МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

О. В. КОВАЛЬОВА

ПРОТИДІЯ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

НАУКОВО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Київ
Дакор
2022

УДК 004 : 34
К

Рекомендовано до друку
Вченою радою Донецького державного університету внутрішніх справ
(протокол № 2 від 29.09.2021 року)

Рецензенти:
Свір П. В. – кандидат юридичних наук, начальник управління карного розшуку Головного управління Національної поліції в Донецькій області, полковник поліції;
Ковальчук С. А. – заступник завідувача лабораторії комп'ютерно-технічних та телекомунікаційних досліджень Державного науково-дослідного експертно-криміналістичного центру МВС України.

Ковальова О. В.

К Протидія злочинам, пов'язаним із несанкціонованим втручанням у державні реєстри : науково-практичні рекомендації / О. В. Ковальова. Київ: ВД Дакор, 2022. 164 с.

ISBN 978-617-8066-__-_

У науково-практичних рекомендаціях розглянуті тактичні особливості протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пов'язаних із втручанням у державні реєстри.

Визначені основні терміни, розкрито поняття кіберпростору, кіберзлочинності, надано рекомендації щодо класифікації кіберзлочинів, розглянуто правову основу протидії кіберзлочинам, надано рекомендації з виявлення кіберзлочинів та встановлення джерел інформації про них.

Надані практичні рекомендації щодо початку досудового розслідування, особливості процесуального керівництва в кримінальних провадженнях у сфері інформаційних (комп'ютерних) відносин, розглянуто особливості проведення окремих слідчих (розшукових) дій, зокрема, огляду місця події, обшуку, залучення експерта, допиту свідка, потерпілого, підозрюваного, проведення негласних слідчих (розшукових) дій, надані практичні рекомендації щодо фіксації, вилучення та збереження «слідової картини» кіберзлочинів, пов'язаних із несанкціонованим втручанням у державні реєстри.

УДК 347(075.8)(477)

ISBN 978-617-8066-__-_

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

АБД – автоматизований банк даних;
АІПС – автоматизовані інформаційно-пошукові системи;
АІС – автоматизована інформаційна система;
БД – база даних;
ДПС – довідкова правова система;
ДКП – Департамент кіберполіції;
НП України – Національна поліція України;
ЕД – електронний документ;
ЕОМ – електронна обчислювальна машина;
ЕЦП – електронний цифровий підпис;
ІПС – інформаційно-пошукова система;
ІС – інформаційна система;
КК України – Кримінальний кодекс України;
КПК України – Кримінальний процесуальний кодекс України;
ООС – Операція об'єднаних сил;
ОС – операційна система;
ПК – персональний комп'ютер;
СУБД – система управління базами даних;
СОГ – слідчо-оперативна група.

ВСТУП

Актуальність дослідження. Нині людство переживає бурхливу інформаційну революцію, пов'язану з формуванням, розвитком і поширенням транскордонних глобальних інформаційно-телекомунікаційних мереж, що покривають усі країни й континенти, проникають до кожного будинку і які одночасно впливають на кожну людину окремо й на величезні маси людей. У суспільстві відбуваються інтенсивні процеси інформатизації та інтелектуалізації: якщо на початку XXI століття мало хто користувався мобільним зв'язком, а інтернет тільки ставав популярним, то сьогодні все більш відчутним стає розвиток інтерактивного телебачення, зростання швидкості обробки інформації, створення різноманітних баз даних, проникнення в усі сфери діяльності мережевих та хмарних систем, смартфонів, планшетів, роботів зі штучним інтелектом. Із появою мережі, зокрема інтернет-середовища, поширення інформації розуміння місця, ролі, значення людини в комунікативному просторі зазнало відповідних змін.

На сьогодні технологічні системи використовуються в науці, політиці, економіці, соціальній структурі, значно зростає швидкість обробки інформації, створення різноманітних баз даних, мережевих та хмарних систем, що призводить до формування глобального кіберпростору. Утілення в життя комп'ютерних технологій з величезними можливостями є головною умовою для комп'ютеризації господарської та управлінської діяльності, а також інших сфер життя суспільства, у яких порушення нормальної роботи такої техніки може спричинити величезні економічні збитки.

Комп'ютерні технології сприяють учиненню низки загальнокримінальних злочинів, а також зумовлюють виникнення нових видів кримінальних правопорушень, що передбачені розділом XVI КК України, а саме: ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх

розповсюдження або збут», ст. 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», ст. 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», ст. 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» та ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

Слід зауважити, що зазначений вище розділ КК України не охоплює всіх кримінально караних діянь у цій сфері. Через відсутність у чинному законодавстві базового поняття «кіберзлочини» класифікувати на законодавчому рівні вказані злочини на сьогодні неможливо. Такі кримінальні правопорушення можуть бути вчинені різними способами (викрадення комп'ютерної інформації, DoS-атаки, дефейс, розповсюдження шкідливих програм (вірусів), кардинг, фішинг, стирання програм або даних, розсилки листів (спамів), створення несправжніх інтернет-аукціонів та ін.) і часто кваліфікуються як загальнокримінальні злочини.

