки та кібернетичного захисту. Встановлено державну структуру кібербезпеки та розподіллено обов’язки між органами, основним напрямком діяльності яких є підтримка мирного кіберпростору. Очевидним стало те, що функціонал наданий КТ знайшов часте використання при здійснені багатьох злочинів [7, с. 1].

Кібернетичний простір отримав широкі масштаби, яке стало підґрунтям для вдосконалення злочинності. Нормативне регулювання кібернетичного простору в одній країні не має наслідок дотримання законодавства в іншій, тому на нашу думку є необхідним надати Інтернету статус, такий як у територій загального користування, це наддасть можливість застосувати відповідальність за незаконні дії в кібернетичному просторі відповідно до принципу кримінальної юрисдикції, що діє і на решті територій спільного користування. Іншими словами особа, що вчинила правопорушення у кібернетичному просторі, буде кримінально покарана відповідно до нормативно правових актів країни свого громадянства, але такий принцип може запрацювати лише у разі затвердження унікального законодавства користування всесвітньою мережею Інтернет та застосування правил обов’язкової співпраці між державами у розслідуванні правопорушень, що здійснюються у кібернетичному просторі та укладання міжнародних договорів про співпрацю [15, с. 156].

За для встановлення основних аспектів злочинів в сфері КТ, охарактеризуємо види комп’ютерних злочинів за законодавством України.

Інформаційні відносини існують у будь-якій сфері життя та діяльності людини і держави при отримані, зберіганні, поширені та використані інформації [38]. Фігель М.В. охарактеризовує інформаційні відносини, як врегульовані нормами інформаційного права суспільні відносини де суб’єкти, що беруть в них участь є носіями юридичних прав і обов’язків, які регулюють норми щодо встановлення, поділу та застосування інформації, що міститься в таких нормах [39, с. 234].

Значного розвитку в галузі інформаційно-телекомунікаційних систем отримали технології, що дотичні із мережею Інтернет, яке призвело до створення кардинально нових груп, таких як: електронний бізнес, електронний уряд, електронна торгівля [32, с. 262]. Основні плюси Інтернет технологій для здійснення наукових досліджень, цифрового бізнесу та господарської діяльності в інформаційному суспільстві призводять до появи загроз, де основною є масове застосування кримінальним світом новітніх КТ для обману, викрадень, відмивання коштів, поширення неправдивої інформації та інше.

Кіберзлочини включають багаторівневий характер зокрема: 1) комп’ютерне шахрайство з даними і програмами; 2) комп’ютерне піратство; 3) комп'ютерний саботаж; 4) комп’ютерний підлог; 5) незаконний доступ до систем комп’ютера [40, с. 263].

До незаконних дій у сфері КТ належать всі протиправні дії, у випадку яких електронна обробка інформації є предметом або знаряддям вчинення.

В загальному належать:

* неодноразове викрадення системного та/або прикладного програмного забезпечення;
* незаконне вторгнення у інформаційно-обчислювальну мережу або бази даних з корисливими намірами;
* незаконний перегляд чи викрадення інформації з баз даних;
* незаконне дублювання, коригування або видалення інформації;
* протиправне використання комп’ютерних систем задля аналізу або моделювання протиправних дій для їх вчинення у комп’ютерних системах;
* шантаж, інформаційне блокування або інші способи комп’ютерного тиску;
* комп’ютерне шпигунство та передача інформації особам, в яких не має доступу до неї;
* підробка комп’ютерної інформації;
* створення та поширення комп’ютерних вірусів в комп’ютерних системах та/або мережах;
* фізичні, електричні, електромагнітні або інші способи дії на інформаційно-обчислювальні системи та/або мережі телекомунікації, які призводять їх пошкодження;
* недобросовісність при розробці, запуску інформаційно-обчислювальних мереж та програмного забезпечення, яке має небажані наслідки та втрату ресурсів [41, с. 63].

Такий перелік на сьогодні невичерпним та весь час збільшується. Правопорушення в сфері комп’ютерних технологій в юридичній літературі поділяються по-різному, в більшості на три групи.

До 1-ої групи входять злочини, де комп’ютер чи дані в ньому є предметом здійснення протиправної дії.

До 2-ої групи входять злочини, де комп’ютер є знаряддям вчинення правопорушення.

До 3-ої групи відносяться злочини, доказовою базою яких є дані, які знаходяться в комп’ютерних системах [32, с. 264-265].

Кібернетичні правопорушення, як і решта будь-яких технологій весь час вдосконалюються, на підставі цього виникають кардинально нові види злочинних діянь. Деякі науковці під поняттям «кібернетичний злочин» мають на увазі злочинне діяння, яке вчинене в мережі Інтернеті під час якого комп’ютер є або знаряддям, або предметом посягання. Звідси виникає чимала кількість підвидів кіберзлочинів: 1) зневага; 2) кардерство; 3) поширення шкідливих програм; 4) екстремізм у мережах; 5) комп'ютерне шпигунство; 6) дефейс(заміна сторінок сайту); 7) онлайн шахрайство; 8) наклеп; 9) Dos-атаки [42, с. 77].

Найбільш розповсюдженими видами кіберзлочинів є наступні:

* *за допомогою платіжних систем:* 1) скімінг - вид шахрайства із банківськими картами, який полягає в зчитуванні і копіюванні інформації з магнітного чіпа; 2) кеш-трепінг - заклеювання отворів з видачі готівки з метою подальшого викрадення коштів після відходу клієнта від банкомату; 3) кардінг - вид шахрайства, в якому проводиться операція з використанням платіжних карток або їх реквізитів, яка не ініційована або не підтверджена власником; 4) незаконне привласнення грошових коштів з банківських поточних рахунків осіб з використанням систем віддаленого банківського обслуговування.
* *в галузі електронної комерції та комерційної діяльності:* 1) онлайн шахрайство; 2) фішинг.
* *в галузі інтелектуальної власності:* 1) піратство; 2) кардшарінг – це метод, завдяки якому декілька незалежних ресурсів можуть отримувати доступ до перегляду платних каналів супутникового чи кабельного телебачення шляхом використання однієї карти доступу.
* *в галузі інформаційної безпеки:* 1) соціальна інженерія; 2) malware; 3) заборонений контент; 4) рефайлінг та інші [43].

Давайте детальніше розглянемо перелічені види кібернетичних злочинів.

В галузі використання платіжних систем:

Скімінг (шимінг) протиправне копіювання змісту магнітної смуги банківських карток. Задля викрадення інформації з банківських карток правопорушники записують інформацію клієнтів на скриті камери. В той же момент до щілини, куди вводять пластикову банківську картку під’єднають спеціальний мініатюрний прилад, що зчитує та дублює дані по рахуну з магнітної стрічки. Одним зі способів вчинення такого виду злочину є встановлення на клавіатуру з цифрами точної копії, яка за своїми технічними можливостями може фіксувати пін-код власника картки. Викрадену такого роду інформацію правопорушники копіюють на чисті картки, що вбільшості виготовлені в іншій країні та переводять на особистий рахунок грошові кошти. Постраждала особа може і не помітити, що в неї списуються кошти, оскільки оригінальна картка весь час перебуває у власника.

Кеш-трепінг - заволодіння готівкою з банкомату в спосіб вмонтування на шатер банкомату спеціальної утримуючої накладки. Щоб здійснити такий злочин запломбовують отвір для видачі готівки в банкоматі спеціальною накладкою з клейкою смужкою на іншій стороні. Коли особа хоче здійснити операцію зі зняття коштів відбувається захват купюр і кошти приклеюються до клейкої стрічки, яка запобігає їх видачі власнику карти. Частіше всього осаба не отримавши коштів вирішує що сталася якась помилка роботи банкомату, або закінчилася готівка в ньому та вирішують йти до іншого, навіть не підозрюючи що проти них були вчинені шахрайські дії, після того, як людина відходить на безпечну відстань для зловмисника, він спокійно заволодіває коштами. Така операція може вчинятися декілька раз в одному й тому же місці.

Кардінг - протизаконні платіжні операції за участю платіжних карток або їх реквізитів, які не здійснювалися або не підтверджувалися її власником. Реквізити пластикових банківських карток можуть отримувати із ЕОМ, зі зламаних серверів інтернет-магазинів, платіжних та/або розрахункових систем, або за допомогою програм віддаленого взлому, наприклад вірусів троянів чи черв’яків. До найпопулярнішого злочину в галузі кардінгу належить злом глобального процесингу кредитних карток World pay та викрадення з його допомогою інформації більше 9 000 000 (дев’яти мільйонів) доларів.

Незаконне перерахування грошей з поточних рахунків за допомогою програми віддаленого банківського обслуговування [45, с. 194].

