СХІДНОЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ РАУФА АБЛЯЗОВА

Кафедра права та інформаційної справи

КУРСОВА РОБОТА

з дисципліни «Кримінальне право»

на тему: «Основи розслідування злочинів в галузі комп'ютерних технологій»

Студент-виконавець:

Диць Віталій Олексійович,
група ЮР-21

Керівник курсової роботи:

Ландіна Анна Валентинівна

Курсова робота захищена з оцінкою

_____

Протокол захисту курсових робіт

№ ___ від _____ 20____ р.

Черкаси 2025

Зміст

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:

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.
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 удосконалення законодавства у цій галузі, а також шляхів, що дадуть можливості для ефективного впровадження цих норм на практиці.

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 незаконного 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, С. 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.

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. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ В ГАЛУЗІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

1.1. 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. 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.

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, с. 8].

Криміналістичні ознаки злочинності в галузі КТ відрізняється від загально розповсюджених злочинних посягань в криміналістиці.

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.

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. [18, с. 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.

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, с.54].

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 безлеки організації, що є шкодою для неї;

– страх ймовірності 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.

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.

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, с. 15].

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

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

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.

1.2. 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 кібератак.

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.

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].

У пункті 14 Доповіді Комітету II 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].

За характером, злочини у сфері КТ 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.

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].

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.

Відповідно до норм Конвенції, об'єктом злочинів в сфері КТ, є значне коло суспільних відносин, що регулюються нормами права.

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 ЗАДЛЯ 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.

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].

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.

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.

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].

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].

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.

РОЗДІЛ 2. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В ГАЛУЗІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

2.1. 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 причини 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, с. 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.

2.2. 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].

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.

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].

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 підготовки до допиту 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, с.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.

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 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.

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, с.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, с.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, с. 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.

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.

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, с.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, с. 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.

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.

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.

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.

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.

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.

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 найстрімкіше 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 більш 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. Белеський В. Н. Сучасна історія злочинів у сфері комп'ютерної безпеки. *Правова держава*. Вип. 1 (3), 2011. 111 с.

2. Гуцалюк М. І. 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.

3. 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

4. Амелін О. Ю. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2016. Вип. № 3. С. 1–10.

5. Про Доктрину інформаційної безпеки України: Указ Президента України від 8.07.2009 № 514/2009. Офіційний вісник України. 2009. № 52. С. 7.

6. 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.

7. 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

8. Бельський Ю. А. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. Вип. 6, 2014. С. 414 - 418.

9. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016. URL: http://zakon2.rada.gov.ua/laws/show/96/2016.

10. Копатін О. В., Скулишин С. В. Словник термінів з кібербезпеки. Київ: ВБ «Аванпост-Прим», 2012. 214 с.

11. 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.

12. 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.

13. Сухонос В. В. Кримінальне право України. Загальна частина: підр. Суми : Університетська книга, 2016. 375 с.

14. Анісімов Г. М., Володіна О. О., Зінченко І.О. Кваліфікація злочинів : навч. посіб.; за ред. М. І. Панова. Харків : Право, 2016. 356 с.

15. 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.

16. Голубєв В. О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту.* 1997. Вип. 2. С. 39 - 40.

17. Корнякова Т. В., Соколенко О. Л., Юзіков Г. С. Віктимологічне моделювання у системі заходів забезпечення кримінологічної безпеки суспільства : моногр. Дніпропетровськ : ЛІРА, 2016. 220 с.

18. 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.

19. Конвенція «Про кіберзлочинність» від 23.11.2001 № 994_575. URL: http://zakon2.rada.gov.ua/laws/show/994_575/.

20. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. Вип. 3. С. 129-136.

21. 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.

22. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права.* 2009. Вип. 2. С. 434–441.

23. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.

24. 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.

25. Про міжнародне приватне право: Закон України від 23.06.2005 № 2709- IV. URL: https://zakon.rada.gov.ua/ laws/show/2709-15.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. Фігель М. В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. 336 с.

32. 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

33. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С.. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.

34. 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.

35. Кіберполіція (крок реформі) . *Українська правда.* URL: http://blogs.pravda.com.ua/authors/avakov/ 561a92c183c27/ view_print/.

36. 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.

37. 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.

38. Кримінальний кодекс України: Закон України від 05.04.2001 No 2341-III // Відомості Верховної Ради України (ВВР), 2001, No 25-26, - 131 с.

39. Голубев В. О. Питання кримінально-правової відповідальності за злочини у сфері використання комп'ютерних технологій. *Вісник Запорізького юридичного інституту.* 2002. № 3. С168-169

40. 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).

41. 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/.

42. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінальноправове дослідження): монографія. Київ: Атіка, 2007. 304 с.

43. Кримінальний процес України : підручник /за ред. Ю. М. Грошевого, В. М. Хотенця. Харків : «Право», 2000. 496 с.

44. Голубев В. О. Деякі особливості тактики окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Підприємництво, господарство і право.* 2003. № 7. 132 с.

45. Про тактичні та психологічні прийоми допиту докладніше див.: Белкин Р. С., Лившиц Е. М. Указ. соч. – 129 с.

46. Курс лекцій з криміналістики: навч. посібник / за ред. О. А. Кириченка. Миколаїв: Вид-во ЧДУ ім. Петра Могили, 2014. 348 с.

47. 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.

48. 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

49. Пашнєв Д. В. Властивості комп'ютерної інформації як предмету злочину. *Вісник Кримінологічної асоціації України : збірник наукових праць.* Вип. № 1. Харків : ХНУВС, 2012.С. 115-125.

50. Особливості допиту підозрюваного / Белкин Р. С., Лившиц Е. М. та ін. Житомир, 2003. 174 с.

51. 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.

52. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп'ютерна злочинність. Навчальний посібник. – Київ: Атіка, 2002. 240 с.

53. Селюк А. В. Розслідування комп'ютерних злочинів: наук. метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 с.

54. Безруков Н. Н. Компьютерная вирусология: справ. руководство. Київ: УРЕ, 1991. 38 с.

55. Тищенко Є. Ф. Розслідування комп'ютерних злочинів: наук. метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 с.

56. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.