Мета дослідження полягає у визначенні особливості протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пов'язаних із втручанням у державні реєстри.

Для досягнення зазначеної мети слід виконати такі **завдання:**

1) висвітлити сутність поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;
2) проаналізувати види кіберзлочинності за міжнародним та національним законодавством;

3) розглянути криміналістичний аспект злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Об'єкт дослідження – суспільні відносини, що виникають під час здійснення інформаційних процесів з приводу виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, розповсюдження і споживання комп'ютерної інформації, а так само в інших сферах, де використовуються комп'ютери, комп'ютерні системи й мережі.

Предмет дослідження – тактичні особливості протидії злочинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пов'язаних із втручанням у державні реєстри.

Аналіз останніх досліджень і публікацій. Під час підготовки науково-практичних рекомендацій було використано норми чинного вітчизняного та міжнародного законодавства, що регламентують процес здійснення досудового розслідування, оперативно-розшукову діяльність, матеріали слідчої практики, а також наукові праці, присвячені проблемам формування сучасного кіберпростору, тлумачення понять «кіберпростір», «кіберзлочин», боротьби із кіберзлочинами, таких учених, як О. Ю. Буров, М. О. Будаков, В. М. Бутузов, М. М. Галамба, Р. А. Калюжний, В. В. Камишин, М. О. Кравцова, О. М. Литвинов, Ю. Є. Максименко, Ю. Ю. Нізовцев, О. В. Орлова, Н. І. Поліхун, О. Р. Росинська, В.Б. Толубко, Т. Л. Тропіна, В. О. Хорошко, В. С. Цимбалюк, О. М. Черкун, О. К. Юдін та ін. Окремі питання щодо кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку й напрямів протидії їм розглядалися Д. С. Азаровим, В. І. Алескеровим, П. Д. Біленчуком, В. Б. Веховим, В. А. Глушковим, Н. А. Гуторовою, Н. В. Карчевським, В. А. Мазуровим, П. І. Орловим, С. А. Орловим, Н. І. Хавронюком, М. А. Єфремовою та ін. Дослідженням проблемних питань боротьби та припинення злочинів, пов'язаних із несанкціонованим втручанням в автоматизовані системи, займалися такі науковці: П. Д. Біленчук, І. В. Діордіца, І. В. Європіна, О. В. Манжай, А. І. Марущак, Д. О. Ричка, А. А. Русецький, О. А. Самойленко, Г. В. Форос, А. Г. Чубенко та інші.

Методи дослідження. Для дослідження організаційно-технічних засад, положень і принципів упровадження сучасних засобів комунікації як основних використано діалектичний метод, що дозволило розглянути предмет науково-практичних рекомендацій у сукупності та взаємозв'язку його складників. Крім того, поставлені для досягнення мети завдання було вирішено за допомогою комплексу загальнонаукових і спеціальних методів, у тому числі формально-логічних (аналіз, синтез, дедукція, індукція, аналогія, абстрагування), системно-структурного та порівняльно-правового методів.

ВИЗНАЧЕННЯ ОСНОВНИХ ТЕРМІНІВ

Автоматизований банк даних (АБД) – це система інформаційних, програмних, мовних, організаційних і технічних засобів, які необхідні для інтегрованого нагромадження, зберігання, ведення, актуалізації, пошуку й видачі даних.

Автоматизована інформаційно-пошукова система (АІПС) – це організаційно-технічна система, яка має систему сукупних методів і засобів, призначених для зберігання, пошуку та накопичення інформації, відомостей.

Автоматизована система (АС) – це організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються різні бази даних, накопичується та обробляється інформація, яка є результатом наукових спостережень чи експериментів, збирається, систематизується та оновлюється в електронному вигляді статистична інформація.

Блокування інформації – це дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Блокування комп'ютерної інформації – це дії, внаслідок яких унеможливлюється доступ до інформації.

Витік інформації – це ситуація, коли внаслідок певних дій інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Втрата інформації – ситуація, коли інформація, яка раніше існувала в АС, перестає існувати для фізичних або юридичних осіб, які мають право власності на неї, в повному чи частковому обсязі.

Збут шкідливих програмних чи технічних засобів полягає в оплатній (як правило) чи безоплатній (наприклад, подарунок) передачі вказаних засобів будь-якій іншій особі.