Незаконне втручання до електронних банківських рахунків і зміни даних, які містяться в них. Таким чином здійснюється переведення грошей на рахунки правопорушників. До прикладу, в Сполучених Штатах Америки шкода від шахрайських дій з кредитними картками у 1992році була більшою одного трильйона доларів США. Прибутки кіберзлочинців займають третє місці після прибутків від торгівлі наркотиками і зброєю. Після того як банки Канади виготовили в обіг близько двадцяти п’яти мільйонів кредитних карток, правоохоронці встановили, що більше 55 000 було використано у шахрайстві [32, с. 265].

У сфері електронної комерції та господарської діяльності:

Фішинг – отримання шляхом обману від користувачів Internet їх логінів та кодів до цифрових гаманців, сайтів онлайн аукціонів, переказування чи обміну валюти, та інше. В загальному злочинні дії спрямовані на те, щоб власники даних самостійно відкрили їх, до прикладу можна вказати наступне, відправляючи електронні повідомлення з проханням підтвердження реєстрації запису нового користувача, який має в собі шлях на веб-сайт, ззовні які точно копіюють дизайн оригінальних та відомих ресурсів. Фішинг являє собою вид соціальної інженерії, що існує на тлі необізнаності користувача загальним правилам комп’ютерної безпеки.

Онлайн шахрайство є викрадення грошей осіб через сайти, інтернет-магазини, інтернет-аукціони та телекомунікаційні засоби зв’язку;

У сфері інтелектуальної власності до поширених правопорушень належать:

Піратство - протиправне поширення інтелектуальної власності в Internet.

Кардшарінг - передача незаконного доступу до перегляду кабельного чи супутникового TV.

У сфері інформаційної безпеки:

Соціальна інженерія - метод керування людьми в Internet середовищі;

Мальваре - формування та поширення вірусів та/або шкідливого програмного забезпечення;

Протиправний контент - дані, які пропагують екстремізм, наркоманію, тероризм, порнографію, жорстокість та насильство;

Рефайлінг - протиправна заміна мобільного трафіку [45, с. 201].

Новітні технології йдуть вперед, безперечно будуть з’являтися нові види протиправних дій та посягань, і до цього слід готуватися.

З вище зазначеної класифікації можна встановити, що кібернетичних злочинів не стає менше, вони все частіше і частіше вкоріняються у наше життя, яке уже майже неможливо представити без комп’ютерних технологій. Більшу небезпеку несуть правопорушення 4 групи, оскільки вони безпосередньо здійснюються в найцінніших людських здобутках, свободи і незалежності. Також буде невірним не брати до уваги загрози, яку несуть комп’ютерні віруси, яких існує незліченна кількість, що мають можливість завдати значної шкоди як інформації, що зберігається на комп’ютерах чи у комп’ютерних мережах, та й і самій комп’ютерній техніці.

Отже, протягом уже тривалого періоду, науковцями вивчаються проблеми, пов’язані з бурхливим розвитком феномена, відомого в усьому світі під назвою «комп’ютерна злочинність».

Це складне нове явище в кримінально-правовій практиці, яке потребує більш досконалого спеціального і систематичного вивчення. Комп’ютерні злочини – це якісно новий вид злочинності в нашій країні, їх діапазон у світовій практиці надзвичайно широкий. Цей вид суспільно небезпечного діяння поки що залишається недостатньо вивченим.

На сьогоднішній день комп'ютерні злочини є однією з най динамічніших груп суспільно небезпечних посягань світового рівня. Швидке поширення цих злочинів стало зворотною, негативною стороною інформатизації, пов’язаних з протиправним використанням комп’ютерних технологій або так званими «кіберзлочинами».

**РОЗДІЛ 3. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В ГАЛУЗІ КОМП’ЮТЕРНИХ ТЕХНОЛОГІЙ**

**3.1. Початковий етап розслідування злочинів у галузі комп’ютерних технологій**

Проведене дослідження показало, що найпопулярнішими підставами відкриття кримінальної справи за ст. 361 КК України можна виділити:

* 40 % повідомлення надходили від посадових осіб організацій або їх об'єднань;
* 35 % подані заяви від громадян;
* 20 % напряму виявляли органи дізнання, прокурор або слідчий будь яку інформацію, що стосується скоєного злочину;
* 5 % інформація доходила шляхом ЗМІ.

Зібрана статистика вказує, що для порушення кримінальної справи за статтею 361 Кримінального кодексу України потрібно встановити наступні факти:

* Несанкціонований вхід виявлено в результаті користуванням комп’ютерними даними незаконним користувачем, можна навести приклад, при розсиланні інформації, що має конфіденційний характер.
* злочинець не був виявлений в несанкціонованому посяганні в функціонування комп’ютерних технологій, тоді коли законний представник виявив втручання;
* правопорушника було виявлено законним користувачем, шляхом фіксування інформації особи на ЕОМ;
* злочинця зловили на місці вчинення протипоказаного втручання в роботу комп’ютера;
* протизаконне втручання в роботу електронно-обчислювальної машини, без виявлення злочинця [46].

Для того щоб визначити підстави для відкриття кримінальної справи, потрібно виконати стандартні перевірочні дії:

* збір пояснень;
* огляд місця події;
* збирання матеріалів, які необхідні;
* виконання оперативно-розшукових заходів.

Щоб визначити причини відкриття кримінальної справи за статтею 361 Кримінального кодексу України обов’язково потрібно зібрати пояснення інженерів-програмістів – ці спеціалісти розробляли ПЗ і його обслуговували. Також необхідно зібрати пояснення спеціалістів, що займаються технічним забезпеченням та які контролюють безпеку комп’ютерів, операторів що займаються використанням і ремонтними робота КТ, інженерів та системних програмістів [47, с. 168-169].

Під час збирання пояснень необхідно вияснити:

* встановити носіїв даних на територія злочину;
* встановити особистий інтерес співробітників до корзин для відходів та сміття ;
* встановити маніпуляції зі сторони працівника з даними;
* встановити порушення встановленого принципу роботи будь яких комп’ютерних технік;
* встановити втрачену інформацію без причини;
* встановити активацію приладів захисту комп'ютерної системи;
* встановити присутність в будівлі з КТ сторонніх осіб, ви видавали себе за електрика, охоронця, сантехніка, телемайстра тощо;
* встановити факт допущення відхилень від норм ведення журналу обліку режиму роботи комп’ютерних програм, вияснити хто саме допустив помилку;
* встановити маніпуляції з даними, чи ніхто не змінював, не стирав без обґрунтованої причини;
* встановити роботу після закінчення робочий часу;
* встановити можливий інтерес співробітників до даних, що їх не стосується;
* встановити осіб, які перебували без причин у місцях з КТ, таких як інші підрозділи і служби організації;
* встановити незадоволених працівників над якими здійснювався нагляд за їхньою роботою;
* встановити працівник, незадоволених повсякденною роботою;
* встановити працівників, що легковажно віднеслися до своїх повноважень з засобами комп'ютерної техніки;
* встановити інші місця встановлення комп’ютерної техніки;
* встановити відповідність правилам безпеки комп’ютерів з процедурами техніки та управління;
* встановити жучки в телефонних апаратах, чи ніхто не прослуховував розмови [48, с. 315].

Відповідно до статті 150 Кримінального кодексу України, за особливих обставин можна провести огляд місця події до відкриття кримінальної справи [49].

Для того щоб виїхати на місце події, потрібно дотриматися обов’язкових підготовчих заходів:

* потрібно вияснити у людини яка має інформацію деталі про подію, а саме: дізнатися де, коли, за яких обставин розкрили злочин, хто повідомив про злочин що відбувся або відбувається у цей час;
* донести деталі про злочин та зв’язатися з працівниками компетентних служб, такі як: СБУ, МВС.
* брати участь в огляді місця події повинні професіонали з боку підприємства. Потрібно оголосити їхні права та обов'язки, відповідно ст. 128, 128-1 КПК України, пояснити про можливу відповідальність за відмову або ухилення від своїх обов'язків.
* особливою ознакою розслідування несанкціонованого втручання в роботу ЕОМ обов’язково під час слідчих дій повинен бути задіяний професіонал, це необхідно під час огляду місця події [36]. Після опитування спеціалістів інформаційних технологій - 92% вказали, що в час стрімкого розвитку комп’ютерів майже неможливо віднайти "секретні" деталі без спеціаліста, щоб її не знищити [49]. Саме слідчий повинен мати свій наперед продуманий список спеціалістів та вияснити їх професіональність, які допомагає йому в слідстві.
* запросити понятих, пояснити їм їх обов'язки, відповідно до статті 127 КПК України та попередити про недопустимість розголошення даних попереднього слідства, що стали їм відомими, відповідно до статті 121 КПК України [17].
* науково-технічні засоби мають бути справні та готові до роботи.
* здійснити інструктаж учасників слідчо-оперативної групи. В будівлі, де відбуватимемся огляд можуть знаходитися багато осіб, на яких потрібно звернути увагу слідчо-оперативної групи, а особливо на їхню поведінку, зробити комфортні умови для спеціаліста.
* запитати думку професіоналів, на рахунок огляду місця події, а саме КТ. Спеціалісти повинні надати деталі про комп’ютер, ЕОМ та їх мережі.