Зміна комп'ютерної інформації – заміна або вилучення будь-якої складової частини відповідної інформації чи внесення до цієї інформації певних додаткових, раніше відсутніх у ній складових частин.

Зміна, знищення, блокування, перехоплення, копіювання інформації є несанкціонованими, якщо вони здійснені без дозволу (згоди) власника інформації або уповноваженої ним особи.

Знищення комп'ютерної інформації – дії, наслідком яких є зникнення інформації в ЕОМ, АС, комп'ютерній мережі чи на носії. Це не лише ліквідація файлу, каталогу тощо, у вигляді яких існувала інформація, а й приведення певної інформації у такий стан, що унеможливлює її використання, оскільки в цьому випадку результатом також є зникнення початкової інформації.

Кіберзлочинність – сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кіберпростір – інформаційний простір, що моделюється за допомогою комп'ютера, у якому існують визначені об'єкти або символьне уявлення інформації, взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує мережа Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача.

Комп'ютерна інформація – це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватися, змінюватися чи використовуватися за допомогою ЕОМ, а також передаватися іншими каналами зв'язку (за допомогою факсу, телетайпу, телексу).

Комп'ютерна інформація з обмеженим доступом, згідно зі ст. 30 Закону України «Про інформацію», за своїм правовим режимом поділяється на конфіденційну і таємну.

Комп'ютерна мережа – це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів іншої (інших) ЕОМ та до інформації, що зберігається в системі іншої (інших) ЕОМ.

Комп'ютерна програма – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, які виражені у вихідному або об'єктному кодах).

Конфіденційна інформація містить відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються лише за їх бажанням та згодою відповідно до встановлених умов, і мають відповідний правовий статус. Режим доступу до конфіденційної інформації громадян та юридичних осіб визначають самостійно та встановлюють для неї систему способів захисту компетентні державні органи або власники інформації.

Копіювання комп'ютерної інформації – виготовлення із застосуванням можливостей комп'ютера електронної копії певної комп'ютерної інформації.

Мережі електрозв'язку – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж – це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини.

Несанкціонованим втручанням у роботу мереж електрозв'язку є будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж, що забезпечують роботу мереж електрозв'язку) вчинені без

згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких припиняється (зупиняється) робота мережі електрозв'язку або відбуваються зміни режиму цієї роботи.

Несанкціонований збут інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, – це несанкціоноване розповсюдження такої інформації без згоди її власника на платній основі – шляхом купівлі-продажу, міни та ін.

Несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, – це вчинення будь-яких дій, якими без згоди власника інформації така інформація безпосередньо чи опосередковано надається іншим особам чи доводиться до їх відома, вводиться в обіг шляхом будь-якої, крім оплатної, форми.

Оброблювання інформації – це виконання певних дій за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, які включають різні види маніпуляцій з такою інформацією згідно з відповідними комп'ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ тощо.

Перехоплення комп'ютерної інформації – дії, внаслідок яких комп'ютерна інформація, що передається певному адресату каналами зв'язку, потрапляє в розпорядження іншої особи.

Порушенням роботи ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку є зміна встановлених власником чи уповноваженими ним особами параметрів процесу обробки інформації у зазначених машинах, системах чи мережах, зокрема прискорення, уповільнення цього процесу, припинення обробки частини інформації, перекручення результатів обробки інформації тощо.

Порушення порядку чи правил захисту інформації, яка обробляється ЕОМ (комп'ютерами), АС, комп'ютерними мережами чи мережами електрозв'язку – це невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації, що обробляється у вказаних

електронних системах особами, які мають здійснювати відповідні заходи із забезпечення захисту інформації.

Припиненням роботи ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку є ситуація, коли обробка інформації у вказаних чи зазначених машинах, системах чи мережах повністю припиняється.

Простір – множина об'єктів, між якими встановлені відношення, подібні за своєю структурою зі звичайними просторовими відношеннями типу околу, відстані та ін. Загальні властивості простору: протяжність, єдність дискретності та неперервності.

Програмні засоби (комп'ютерні програми) – це певний набір інструкцій у вигляді слів, цифр, кодів, схем, символів, виражених у формі, придатній для зчитування комп'ютером, який приводить цю програму в дію для досягнення певної мети.

Програма-вірус – це спеціально створена програма, яка здатна сама приєднуватися до інших програм (тобто пристосовуватися і «заражати» їх) і під час запуску спричиняти різні негативні наслідки: псування файлів і каталогів, перекручування інформації, у тому числі результатів обчислення, засмічення чи спотворення пам'яті ЕОМ, створювати інші перешкоди в роботі ЕОМ чи АС.

Розповсюдження шкідливих програмних чи технічних засобів – це оплатна чи безоплатна передача в будь-який спосіб зазначених засобів відносно широкому і невизначеному колу осіб (фізичних чи юридичних), навіть через мережу Інтернет.

Сервери є найбільш типовими різновидами ЕОМ. Це потужні комп'ютери, призначені для обробки великої кількості інформації, одночасного функціонування багатьох програм, забезпечення роботи АС, мереж тощо.

Спотворення процесу обробки інформації – зміна методики чи процесу обробки інформації комп'ютером або АС, унаслідок якої обробка інформації не дає результатів узагалі, дає неправильні результати або ж дає лише частину тих результатів, які можна було отримати до цієї зміни.

Створення програмних чи технічних засобів – це виготовлення програмних чи технічних засобів, внаслідок чого виникають нові шкідливі предмети (яких раніше не існувало), здатні до

несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. До створення таких предметів слід віднести і модифікацію (перероблення) програмних чи технічних засобів, які звичайно використовуються в роботі ЕОМ, АС, у комп'ютерних мережах чи мережах електрозв'язку, а внаслідок перероблення набувають якості шкідливих і здатних до несанкціонованого втручання в ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку.

Таємна інформація – інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству або державі.

Технічні засоби – це певне обладнання, устаткування, єдиною або основною функцією якого є забезпечення несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Шкідливі технічні засоби – це різні прилади, обладнання, устаткування тощо, за допомогою яких здійснюється несанкціонований доступ до ЕОМ чи АС.

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО СУТНОСТІ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

1.1. СУТНІСТЬ ПОНЯТТЯ «*КІБЕРПРОСТІР*». ОСОБЛИВОСТІ КІБЕРПРОСТОРУ

Високий рівень розвитку інформаційних технологій, технічних засобів та систем, їх активне впровадження в усі сфери нашого життя призвели до формування інформаційного та кібернетичного просторів, які мають на сьогодні практично необмежений потенціал і відіграють провідну роль у кожній країні [1, с. 123].

Уперше термін «кіберпростір» було введено у вжиток письменником Вільямом Гібсоном у 1982 р. в новелі «Палаючий хром» («Burning Chrome»). У 1984 році це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). На думку Гібсона, кіберпростір («cyberspace») – це злагоджена галюцинація, яку щодня зазнають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів усього розумного людства; потоки даних, що протікають у просторі розуму; скупчення та сузір'я інформації [2, с. 118; 3].

В іноземних та міжнародних документах поняття «кіберпростір» почало використовуватися або застосовуватися з кінця XX ст. У цьому контексті можна згадати визначення кіберпростору, надане Верховним судом США: унікальний носій, відомий його користувачам як кіберпростір, що не знаходиться на певній території, але доступний кожному в будь-якій точці світу через мережу Інтернет [2, с. 118; 4]. У рекомендації «Про розвиток та використання багатомовності та загальному доступі до кіберпростору», прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., кіберпростір визначається як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [5].

Словосполучення «кіберпростір» утворено із двох слів: «кібер» тобто «кібернетичний» та «простір». У цьому словосполученні основним є слово «простір», а спрямованість, характер цього простору визначає слово «кібернетичний».

Енциклопедичне визначення поняття «простір» має два значення:

1) *простір* (математ.) – множина об'єктів, між якими встановлені відношення, подібні за своєю структурою зі звичайними просторовими відношеннями типу околу, відстані та ін.;
2) *простір* – форма співіснування матеріальних об'єктів, процесів (характеризує структурність і протяжність матеріальних систем). Загальні властивості простору: протяжність, єдність дискретності та неперервності [6, с. 251].

Для розуміння спрямованості простору, який розглядається, слід звернути увагу на значення поняття «*кібернетика*» – наука про управління, зв'язки і переробку інформації. Основний об'єкт дослідження – так звані кібернетичні системи, що розглядаються абстрактно, незалежно від їх матеріальної природи. Приклади кібернетичних систем – автоматичні регулятори в техніці, ЕОМ, людський мозок, біологічні популяції, людське суспільство. Кожна така система є множиною взаємопов'язаних об'єктів (елементів системи), здатних сприймати, запам'ятовувати та переробляти інформацію, а також обмінюватися нею [7].

Кіберпростір включає в себе як матеріальну складову, наприклад засоби обчислювальної техніки, засоби зв'язку, матеріальні складові телекомунікаційних мереж, написання алгоритмів і кодів та ін., так і нематеріальну: інформацію, процеси зчитування кодів, процеси передачі інформації та ін. На нашу думку, у цьому разі «матеріальність» слід розуміти, на відміну від філософського тлумачення, як усе те, що можна побачити, відчути або до чого можна доторкнутися.