Після прибуття на місце події необхідно:

* зберегти всі предмети на своїх місцях, що зафіксовані під час огляду місця події, також переглянути справність охоронної системи будівлі, вияснити скільки кімнат з комп’ютерною технікою, сторонніх осіб вивести з приміщення, допитати свідків;
* не надавати можливості стороннім особам та спеціалістам залишати свої відбитки та переміщати обладнання;
* вияснити чи одна лінія зв’язку між комп’ютерами в всіх кімнатах;
* вияснити чи поєднані комп’ютери з обчислювальною технікою в інших будівлях;
* вияснити, комп’ютер з’єднаний чи ні з телефонною лінією;
* записати в протоколі опис зображення що на екрані комп’ютера, та зафіксувати програми, які бути запущені [50, c. 306].

Потрібно вказати яким способом злочинець вчинив протиправні дії з комп’ютерною технологією. Він міг використати різні види доступу: пошкодження роботи, знищення або копіювання інформації, модифікація.

Щоб це вияснити програмісту потрібно контролювати роботу програм, слідкувати за базами даних та вмістом текстових файлів. Якщо результат бути позитивний, потрібно знайти сліди пальців рук, які залишив злочинець на будь якому комп’ютерному обладнані. Після такого як все буде перевірено та зафіксовано, вся інформацію долучається справи відповідно статті 190 Кримінального кодексу України.

Практика показує для вияснення способу скоєння злочину потрібно не лише години а і дні, до такої роботи спеціаліст повинен бути готовий. Під час розслідування незаконного втручання в роботу ЕОМ бувають випадки, коли комп’ютери не перевозитимуть у спеціальне місце для повного дослідження техніки, у такій ситуації потрібно:

1) після перегляду засобів комп’ютерної техніки необхідно виключати мережі електропостачання і обов’язково перекрити будівлю, де був скоєний злочин;

2) носії комп’ютерних даних мають рухатися у просторі та зберігатися лише у спеціально опломбованих та екранованих контейнерах чи у стандартних дискетних чи будь-яких алюмінієвих футлярах заводського виробництва, що унеможливлюють руйнівний вплив будь-яких електромагнітних і магнітних випромінювань;

3) дані з оперативної пам’яті комп’ютера (ОЗП), потрібно вилучати способом копіювання потрібної комп’ютерної інформації на фізичний пристрій, застосовуючи стандартні легалізовані програмні засоби. В таких спосіб вони забезпечуються належним документальним додатком. В протоколі огляду місця події потрібно зафіксувати таке:

* наслідки роботи виявленої програми;
* програмний продукт, що виконується чи виконувався ПК у момент здійснення чи до моменту здійснення слідчої дії. Для цього потрібно детально вивчити та описати зміст речей на екрані монітора ПК, всі діючі при цьому додаткові пристрої та результат їх діяльності. Чимало сервісних програмних продуктів дозволяють встановити та переглянути назви усіх програм, що запускалися попередньо, в тому числі ту, що працювала в останню чергу. До прикладу, в разі використання NORTON COMMANDER, остання виконувана програма віднаходиться за положенням курсора миші, яке виділяється світловою рискою;
* дії з пристроями комп’ютерної техніки, в тому числі натискання на клавіші клавіатури, виконані під час проведення слідчих дій та їх результат (до прикладу, при копіюванні програмних продуктів та даних, визначенні їх характеристик, дати, часу створення та запису), а також при вмиканні чи вимиканні техніки, відключення її окремих частин;

4) конфіскація засобів комп’ютерної техніки вчиняється лише у вимкненому стані. В такому разі повинні бути здійснені та відмічені в протоколі наступні дії:

* встановлено вид пакувальної коробки та транспортування конфіскованих предметів;
* встановлена наявність чи відсутність мережі, використовувані канали зв’язку і телекомунікацій. В останньому випадку визначено техніка, що використовується, логін або робоча частота, серійний номер, тип зв’язку;
* зазначена черговість під’єднання між собою усіх пристроїв із вказанням особливостей такого з’єднання (габарити, колір, характерні особисті ознаки з’єднувальних кабелів, шлейфів, входів, штекерів та їх специфікація, кількісний показник,);
* зафіксовано ввімкнений режим техніки та зафіксовано порядок його вимикання;
* здійснене відключення, з дотриманням всіх обов’язкових заходів безпеки, апаратних частин, пристроїв з одночасним опломбуванням їх технічних виходів та входів;
* встановлене точне місцезнаходження об’єктів, що вилучаються та їх місце відносно один одного та оточуючих предметів, у разі потреби із долученням відповідних схем та планів [9].

Таким чином, викладений порядок проведення перевірочних заходів є підставою прийняття законного і обґрунтованого рішення про порушення кримінальної справи, виключення випадків необґрунтованого порушення кримінальної справи, дає можливість зібрати найбільшу кількість криміналістично-значимої інформації.

**3.2. Особливості проведення окремих слідчих дій**

Особливий і кардинально новий предмет дослідження, є саме інформація, яка знаходиться в пристроях комп’ютерної техніки чи обробляється ними, забезпечує практичні техніки здійснення провадження слідчих дій, таких як обшук, огляд, призначення експертиз, виїмка, які здійснюються для встановлення та дослідження матеріальних джерел криміналістичної справи [54].

На практиці є відчутним відсутність належних та наукових досліджень щодо порядку розслідування комп’ютерних правопорушень, які б містили рекомендації, щодо способів та методів їх вчинення, типових досудових та практичних ситуацій.

Над дослідженнями з питань криміналістичної проблематики здійснення розслідування злочинів у сфері КТ працювали такі науковці, як Рогозіна В.Ю., Крилова В.В., Козлова В.Є., Селіванова М.А., Вехова В.Б., та інші.

Встановлення важливих шляхів та способів розслідування і специфіка тактик окремих слідчих дій прямо або опосередковано залежить від змісту первинної інформації. Враховуючи це, у правовій літературі часто були спроби групування вихідної інформації і на підставі чого з’явилося визначення вихідної слідчої ситуації [54, с. 243]. Під таким поняттям розумілося інформаційне середовище, яке об’єктивно створилося на первинних етапах розслідування [28].

В залежності від змісту вихідної інформації при розслідуванні злочинів у сфері комп’ютерних технологій, систем або мереж та після відкриття кримінальної справи можуть моделюватися різні слідчі сценарії.

І.М. Шумилов виділяє наступні види слідчих сцен в залежності від змісту вихідної інформації, де за основу бере первинний етап розслідування інформаційних правопорушень:

* відкриття кримінальної справи за інформацією в ЗМІ або інформацією публічних промов;
* відкриття кримінальної справи щодо однієї або декількох осіб, які були затримані при здійсненні діяльності, яка має ознаки злочинів щодо інформації;
* відкриття кримінальної справи за даними перевірок при присутності ознак складу правопорушення в галузі інформаційної безпеки;
* відкриття кримінальної справи за заявою та/або скаргою юридичної чи фізичної особи;
* відкриття кримінальної справи за даними наявності наслідків техногенного змісту де присутня матеріальна шкода та/або людські жертви [55, с. 108].

На нашу думку, враховуючи сукупності вихідних даних, які були отримані під час проведення перевірочних дій на початковому етапі розслідування можуть бути такі слідчі ситуації:

* встановлено протиправне втручання в роботу комп’ютерів їх систем і мереж, встановлені особи, що відповідно до свого службового становища несуть за це відповідальність, але зміст їхньої винуватості та обставини доступу не викриті органами розслідування;
* встановлено протиправне втручання в роботу комп’ютерів їх систем і мереж, де чітко прослідковується слід, що веде до підозрюваного, який у свою чергу свідчить правдиво;
* встановлено протиправне втручання в роботу комп’ютерів їх систем і мереж, де чітко прослідковується слід, який чітко викриває підозрюваного, проте той у свою чергу категорично відмовляється визнавати свою причетність до правопорушення;
* встановлено протиправне втручання в роботу комп’ютерів їх систем і мереж, де чітко прослідковується слід, що веде до підозрюваного, який у свою чергу свідчить правдиво;
* встановлено протиправне втручання в роботу комп’ютерів їх систем і мереж, вчинити яке і використати результат такого втручання могли лише особи з обмеженого кола, зокрема які використали своє становище, професійні вміння та знання [56, c.75].