Кіберпростір у цілому неможливо побачити, відчути, почути або до нього доторкнутися. Він, а особливо процеси, які в ньому відбуваються, людиною сприймаються як щось абстрактне. Але окремі складові цього простору можна не тільки побачити, а й доторкнутися до них.

О. Манжай вважає, що «кіберпростір – це інформаційне середовище, яке виникає за допомогою технічних систем під час взаємодії людей між

собою, взаємодії технічних систем та управлінні людьми цими технічними системами». А. Погорецький та В. Шеломенцев кіберпростір тлумачать як «штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо)» [8, с. 145].

Зважаючи на наведене, термін *«кіберпростір»* слід розуміти як *інформаційний простір, що моделюється за допомогою комп'ютера, у якому існують визначені об'єкти або символьне уявлення інформації, взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує мережа Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача* [9, с. 277].

У Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. законодавець визначає *кіберпростір як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних»* [10].

На основі аналізу використання кіберпростору маємо змогу визначити певні особливості кіберпростору:

1) віддаленість (дистанційність) доступу;
2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі;
3) віртуальність, що забезпечує відносну конфіденційність інформації та можливість впливати на свідомість певної категорії осіб;

4) комунікативність;
5) недосконалість забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі [11].

Хоча термін «кіберпростір» часто вжито в міжнародно-правових актах, національних джерелах права, а також у працях зарубіжних та вітчизняних науковців, його застосування є достатньо умовним та суперечливим, він не має чітких загальноприйнятих рамок, здебільшого пов'язується чи ототожнюється з поняттями «інформаційний простір», «віртуальний простір», «комп'ютерна сфера», «інтернет», «інформаційно-комунікаційні системи і мережі». Відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади та активне залучення громадян до управління державою і вирішення питань місцевого значення, забезпечує публічність і прозорість дій влади, сприяє запобіганню корупції.

1.2. ПОНЯТТЯ КІБЕРЗЛОЧИННОСТІ

Переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці, а саме появу кіберзлочинності.

Термін «кіберзлочинність» вжито в американській доктрині на початку 60-х рр., коли було виявлено перші випадки злочинів, здійснених із використанням комп'ютерів. Саме тоді з'явилися перші «хакери», ними були студенти Массачусетського технологічного інституту, які маніпулювали з програмами нового університетського комп'ютера [12, с. 294]. Електронно- обчислювальні машини (ЕОМ) набули широкого застосування як серед працівників правоохоронних органів, так і серед учених, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [13, с. 39].

Термін «кіберзлочинність» у національних офіційних нормативно-правових документах не визначено, незважаючи на його застосування в окремих нормативно-правових актах, що регулюють суспільні відносини в кіберпросторі. Проте саме поняття стало закріпилося в лексиконі правоохоронних органів розвинених держав Європи і світу [14]. Цей

термін зазвичай уживають у такому значенні: сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

У Конвенції про кіберзлочинність немає визначення поняття «кіберзлочинність» [15]. Водночас у її преамбулі вказано, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом установлення кримінальної відповідальності за таку поведінку як це описано в Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, а також укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [16].

Кіберзлочинність – явище новітньої, цифрової доби, тому слід зазначити, що за своєю суттю мережа Інтернет є достатньо сприятливою для вчинення комп'ютерних злочинів. Такі її властивості, як глобальність, транскордонність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі та їх взаємозамінність створюють кіберзлочинцям, які використовують мережа Інтернет, переваги на всіх етапах вчинення злочину, а також дозволяють ефективно переховуватися від правоохоронних органів [17, с. 75].

Термін «кіберзлочинність» нині або на сьогодні часто вживається разом із терміном «комп'ютерна злочинність», до того ж нерідко ці поняття використовуються як синоніми.

1. Злочини, пов'язані із застосуванням комп'ютерів, *«комп'ютерні злочини»* розуміють як ті правопорушення, що жодним чином не стосуються мережі, а лише окремо розташованих комп'ютерних систем, тобто злочини проти комп'ютерів або комп'ютерних даних [14], під час яких комп'ютер є предметом, знаряддям або засобом скоєння злочину.

2. Поняття «кіберзлочинність» використовується для опису

широкого кола правопорушень, *«кіберзлочинів»*, які пов'язані як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж [14], включаючи традиційні комп'ютерні злочини.

На думку експертів ООН, комп'ютерна злочинність тотожна «кіберзлочинності», і її можна визначити так: «…охоплює будь-який злочин, який можна вчинити за допомогою комп'ютерної системи або мережі, в межах комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі» [18, с. 424]. Тому можна зробити висновок, що це поняття охоплює будь-який злочин, який може бути вчинений в електронному середовищі.

Варто звернути увагу, що в науковій юридичній літературі наведені такі ознаки кіберзлочинів, що відрізняють їх від «звичайних» злочинних посягань і значно підвищують їх суспільну небезпечність:

1) кіберзлочин не вимагає фізичного зближення жертви та суб'єкта злочину в момент учинення такого;
2) кіберзлочин є «автоматизованим» злочином (суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч);
3) суб'єкт кіберзлочину не підвладний обмеженням, які існують у реальному, фізичному світі. Так, кіберзлочини можуть бути вчинені моментально, а тому потребують швидкої реакції на них [17, с. 75].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [10].

Отже, кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створювати особисту

небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці.

Таким чином, кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [19, с. 332].

Крім того, кіберзлочинність визначають як соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [20, с. 12].

На останньому форумі Конгресу ООН з проблем протидії кіберзлочинам (2015 р.) до категорії «кіберзлочинність» віднесено такі діяння, об'єктом злочину яких є комп'ютерні дані або системи, а також діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину.

До першої класифікаційної групи належить отримання незаконного доступу до комп'ютерних даних або систем (іноді їх називають «основними» кіберзлочинами). До другої – використання комп'ютерних даних або систем для шахрайства, розкрадання чи спричинення шкоди іншим особам; злочини, пов'язані з використанням комп'ютерів та інтернет-контенту, включаючи пропаганду ненависті, дитячу порнографію, злочини з використанням особистих даних і продаж заборонених товарів.

Сутність кіберзлочинів полягає в тому, що це протиправні суспільно небезпечні діяння, тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує мережа Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача [19].

Отже, узагальнюючи наявні доктринальні та законодавчі дефініції, «кіберзлочин» пропонуємо розуміти як:

1) незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей [21, с. 33];
2) протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер, створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад, комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо) [22, с. 85];
3) злочини, які вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [23];
4) злочини у сфері комп'ютерної інформації [10, с. 89], тобто під час використання текстової, графічної чи будь-якої іншої інформації (даних), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватися, змінюватися чи використовуватися за допомогою ЕОМ [12];
5) передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає у протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [24];
6) злочини, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [25, с. 267].

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття кіберзлочину, можна зробити висновок, що серед сучасних українських науковців немає єдиного підходу до визначення терміна «кіберзлочин». До того ж підходи досить суттєво відрізняються, що може бути причиною хибного трактування, а це, у свою чергу, може призвести до неправильної кваліфікації злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівні.

1.3. КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ

Кіберзлочини поділяють на види залежно від об'єкта, від предмета посягання, від способів скоєння і т. д. [15].

Найбільш поширена класифікація кіберзлочинів на сьогодні ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація нині є «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика використовують саме цей поділ.

Конвенція передбачає чотири групи злочинів, пов'язаних із використанням комп'ютерних технологій як інструменту їх учинення [10].

До першої групи віднесено злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм).

До другої групи – злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство).

До третьої групи належать злочини, пов'язані зі змістом даних, зокрема правопорушення, пов'язані з дитячою порнографією, – вироблення, пропонування або надання, розповсюдження або передача, здобуття, володіння (ст. 9 Конвенції).

Четверту групу становлять правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10 Конвенції) [26].

Держави, що приєдналися до Конвенції, взяли зобов'язання переглянути своє законодавство з метою його узгодження з рекомендаціями, викладеними в цьому міжнародному документі.

Так, у Великій Британії було прийнято спеціальний закон – Акт про комп'ютерні зловживання (Computer Misuse Act), який одним з перших встановив кримінальну відповідальність за використання комп'ютерної інформації з метою вчинення злочину [27]. Комп'ютерне або інформаційне шахрайство винесено в окремий склад злочину в кримінальних кодексах Естонії (ст. 213), Італії (ст. 640), Республіки Молдова (ст. 260-6), ФРН (§ 263 а) та інших країн світу [28, с. 150]. У Кримінальному кодексі Грузії є розділ XXXV «Кіберзлочини», який передбачає кримінальну відповідальність за ст. 284 «Самовільне проникнення в комп'ютерну

систему»; ст. 285 «Незаконне використання комп'ютерних даних або (і) комп'ютерних систем»; ст. 286 «Посягання на комп'ютерні дані або (і) комп'ютерну систему» [29].

Терміни, які вживаються в Конвенції та додатковому протоколі до неї, відображено й у вітчизняному законодавстві. Однак у Кримінальному кодексі України, що містить вичерпний перелік правопорушень, за які передбачена відповідальність, немає спеціальних норм, які визначають відповідальність за злочином із префіксом «кібер-»: «кіберзлочин», «кібератака», «кібербезпека», «кіберпростір», «кіберзагроза», «кібернетичний захист», «кібертероризм», «кібершпигунство».