Одна із вище вказаних слідчих практик є найбільш складною, у зв’язку з тим, що відсутні дані про винність особи, сліди вчинення правопорушення, не встановлений спосіб вчинення.

Для знаходження відповідей на слідчих ситуацій, які формуються після відкриття кримінальної справи, здійснюються такі слідчі дії: 1) огляд приміщень; 2) призначення відповідних експертиз; 3) допит підозрюваного; 4) опитування свідків; 5) звірка з оперативними довідниками; 6) перегляд розшукових і криміналістичних обліків.

Під час приготування слідчим до допиту, він може звернутися за допомогою до спеціаліста у сфері КТ, де роз’яснення та відповіді останнього будуть сприяти, на нашу думку, вірному розумінню змісту та суті розслідуваного правопорушення (злочину), правильному встановленню групи обставин, які матимуть доказовий зміст та сприятимуть вірному та безпечному процесу підготовки речових доказів та інших доказів по справі, які потребують обов’язкового дотримання відповідних умов та правил їх зберігання, перевезення та наступного поводження з ними, що повинно звести до мінімуму можливість їх пошкодження або втрати під час проведення слідчих дії.

Під час підготовки до порядку здійснення і поетапного проведення допиту, слідчому необхідно:

* підготувати не легкі для правопорушника питання, потрібно їх сформувати так, щоб у правопорушника не було змоги обмовитися чи вчинити самообман;
* встановити умови, для яких необхідно здійснити уточнення інформації. До таких належать: інформація про потерпілу сторону, механічні і конструктивні відмінності комп’ютерної системи, яка зазнала впливу, засоби комп’ютерної техніки, якими користувався правопорушник, про особу потерпілого, особу підозрюваного;
* встановити особливості злочину, а головне питання, які відносяться до технічної сторони підготовки та втілення замислу злочинця [57, c. 97].

В такій не легкій для розуміння сфері знань, як комп’ютерні технології, злочинець, добре володіє спеціальними термінами, може запросто спеціально занизити свої знання або навпаки зависити ніж є реально. Задаванні питання та їх черговість повинні бути такими, щоб особа, що здійснює допит могла з легкістю контролювати вірність отриманих відомостей.

Тому, під час підготовки питань може бути необхідна кваліфікаційна допомога спеціалістів з різних сферах знань, до прикладу спеціалістів у сфері програмного або апаратного забезпечення комп’ютерів:

* звернути увагу на підготовку наукових та технічних засобів фіксації процесу розслідування;
* зібрати доказову базу або інші докази для аргументування ними в разі потреби, за умови дотримання їх цілісність [58, c.75].

Визначення території та часу здійснення допиту, його порядок по відношенню до інших слідчих дій здійснюється відповідно з наявною слідчою ситуацією. Обсяг запитань, що варто встановити при допиті свідків, змінюватимуться відповідно до особи що допитується та способу здійснення правопорушення.

Під час розслідуванні протиправного втручання в роботу комп’ютерної техніки, систем та мереж на первинному етапі в ролі свідків допитуються громадяни різних держав де для кожного з них наявні свої особливості.

Законодавчі акти вирізняє три види обшуку: 1) обшук на території вчинення правопорушення; 2) індивідуальний обшук 3) обшук приміщення.

При здійснені обшуку приміщення де розташована комп’ютерна техніка, потрібно брати до уваги особливості комп’ютерної інформації. Давайте запропонуємо особливі тактичні прийоми, передбачення яких на нашу думку, може забезпечити позитивний результат пошуку й вилучення комп’ютерних даних під час здійснення слідчих дій [59, с. 59].

Під час підготовки до обшуку необхідно:

* протестувати належну комп’ютерну техніку, що буде застосовуватися для вилучення та зберігання вилучених даних;
* передбачити суть даних, які зберігаються у ПК, їх роль в оперативному та результативному обшуку та встановити, які саме комп’ютерні дані слід дослідити на місці, а які конфіскувати для наступного вивчення;
* залучити фахівця з комп’ютерних технологій, якщо його навички потрібні протягом підготовки до обшуку, а також для швидкого аналізу даних і спеціалізованого їх вилучення;
* дослідити особу власника комп’ютерної техніки, наявні в нього вміння та навички у володінні технікою;
* встановити чи комп’ютерна техніка перебуває в приміщенні в якому здійснюється обшук, та встановити її кількісний склад;
* встановити часові межі збору даних, який забезпечить їх конфіденційність;
* визначити чи застосовуються разом зі комп’ютерною технікою засоби автономного або безперебійного живлення, та встановити що може спричинити вимкнення електроживлення [60, с. 157].

На підготовчому етапі обшуку потрібно перш за все забезпечити безпеку комп’ютерів. Заборонити доступ до них усіх присутніх у приміщенні. Потрібно розуміти, що зміни чи знищення даних може призвести не лише робота з клавіатурою, але й також вмикання або вимкнення ПК. Отже, якщо під час входу до приміщення ПК був увімкнений, то він має бути увімкненим до повного його огляду фахівцем, та навпаки власника приміщення або працівника електронно-обчислювальної техніки не варто допускати до неї, навіть якщо обшукуваний дає згод на добровільну видачу даних, що цікавлять розслідування. Будь-які дії з комп’ютерною технікою повинен здійснювати запрошений фахівець. Будь-які спроби будь-кого вчинити що-небудь з ЕОМ чи клавіатурою, сюди відноситься вимикання та/або вмикання ПК варто розцінювати, як спробу знищення даних в ПК і таку спробу потрібно описати у протоколі.

На стадії огляду під час обшуку потрібно:

1) встановити факт під’єднання ПК до модему;

2) вияснити чи підключений ПК до техніки яка знаходиться за межами приміщення де здійснюються оперативні дії.

Свідчити про те, що ПК працює не в режимі очікування наступної команди, а здійснює виконання попередньо поставлених завдань, може спостерігатися в такому випадку:

* на екрані монітору є інформації, яка свідчить про роботу програми.

Така інформація може бути окреслена кольором або виділятися контрастністю повідомлення чи виділено рядок тексту на екрані меню;

* спеціальні знаки на моніторі, що міняється, такі як рухома стрічка, знак, який змінює місце розташування;
* сигналізування лампочки жорсткого диску, CD-ROM, гнучкого диску. Такий індикатор розміщений на лицьовій стороні, а його увімкнений або миготливий стан сигналізує передачу даних, або легке потріскування чи шелест CD-ROM або інших носіїв даних. Схожими ознаки роботи зберігачів даних присутні і в переносних накопичувачах.

У разі встановлення, що на момент проведення слідчої дії на комп'ютері запущені які-небудь програми, спеціалістові необхідно вжити заходів до їх призупинення;

3) встановити чи підключені ПК, що перебувають в приміщенні у єдину локальну мережу;

4) перевірити наявність на ПК даних, що можуть допомогти розслідуванню. Таку професійну перевірку може здійснити лише спеціаліст шляхом огляду даних, що знаходяться на жорсткому дискові;

5) встановити, чи є будь-які запущені програмні продукти на ПК і які саме. Щоб це здійснити потрібно переглянути зображення на ПК, детально їх охарактеризувати у протоколі [51, с.98].

Основний етап обшуку є занадто об’ємним та потребує великих знань та кваліфікованості не тільки фахівця з комп’ютерних технологій, але і всієї слідчо-оперативної групи. Окрім особливих маніпуляцій з ПК, на даному етапі також необхідно вірно забезпечити розшукові дії, які направлені на знаходження схованок де можуть перебувати звичайні документи чи предмети.

Значну частину даних, які знаходяться та обробляється ПК завжди можна продублювати на переносні гнучкі магнітні дискети. Процес відшукування цих носіїв потрібний та обов’язковий, у зв’язку з тим, що такі носії інформації мають невеликі об’єми, діаметром до 150 міліметрів і товщиною 2 міліметри, то таке їх виявлення стає не легким. Якщо фахівець не має змоги перевірити носії інформації на місці, то вони повинні бути конфісковані для наступного їх дослідження, за умови дотриманням всіх процесуальних норм.

Для збереження даних, крім дискет, можуть слугувати лазерні диски та магнітофонні стрічки. Такі лазерні диски нічим не відрізняються від аудіо дисків чи відеодисків, що надає можливість їх наступного зберігання біля музичної чи відео колекції.

Така ж річ з магнітофонними чи відеокасетами. Зазвичай смужка для збереження комп’ютерних даних має незвичайні розміри, дещо посереднє між аудіокасетою та відеокасетою. Але є магнітофони, які в комп’ютерній техніці носять назву стримери, які записують дані в комп’ютерному форматі на звичайні відео чи аудіо касети.

Віднаходження сховищ з CD-дисками, дискетами, магнітними стрічками стає складнішим через те, що неможливо застосувати металошукачі чи інше пошукове обладнання у зв’язку з тим, що таке використання може завдати шкоди або знищити дані на носії. Щоб запобігти небажаного знищення даних, носії інформації в більшості зберігають у залізних захисних скриньках [61, c.115].

Магнітні носії даних можуть бути залучені до кримінальної справи як речові докази, у разі дотриманням передбаченого в Кримінально-процесуальному кодексі порядку.

Якщо в час обшуку ПК був увімкненим, то на носій інформації потрібно продублювати програми та файли, що знаходилися на віртуальному дискові чи в оперативній пам’яті комп’ютера.

У разі відсутності можливості оперативного аналізу великих об’ємів даних на ПК, її краще всього конфіскувати для наступного дослідження. Пристрої на які ведеться копіювання повинні бути належним чином запаковані та запечатані.

У разі, коли у використанні оперативної-слідчої групи відсутні портативні ПК, що записують CD-ROM, буде достатньо конфіскувати жорсткий диск, або диски, якщо їх не один, зі знайденого ПК. Конфіскація повинна здійснюватися з дотриманням всіх процесуальних норм законодавства. При конфіскації диску необхідно здійснювати відеозапис такого процесу.

У разі, якщо в складі групи відсутній фахівець з КТ, який може вірно провести відключення жорсткого диска, то буде доцільним здійснити вилучення всього ПК.

Коли в місці обшуку декілька ПК чи фахівець не впевнений в здатності огляду комп’ютерних даних при конфіскації одного системного блока, потрібно вилучити весь ПК. В такому випадку потрібно: 1) здійснити фотофіксацію комп’ютерної техніки в складеному та розібраному вигляді; 2) обережно запакувати кожен окремий пристрій та з’єднувальні дроти; 3) вірно та точно прописати порядок підключення між собою пристроїв ПК [61, c.125].

У більшості ПК не дивлячись на їхню високу вартість відсутні заводські та серійні номери, що значно унеможливлює їх пошук та ідентифікацію. Але такий номер повинен бути на жорсткому дискові, дисководах, магнітних носіях та материнській платі, у зв’язку з тим, що ці механізми є основними і найдорожчими, тому таку ідентифікацію ПК можна провести за їх серійним номером.

На вирішальній стадії слідчих дій формується протокол і описи до нього, малюються план і схеми будівель в яких здійснювався обшук, здійснюється додаткова фото та відео фіксація.

Під час допиту особи-підозрюваного в усіх окремих випадках потрібно отримати відповіді, що найменше на такі питання:

* В якому місці та на якій посаді працював підозрюваний?
* Чи володіє підозрюваний навичками роботи на ПК? Чи має будь-яке програмним забезпеченням? Який рівень його спеціалізації?
* В якому місці та на якій посаді працював підозрюваний?
* Яким способом підозрюваному вдалося проникнути до комп’ютерної мережі;
* Які системні коди та паролі закріплені за ним, в тому числі при роботі в мережі?
* Які типи дій з комп’ютерними даними особа здійснювала на момент дослідження?
* Хто передав вміння його працювати з окремими програмними продуктами?
* До яких комп’ютерних даних у нього є доступ? Які дії з даними має право здійснювати? Яка в нього категорія доступу до даних?
* Звідки чи від кого підозрюваний взнав про зміст даних, до яких здійснив правопорушення?
* доступ до яких програмних продуктів має підозрюваний? Місце його походження? Чи фіксувалися програми незрозумілого походження [62, c.97]?

На початковій стадії розслідування злочинів у сфері комп’ютерних технологій обов’язково проводять експертизу. Експертизи є різних видів: економічні, криміналістичні, також проводять експертизи на речовинах та матеріалах. Сукупність експертиз залежить від механізму та способу вчинення злочину.

В списку інженерно-технічних експертизи також є комп'ютерно-технічна, що має пряме відношення до злочинів у сфері комп’ютерних технологій, їх можна розділити на два види:

* технічна експертиза комп’ютерної техніки та їх комплектуючих здійснюється шляхом дослідження особливостей, будову техніки, досліджують периферійні пристрої та магнітні носії даного комп’ютера, також потрібно вияснити через що виникли проблеми з роботою комп’ютера;
* експертиза даних та ПЗ(програмне забезпечення) виконується шляхом дослідження даних, які залишилися на обладнані [63, c. 113].

Комп'ютерно-технічну експертизу, розділяють на різні види, такі як:

* технічна експертиза комп’ютерної техніки, ця дія відбувається для того щоб дослідити всі деталі та нюанси технічного обладнання, в тому числі і комп’ютера;
* технічна експертиза техніки, що має за мету захистити інформацію що в робочому комп’ютері;
* експертиза даних в комп’ютері та ПЗ Електронно-обчислювальної машини, що має на меті дослідити інформацію, що залишилася на ПК та на портативних зберігачах даних, також дослідити способи захисту комп’ютерних даних;
* експертиза інформації системного забезпечення, що застосовуються в мережі Internrt, що має на меті дослідити інформацію, що використовується в мережі Internrt.

Прослідковуючи статистку судових справ, зазвичай також назначають сукупність різних експертиз, таких як:

* дактилоскопічну;
* експертизу речовин і матеріалів;
* комп'ютерно-технічну експертизу;
* техніко-криміналістичну експертизу документів.

Для того щоб допомогти виконати експертизу у сфері комп’ютерної техніки, буду обговорюватися наступні запитання:

* Вилучений комп’ютер та технічне обладнання, які його технічні характеристики (модель)?
* В якому стані комп’ютер та технічне обладнання, чи можна нею користуватися?
* Перевірити чи збігається інформація зазначена в документах з характеристиками технічного обладнання.
* Які умови складання комп'ютера і його комплектуючих: фірмове збирання, збирання з комплектуючих на іншій фірмі або кустарне збирання? Чи всі пристрої представленні для експертизи, чи залишилися без уваги додаткові обладнання?
* Чи не було проведені зміни в комп’ютері для особливого користувача, наприклад якщо він лівша або в нього проблеми з зором?

Для того щоб виконати експертизу техніки, що має за мету захистити інформацію будуть обговорюватися наступні запитання:

* Технічні деталі пристроїв, що були залучені для захисту інформації;
* Перевірити наявність документів в яких зазначалися вся характеристика про пристрої, та відповідність з дійсністю;
* Чи піддавалися програми захисту змінам чи фізичному впливові? Чи застосовуються неофіційні способи засоби інформації?

До предметів комп'ютерно-технічних експертиз не враховуючи стандартні технічні обладнання, можна віднести: електронні записні книжки, пейджери, мобільні телефони, електронні касові апарати, інші електронні носії текстової або цифрової інформації, документації до них. При експертизі вказаних пристроїв обговорюють вже зазначені питання.

Пропоную розглянути погляди науковців П. Д. Біленчука та Б. В Романюка. На їхню думку, в розслідувані комп’ютерних злочинів стандартний етап – експертизу, можна застосовувати не у всіх випадках, а також було доречно використовувати слідчий огляд або слідчих експеримент. Можна навести приклад, щоб підтвердити їхню теорія – коли слідчий достатньо кваліфікований, щоб самостійно задокументувати потрібну інформацію про комп’ютерну техніку, таку дію можна відмітити як слідчий огляд за участю спеціаліста, без додаткової технічної експертизи [64, c.34].

Щоб дослідити окремі пристрої ПК, програмні продукти та операційні системи, необхідно звертатися до інженерів-електронників та до програмістів. Також якщо потрібно дослідити специфіку рамок співвідношення загальних та місцевих комп’ютерних мереж потрібно запитати думку професіоналів, що працюють у сфері електричного зв'язку.

На інженерно-технічній експертизі перелік спеціалістів у сфері комп’ютерних технологій не закінчується. У випадку залучення експертів других сфер де використовують комп’ютер слідчий має обов’язок підготувати питання до експертів відповідно до їх кваліфікації. Така практика може скластися позитивно для вирішення справи. Для того щоб вивчення технічних приладів пройшло без проблем, потрібно щоб все було підготовлено [65, c.54].