Так, розділ XVI Особливої частини КК України містить низку статей, що передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку:

- ст. 361 «Несанкціоноване втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;
- ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
- ст. 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»;
- ст. 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»;
- ст. 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;
- ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку)» [30].

Водночас перелік кіберзлочинів не вичерпується діяннями, визначеними в розділі XVI Особливої частини КК України. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах.

Кіберзлочини мають низку особливостей, завдяки яким вони посягають через комп'ютерні системи на сфери міжнародного правопорядку і, зокрема, на міжнародний обмін інформацією.

Підсумовуючи, можна стверджувати, що законодавство України про кримінальну відповідальність не містить у повному обсязі понять, які розкривають зміст або сутність кіберзлочинності.

1.4. ПРАВОВА ОСНОВА ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Розвиток правових засад організації кібербезпеки в Україні, а саме захист відносин, що виникають під час одержання, використання, поширення та зберігання інформації, регулюються положеннями Конституції України, законами України: «Про інформацію», який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [31]; «Про доступ до публічної інформації», що визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [32]; «Про Національну програму інформатизації», який визначає загальні засади формування, виконання та коригування Національної програми інформатизації [33]; «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [34]; «Про телекомунікації», який визначає повноваження держави щодо управління та регулювання зазначеної

діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у такій діяльності або користуються телекомунікаційними послугами [35]; «Про електронні документи та електронний документообіг», що встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів [36]; «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом й обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних [37]; «Про електронні довірчі послуги», що визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації [38].

Найбільшим «проривом» вітчизняного законодавства у сфері забезпечення кібербезпеки стала ратифікація в 2005 році Конвенції про кіберзлочинність, прийнятої Радою Європи. Відповідно до Преамбули, метою створення документа стала необхідність зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, та укладення домовленостей щодо швидкого й надійного міжнародного співробітництва [10].

У січні 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України з урахуванням викликів, які стоять перед нашою державою: агресивних дій Російської Федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом [39, с. 166].

Стурбованість міжнародного співтовариства щодо розвитку кіберзлочинності відображено, зокрема, у таких міждержавних угодах, як Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.), Всесвітній саміт з питань інформаційного суспільства та Конвенції Ради Європи «Про кіберзлочинність» (2001 р.).

У цих документах йдеться про спільне протистояння кіберзлодіям шляхом прийняття відповідних законодавчих актів, що не будуть суперечити ні законам окремої держави, ні пунктам договорів, які ратифікувала ця держава.

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж декілька років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерній злочинності.

Прикладом цьому може бути Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», який мав на меті розвиток національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу громадян до цієї мережі, ефективного використання її можливостей для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності, зміцнення міжнародних зв'язків, належного інформаційного забезпечення здійснення органами державної влади та органами місцевого самоврядування своїх повноважень, повнішого задоволення потреб міжнародного співтовариства в об'єктивній, комплексній інформації щодо різних сфер суспільного життя в Україні, а також вирішення інших завдань [40].

Уперше стан і проблеми імплементації Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації докладно дослідив М. В. Плугатир. Відстоюючи необхідність узгодження норм кримінального законодавства України з

положеннями Конвенції про кіберзлочинність, автор обмежує своє дослідження пропозиціями щодо імплементації статей 2–6 Конвенції, що стосуються правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних та систем і мають охоплюватися розділом XVI Особливої частини КК України. Водночас дослідник не вивчає стан реалізації в Україні вимог Конвенції щодо правопорушень, пов'язаних із використанням комп'ютерних засобів (статті 7, 8), зі змістом даних (контентом) (ст. 9), а також із порушеннями авторського права та суміжних прав (ст. 10). У березні 2016 року Указом Президента України від 15 березня 2016 року № 96/2016 було затверджено рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [41].

Отже, у нормативно-правовій базі України з'явився уніфікований нормативно-правовий акт, у якому передбачено створення «активного кіберзахисту» та забезпечення належних умов для безпечного використання кіберпростору в інтересах держави й суспільства. Проте у Стратегії застосовано поняття та терміни, офіційне тлумачення яких ще не визначено національним законодавством України. Деякі з них вжито відповідно до ратифікованої Україною Конвенції Ради Європи про кіберзлочинність 2001 р. Наразі законодавець пропонує надати офіційне тлумачення деяким термінам у Законі України «Про основні засади забезпечення кібербезпеки України» [10]. Так, необхідно зазначити, що певною мірою Закон не відповідає умовам сьогодення і прийнятий так би мовити на «перспективу», оскільки існують питання, що потребують роз'яснення.