Вказані необхідні умови використовують на практиці для того щоб, вірно та без помилок задокументувати інформацію про отримані речові докази. Ці вимоги маю за мету створити всі умови, які необхідні для вияснення їх співвіднесення до справи розслідування та оцінки правдивості встановлених даних. Процесуальний порядок, що закріплений у нормативно-правових актах гарантує законність речових доказів закріплених у справі, тобто ці закони забезпечують неможливість замінити та фальсифікувати докази.

Дослідивши особливості проведення окремих слідчих дій, можна зупинитися та розглянути помилки, які здійснюють слідчі у сфері комп’ютерних технологій.

До основної помилки можна віднести: некоректну роботу з комп'ютером. Щоб уникнути такої ситуації, ні за який обставин не використовувати конфіскований комп’ютер, тому що він є предмет для вивчення спеціалістів. Рекомендовано вилучений комп’ютер не запускати в роботу перед експертизою, тому що експерти для дослідження використовують спеціальні програми для захисту інформації. Часто користувачі встановлюють захисний пароль для включення ПК, тому якщо не спеціаліст спробує відключити пароль це може призвести до знищення всіх даних.

Друга розповсюджувана помилка: доступ до ПК його законного користувача. Щоб не допускати даної помилки потрібно зробити резервні копії даних що є на комп’ютері, і лише після того допускати користувача. Перш, ніж надати доступ до комп'ютера, слід зробити резервні копії комп'ютерної інформації.

До третьої помилки можна віднести: не здійснення стандартної перевірки на віруси та програмних закладок [66]. Щоб уникнути цю помилку потрібно здійснювати запуск комп’ютера не особистої операційної системи. А завантажувати з магнітних носіїв, які потрібно спеціально підготувати.

Потрібно зробити все можливе, що суддя не піддав сумніву слідчі дії в умисному зарядженні вірусами та не професійності слідства, також щоб не обвинуватив в недбалості. Динний висновок судді оспорити дуже складно, бо вияснити, коли вірус був занесений в комп’ютер не можливо, що призводить до помилкових висновків експерта.

Щоб не допускати помилок, які можуть зашкодити слідчим діям, розпочинаючи перший етап слідчих дій - огляд комп'ютера, слідчий та експерт, повинні дотримуватися таких запобіжних заходів [67]:

* для початку закрити всі активні програми потім вимикати комп’ютер, тому що неправильний вихід з програм, що використовувалися, може призвести до знищення інформації;
* зробити все можливе, щоб встановити пароль допуску до захищених програм;
* відключити електроенергію комп'ютерів, що виявлені у приміщені, вилучити у спеціальне місце для вивчення даних та опечатати;
* провести допит у різних співробітників організації, якщо це потрібно. Завдяки даної дії можна отримати правдиву та користу інформацію для слідства;
* необхідно конфіскувати всі суміжні технічні обладнання що є у приміщенні (принтер, сканер, модем);
* якщо є місцева обчислювальна мережа, потрібно залучати фахівців з вивчення інформаційної мережі
* детально ознайомитися з документацією, особливо звернути увагу на записи, що робили оператори електронно-обчислювальної машини. Нерідко буває так, що саме в таких нотатках некомпетентних користувачів можна виявити потрібні паролі та багато корисної інформації;
* зафіксувати усіх співробітників що працюють на організації, підприємстві, для того щоб знайти спеціалістів в інформаційних технологіях. Після чого потрібно встановити та записати паспортні дані та адресу проживання;
* всіх особи, які були у приміщенні, потрібно затримати та зафіксувати їх дані, не беручи до уваги причину їх перебування у приміщенні;
* окремо записати дані всіх працівників, які мали можливість працювати з комп’ютерною технікою або перебувати у тому приміщення де знаходилося обладнання [68, c.54].

На первинному етапі розслідування злочинів у сферу комп’ютерних технологій, слідчому необхідно звернути увагу на рекомендації, що запропонують, тому що вони впливатимуть на:

* правильній оцінці інформації про події;
* первинність слідчих дія;
* логічне застосування спец знань і технічно-наукових засобів способів.

Щоб позитивно пройшли всі етапи слідчих дії буде недостатньо вирішити лише запитання з технічної тактики на першому етапі підготовки. Під час слідчих дій слідчий повинен бути готовим до особливостей, що будуть виникати, що характеризуються:

* особливими умовами проходження слідчих дій;
* порядком і вимогами їх відкриття;
* унікальністю інформації доказування, яка була вилучена в результаті попередній слідчих дій [69, c. 198].

Отже, можна зробити висновок, що у спеціалістів виникають проблеми у виконані своєї роботи на високому рівні, тому що початковий етап розслідування злочинів у сфері комп’ютерних технологій не закінчується слідчими діями, які були зазначені. Також проведене дослідження показало, що може підвищити ефективність та якість розслідування, а саме специфіка тактики проведення окремих слідчих.

**ВИСНОВКИ**

З проведеного дослідження можна зробити висновок, що сучасні технології є дуже важливою складовою життя кожної особи, це характеризується глобальним використанням в різних сферах людської діяльності новітніх технологій. Велика кількість підприємств та організацій щоденно використовують їх у свій щоденній роботі.

Але в розвитку сучасних технологій є негативна сторона, що заключається у злочинах у сфері комп’ютерних технологій. Злочинні дії можуть здійснюватися у різних діяльності: політичній, економічній та технічній сферах.

Хоча комп’ютерні злочини і та й самі комп’ютерні технології з’явилися не так давно, але уже тривалий період, науковцями вивчаються проблеми, пов’язані з бурхливим розвитком феномена, відомого в усьому світі, що називають «комп’ютерна злочинність».

Тому, стрімкий розвиток технологій та наукові відкриття в цій сфері має свої позитивні і негативні наслідки. Зокрема позитив – це створення першого ЕОМ, його активне застосування в сферах оборони, фінансовому ринку, комерційній сфері і т.д., що призводить до виникнення нового виду злочину, які вчиняються за допомогою цих же технологій, що потребує швидкого реагування на державному рівні відповідних органів, з метою їх запобігання, виявлення, розслідування та ліквідації таких злочинних наслідків.

Можна сформулювати визначення комп’ютерної злочинності – це небезпечні дія чи бездіяльність для суспільства, що виконується за допомогою комп’ютерних технологій та технічного обладнання шляхом неправовірних дій в сторону держави, громадян та підприємств, та правам окремої особи.

Сформульоване визначення комп’ютерної злочинності дозволяє зробити висновок, що це складне нове явище в кримінально-правовій практиці, яке потребує більш досконалого спеціального і систематичного вивчення. Комп’ютерні злочини – це якісно новий вид злочинності в нашій країні, їх діапазон у світовій практиці надзвичайно широкий. Цей вид суспільно небезпечного діяння поки що залишається недостатньо вивченим.

Отже, у зв’язку з широким переліком сфер застосування комп’ютерних технологій в повсякденній діяльності, а в деяких із них, неможливість діяльності без таких технологій, в практиці можливе знищення потрібної інформації, все через те що користувачі користуються комп’ютером як «безпечним складом» для важливої особистої та робочої інформації. На жаль велика кількість користувачів не знайомі з засобами захисту інформації в комп’ютері, що є необхідним для оборони від злочинців. Тому для того щоб не стати потерпілим злочину у сфері комп’ютерних технологій, потрібно кожному спеціалізуватися в даних питаннях.

В сучасному світі злочини у сфері комп’ютерних технологій стрімко розвиваються на світовому рівні. Динамічне розширення цих злочинів по всьому світі утворило негативний результат інформатизації, головною причиною є незаконне використання цих технологій, тобто «кіберзлочин».

Ці чинники вплинули на те, що у КК України з 2001 року, комп’ютерним правопорушенням виділений окремий розділ, що зазнав кардинальних змін з часу його першого написання. Відповідно до нормативно-правових актів, родовим об’єктом злочинів в сфері КТ є зафіксований порядок користування автоматизованими електронно-обчислювальними машинами, їхніми системами та комп’ютерними мережами і каналами електронного зв’язку. Основним об’єктом є право власності на інформацію, щодо якої її законним володільцем встановлюється особливий режим користування або таке користування забороняється взагалі для інших користувачів з метою унеможливити доступність до такої інформації з різних особистих підстав.

Предметом таких злочинних дій є комп’ютерні пристрої, системи електронно-обчислювальних машин, мережа, зберігачі комп’ютерних даних, комп’ютерні віруси, комп’ютерні дані та інформація, програмні, системні та технічні засоби для протиправного проникнення. Злочини в сфері КТ є протиправними діями з матеріальним складом. Пізнання об’єктивної сторони комп’ютерних правопорушень має на своєму шляху низку проблем, зокрема пов’язаних з питанням встановлення часу, способу та місця вчинення правопорушення.

Суб’єктивною стороною злочинних дій в сфері КТ є лише провина у формі непрямого або прямого умислу.

Суб’єктом злочинних дій може бути особа, якій до моменту вчинення правопорушення виповнилося шістнадцять років. Кримінальна караність за два з них може бути застосована лише щодо осіб, які мають ознаки спеціального суб’єкта, тобто: 1) відповідають за експлуатацію ПК, автоматизованих систем, мереж чи мереж електронного зв’язку – стаття 363 КК України; 2) мають право доступу до інформації – стаття 362 КК України.

Основними ознаками усіх проаналізованих правопорушень, крім злочину, встановленого у статті 363 КК України, є як наслідок заподіяння ними значних збитків, вчинення їх повторно або за попередньою змовою групою осіб. Законодавча база та судова практика з вирішення справ по злочинам у сфері КТ в Україні має кілька «білих плям» та суперечливі питання, що необхідно вирішувати як нормотворцям, так і науковцям.

Особливо кваліфікуючими ознаками слід зазначити вчинення правопорушення спеціальним суб’єктом, таким як адміністратор телекомунікаційної мережі або комп’ютерних систем, та спричинення правопорушенням шкоди в особливо великому розмірі чи інших тяжких наслідків.

Тому, можна сміло стверджувати, що вчиняють злочинні дії цієї категорії злочинів найчастіше особи із спеціальною підготовкою в галузі автоматизованої обробки даних, причому, більша їх половина у складі злочинного угрупування. Основна небезпека прослідковується від внутрішніх користувачів, якими вчиняється більше 90 % правопорушень.

Стандартними слідчими діями, які використовуються при розслідуванні правопорушень у сфері КТ є слідчий огляд, допит потерпілого, підозрюваного, обвинуваченого, свідка, вчинення судово-інформаційно-технічних експертиз, обшук і вилучення, та слідчий експеримент. Слідчий повинен застосовувати свої професійні службові криміналістичні навички, методи, прийоми і засоби криміналістичної техніки за для пошуку, вилучення і фіксації доказів.

На попередній стадії огляду чи обшуку основним є: 1) отримати інформацію про вид і конфігурацію ПК; 2) можливої наявної локальної мережі чи підключення ПК до глобальної мережі Internet; 3) присутності служби безпеки інформаційної; 4) захист інформації від незаконного доступу, за для попередження автоматичного пошкодження чи повного знищення комп’ютерних даних, які можуть бути пошкоджені під час відкриття кришки ПК, відмикання приміщення, де знаходиться ПК, або при інших обставинах; 5) стану системи електронного забезпечення приміщень, в якому встановлена комп’ютерна техніка, рівень обізнаності користувачів, а також відносини співробітників в колективі, які обслуговують комп’ютерну техніку. На попередньому (підготовчому) етапі потрібно скласти план здійснення огляду.

Під час розслідування правопорушень в сфері КТ, здійснюючи слідчі та розшукові дії потрібно не забувати, що всі правопорушення вчиняються за допомогою ПК, це значить, що залишаються сліди на носіях даних комп’ютера, а саме на флеш-картках, вінчестерах, СD-дисках та інших носіях. Завчасне виявлення комп’ютерних засобів і пристроїв, вірне їх відключення впливатиме на ефективність наступної комп’ютерної експертизи, яка призначається з метою закріплення і вилучення даних, що розміщені на пристроях зберігання і встановлення, таким чином, визначених слідів кримінально караної діяльності.

Можна сказати, що злочини в сфері комп’ютерних технологій стали розповсюдженими та актуальними, як для всього світу, так і для України за 30 років їх становлення і розвитку. Загальноприйнятого поняття злочину в сфері комп’ютерних даних в чинному законодавстві України досі не зазначено, але в більшості випадків воно трактується, як правопорушення, об’єктом посягання якого є технічні засоби, комп’ютери та їх периферія.

На нашу думку, ефективними методами боротьби з кібернетичною злочинністю є: 1) забезпечити технічним обладненням органи досудового розслідування; 2) встановлення кардинально нових та гнучких способів фіксації (виявлення) та обробки (дослідження) обставин вчинення таких правопорушень; 3) вдосконалення способів та методів проведення слідчих дій.

Головною умовою протидії та боротьби зі злочинами в сфері КТ є підготовка персоналу та їх належної спеціалізації для підвищення ефективності розслідування та розкриття злочинів цієї сфери.

Наведені вище нами особливості методів проведення кожної окремої слідчої дії, зокрема допит свідків, обшук приміщень, допит підозрюваних, огляд місця події, та перевірочні заходи, такі як витребування матеріалів, отримання пояснень, під час розслідуванні правопорушень у сфері використання КТ, систем та комп’ютерних мереж забезпечать підвищення якості та ефективність слідчих дій, а також отримати більший обсяг доказів.

Для належного протистояння онлайн злочинцям потрібні багато структурна інституційна система кібернетичної безпеки, що захищала б не лише державні інститути а і простих громадян. Структура кібернетичної безпеки складається з різноманітних компонентів, в тому числі підвищення рівня цифрової обізнаності громадян, допомога в поширені особистих засобів захисту даних, шляхи та способи з протидії та профілактики кібернетичних загроз. Таким спеціальним підрозділом може стати Департамент кіберполіції Національної поліції України.

Для попередження злочинів в сфері КТ необхідно здійснювати наступні заходи:

* Інформаційну та аналітичну роботу;
* Формування спецпідрозділів технічного захисту даних в державних органах, збройних силах, органах внутрішніх справ, на підприємствах, організаціях, установах будь-якої форми власності, діяльність яких дотична з інформацією, що потребує технічного захисту;
* Підготовка працівників для роботи у сфері технічного захисту даних.

Тому, на теперішній момент злочини в сфері КТ є однією з най стрімкіше розвиваючих груп суспільно небезпечних посягань міжнародного масштабу. Активне поширення таких правопорушень стало зворотною, а саме негативною стороною комп’ютеризації населення, тому вдосконалення методів, способів, принципів, навичок їх розслідування є основним і важливим питанням, яке потребує постійного нагляду і відшукування на нього відповідей.

Злочини із використанням КТ стають все біль розповсюдженими, але вони і досі залишаються феноменами, оскільки наука ще не в змозі точно встановити законодавче регулювання караності за дані правопорушення, оскільки останні мають безліч особливостей, що і сприяє появі нових або модернізованих видів злочинів в сфері КТ.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Ричка Д. О. Історичні аспекти кіберзлочинності. Матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених «Сучасний стан і перспективи розвитку держави і права». Дніпропетровськ, 2015. 311 c.
2. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002. 496 с.
3. Батурин Ю. М. Проблемы компьютерного права. Москва: Юрид. лит., 1991. 268 с.
4. Бєлєнький В. П. Сучасна історія злочинів у сфері комп'ютерної безпеки. *Правова держава*. Вип. 1 (3), 2011. 111 c.
5. Гуцалюк М. I. Україна та Internet: перспективи розвитку . Електронна стаття «Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet». Центр информационной безопасности. URL: <http://www.bezpeka.com/ru/lib/spec/law/legal-protection-information-systemsInternet.html>.
6. Про ратифікацію Третього додаткового протоколу та Четвертого додаткового протоколу до Європейської конвенції про видачу правопорушників: Закон України від 07.06.2017 № 2090-VIII. URL: http://zakon5.rada.gov.ua/laws/show/2090-19. 185
7. Амелін О. Ю. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2016. Вип. № 3. С. 1–10.
8. Про Доктрину інформаційної безпеки України: Указ Президента України від 8.07.2009 № 514/2009. Офіційний вісник України. 2009. № 52. С. 7.
9. Розенфельд Н. А. Суб'єкт злочину «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж» . Центр исследования проблем компьютерной преступности. URL: <http://www.crime-research.org/library/Rozenf.htm>.
10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19. 184
11. Бельський Ю. А. Щодо визначення поняття кіберзлочину. *Юридичний вісник.* Вип. 6, 2014. С. 414 - 418.
12. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016. URL: <http://zakon2.rada.gov.ua/laws/show/96/2016>.
13. Копатін О. В., Скулишин Є. В. Словник термінів з кібербезпеки. Київ: ВБ «Аванпост-Прим», 2012. 214 с.
14. Болгов В. М., Гадіон Н. М., Гладун О. З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з 174 використанням інформаційних технологій: наук.-практ. посіб. Київ: Національна академія прокуратури України, 2015. 202 с.
15. Мазолина О. В. Вопросы международно-правового регулирования Интернета. *Московский журнал международного права.* 2004. Вып. 4. С. 152-164.
16. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. 2015. № 12. С. 93-98. URL: <http://nbuv.gov.ua/UJRN/Nivif_2015_12_15>.
17. Сухонос В. В. Кримінальне право України. Загальна частина: підр. Суми : Університетська книга, 2016. 375 с.
18. Анісімов Г. М., Володіна О. О., Зінченко І.О. Кваліфікація злочинів : навч. посіб.; за ред. М. І. Панова. Харків : Право, 2016. 356 с.
19. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. Москва: Юрид. лит., 1991. 160 с.
20. Игошев К. Е. Типология личности преступника и мотивация преступного поведения. Горький, 1974. 167 с.
21. Вехов В. Б. Компьютерные преступления: Способы совершения, методики расследования. Москва: Право и закон, 1996. 179 с.
22. Телійчук В. Г. Способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії. *Держава та регіони.* 2014 р. Вип. 2 (44). С. 31-37.
23. Голубєв В. О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту.* 1997. Вип. 2. С. 39 - 40.
24. Корнякова Т. В., Соколенко О. Л., Юзіков Г. С. Віктимологічне моделювання у системі заходів забезпечення кримінологічної безпеки суспільства : моногр. Дніпропетровськ : ЛІРА, 2016. 220 с.
25. Плугатир М. В. Особа, що має право доступу до комп'ютерної інформації як суб'єкт злочину, передбаченого ст. 362 КК України. *Юридична Україна.* Кримінально-правові науки. 2010. №1, С. 113-116.
26. Конвенція «Про кіберзлочинність» від 23.11.2001 № 994\_575. URL: <http://zakon2.rada.gov.ua/laws/show/994_575/>.
27. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества Москва: ООО Издательство «Юрлитинформ», 2002. 496 с.
28. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. Вип. 3. С. 129-136.
29. Ричка Д. О. Транснаціональна злочинність новітніх комп'ютерних технологій. *Науково˗виробничий журнал «Держава та регіони.* Серія : Право». Класичний приватний університет. Запоріжжя, 2018. С. 133-138.
30. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп’ютерних технологій. *Форум права.* 2009. Вип. 2. С. 434–441.
31. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.
32. Сорока Л. В. Види правопорушень у сфері комп'ютерних та інформаційних технологій. *Наукові записки КДПУ.* Серія: Історичні науки. Кіровоград : КДПУ ім. В. Винниченка, 2005. Вип. 9. С. 262-270.
33. Про міжнародне приватне право: Закон України від 23.06.2005 № 2709- IV. URL: https://zakon.rada.gov.ua/ laws/show/2709-15.
34. Про порядок направлення підрозділів Збройних Сил України до інших держав: Закон України від 02.03.2000 № 1518-III. URL: <https://zakon.rada.gov.ua/laws/show/1518-14>.
35. Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України: Закон України від 22.02.2000 № 1479-III. URL: <http://zakon5.rada.gov.ua/laws/show/1479-14>.
36. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів. *«Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності»* : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014. С. 192–194.
37. Куліш, А. М., Тютюнник В. В. Комп'ютерна злочинність: нормативноправове врегулювання. *«Сучасні інформаційні системи і технології»*: матеріали Першої міжнародної науково-практ. конфер., м. Суми, 15-18 травня 2012 р. Суми: СумДУ, 2012. С. 229-231.
38. Про інформацію: Закон України від 02.10.1992 № 2657-XII (у ред. 01.01.2017). URL: <http://zakon2.rada.gov.ua/laws/show/2657-12>.
39. Фігель М. В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. 336 с.
40. Снігерьов О. П., Сергач О. І. Деякі правові проблеми злочинності в сфері комп’ютерної інформації. *«Інформаційні технології та захист інформації»*. Збірник наукових праць. Міністерство внутрішніх справ України. Запорізький юридичний інститут. 1998. Вип. 1. С. 59-64. 187
41. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С.. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.
42. Кривогін М. С. Міжнародно-правові аспекти боротьби з кібернетичними злочинами. *«Держава і право : теорія і практика»*: матеріали II міжнар. науч. конф. (м. Чита, березень 2013 р.). Чита : «Молодий вчений», 2013. С. 77-79.
43. Кіберполіція (крок реформі) . *Українська правда.* URL: http://blogs.pravda.com.ua/authors/avakov/ 561a92c183c27/ view\_print/.
44. Шеломенцев В. П. Боротьба з організованими злочинними угрупуваннями у сфері використання банківських платіжних карток. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Київ: МНДЦ, 2004. Вип. 10. 185-194 с.
45. Школьний В. Б. Криміналістична характеристика основних видів кіберзлочинів. «*Спеціальна техніка у правоохоронній діяльності»*: Матеріали V міжнар. наук. - практ. конф., 25 листоп. 2011 р. м. Київ. Київ: Нац. акад. внутр. справ України, 2012. С. 199-201.
46. Кримінальний кодекс України: Закон України від 05.04.2001 No 2341-IІІ // Відомості Верховної Ради України (ВВР), 2001, No 25-26, - 131 с.
47. Голубев    В. О.    Питання    кримінально-правової відповідальності за злочини у сфері використання комп'ютерних технологій. *Вісник Запорізького юридичного інституту.* 2002. № 3. С168-169
48. Мухин  Г. Н.  Структура  и  содержание  методики расследования преступлений, связанных с посягательством на информационные ресурсы. *Управление защитой информации.* 1999. №3. с.407.
49. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI URL: http://zakon4.rada.gov.ua/laws/show (дата звернення: 01.12.2018).
50. Криминалистика : учеб. для вузов / И. Ф. Герасимов, Л. Я. Драпкин, Е. П. Ищенко и др. ; под ред. И. Ф. Герасимова, Л. Я. Драпкина. 2-е изд. Москва : Высш. шк., 2000. 672 с.
51. Вехов В. Б. Компьютерные преступления. Способы совершения, методики расследования. Москва: Право и закон, 1996. – c. 298
52. Лавров   В. П.   Учение   о   способе   преступления. Криминалистическая характеристика преступления. Курс лекций по криминалистике / за ред. А. Ф. Волынского. Москва: Юридический институт МВД России, 1999. С. 85.
53. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР (у ред. 19.04.2014). URL: <https://zakon2.rada.gov.ua/laws/show/80/94-вр/>.
54. Азаров Д. С. Злочини у сфері комп’ютерної інформації (кримінальноправове дослідження): монографія. Київ: Атіка, 2007. 304 с.
55. Кримінальний процес України : підручник /за ред. Ю. М. Грошевого, В. М. Хотенця. Харків : «Право», 2000. 496 с.
56. Голубев В. О. Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Підприємництво, господарство і право.* 2003. № 7. 132 c.
57. Про тактичні та психологічні  прийоми допиту докладніше див.: Белкин Р. С., Лившиц Е. М. Указ. соч. – 129 с.
58. Курс лекцій з криміналістики: навч. посібник / за ред. О. А. Кириченка. Миколаїв: Вид-во ЧДУ ім. Петра Могили, 2014. 348 с.
59. Кириченко О. А., Ланцедова Ю.О. Курс лекцій зі спецкурсу «Інноваційна процедура протидії правопорушенням»: навч. посіб. Вид. 2-ге. Миколаїв : МНУ імені В. О. Сухомлинського, 2016. 100 с.
60. Мотлях О. І. Тактичні основи проведення обшуку у злочинах, пов’язаних з інформаційними технологіями. *Вісник Академії праці і соціальних відносин Федерації профспілок України.* 2002. № 2. С. 157-159
61. Пашнєв Д. В. Властивості комп’ютерної інформації як предмету злочину. *Вісник Кримінологічної асоціації України : збірник наукових праць.* Вип. № 1. Xарків : ХНУВС, 2012.С. 115-125.
62. Особливості допиту підозрюваного / Белкин Р. С., Лившиц Е. М. та ін. Житомир, 2003. 174 с.
63. Мотлях О. І. Питання організації планування дій слідчого у злочинах вчинених у сфері комп’ютерних технологій. *Вісник Академії адвокатури України.* 2005. Вип. 2. 134 с.
64. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп’ютерна злочинність. Навчальний посібник. – Київ: Атіка, 2002. 240 с.
65. Селюк А. В. Розслідування комп’ютерних злочинів: наук. метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 c.
66. Компьютерные преступления: способы совершения и раскрытия за ред. Б. П. Смагоринского. Москва: Право и закон, 1996. 360 с.
67. Безруков Н. Н. Компьютерная вирусология: справ. руководство. Київ: УРЕ, 1991. 38 с.
68. Тищенко Є. Ф. Розслідування комп’ютерних злочинів: наук. метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 c.
69. Голубєв В.О. Розслідування комп’ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.