1.5. ВИЯВЛЕННЯ КІБЕРЗЛОЧИНІВ ЯК НАПРЯМ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ. ДЖЕРЕЛА ІНФОРМАЦІЇ ПРО КІБЕРЗЛОЧИН

Відповідно до п. 2 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», Національна поліція України вживає заходів для запобігання кіберзлочинам, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [10]. У п. 3 ч. 1 ст. 2 Закону України «Про

Національну поліцію» одним з завдань Національної поліції є протидія злочинності, що передбачає виконання комплексу дій з виявлення, попередження та розкриття злочинів [42].

Сьогодні можна скласти перелік суб'єктів, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів.

1. Національна поліція України (НПУ), відповідно до § 3 Стратегії кібербезпеки України, належить до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі та здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Як суб'єктів виявлення кіберзлочинів можна структурні підрозділи НПУ можна поділити на дві групи.

1.1. Підрозділи Департаменту кіберполіції (ДКП), які згідно з п. 2.1 Положення про ДКП НПУ, уповноважені щодо протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця сфера діяльності названа в Положенні як «протидія кіберзлочинності». В Україні правові основи боротьби з кіберзлочинами визначаються передусім Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП прямо зобов'язані здійснювати оперативно-розшукову діяльність властивими їм методами з метою протидії конвенційним злочинам (відповідальність за які фактично передбачена статтями 163, 176, 185, 190, 200, 301, 361–363-1 КК України).

ДКП є міжрегіональним територіальним органом, юридичною особою публічного права. До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (управління протидії кіберзлочинам у м. Київ, Львівській, Одеській, Харківській та Дніпропетровській областях; відділи протидії кіберзлочинам в інших областях).

1.2. Інші оперативні підрозділи НПУ (Департамент карного розшуку, Департамент протидії наркозлочинності тощо), що здійснюють протидію іншим, альтернативним Конвенції, злочинам, що вчиняються

у кіберпросторі та підслідні слідчим НПУ. ДКП стосовно таких злочинів може тільки сприяти в порядку, передбаченому чинним законодавством, іншим підрозділам НПУ у попередженні, виявленні та припиненні кримінальних правопорушень – забезпечує своєчасне отримання інформації про злочини, що вчинені в кіберпросторі, або про відповідні злочинні наміри.

2. Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України (ДКІБ СБУ). До завдань СБУ також належить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління та економіки й інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Типовими джерелами оперативної інформації про кіберзлочини є:

1) електронні та письмові повідомлення про злочин;
2) запити й повідомлення правоохоронних органів інших держав, міжнародних правоохоронних організацій (у результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст. 6 Закону України «Про оперативно-розшукову діяльність»);
3) матеріали, складені в результаті перевірки заяв і повідомлень громадян, з якими встановлено негласне співробітництво (у результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст. 6 Закону України «Про оперативно-розшукову діяльність»);
4) письмові доручення, постанови слідчого;
5) матеріали інших правоохоронних органів;
6) інші відомості, отримані внаслідок оперативно-розшукової діяльності (у результаті оперативного пошуку) [11].

Слідчі НП України, Служби безпеки України під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні також можуть виявити кіберзлочини.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. Проаналізувавши теоретичні та практичні дослідження щодо визначення поняття кіберзлочину, можна зробити висновок, що серед сучасних українських науковців немає єдиного підходу до визначення терміна «кіберзлочин». До того ж підходи досить суттєво відрізняються, що може бути причиною хибного трактування, а це, у свою чергу, може призвести до неправильної кваліфікації злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівні.

2. Під час аналізу відповідності національної нормативно-правової бази щодо протидії кіберзлочинам установлено, що на сьогодні законодавцем приділено значну увагу питанню кібербезпеки в нашому суспільстві. Законодавцем напрацьовано певну нормативно-правову базу кібернетичної безпеки України, яку формують Конституція України, закони України «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України» та ін., Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згоду на обов'язковість яких надано Верховною Радою України.

Однак, попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення. Законодавство України про кримінальну відповідальність не містить у повному обсязі понять, що розкривають кіберзлочинність. Загалом у КК України немає термінів із префіксом «кібер-», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку. Уважаємо за доцільне стверджувати або висловити думку, що Кримінальний кодекс України повинен бути оновлений відповідно до сучасних термінів, які б розкривали суть кіберзлочинів, у розділі, що передбачає відповідальність за них.

3. Відкриті можливості людей щодо використання кіберпростору обумовлюють виникнення нових загроз. Кіберзлочини мають велику кількість різноманітних видів та форм, які постійно трансформуються, удосконалюються та несуть загрози для інтересів особи та суспільства в цілому.

РОЗДІЛ 2. КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

2.1. ВИДИ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

Несанкціоноване втручання, а саме знищення, зміна чи блокування інформації, яка обробляється в ЕОМ (комп'ютерах), на сьогодні є одним із найпоширеніших видів кримінальних правопорушень у сфері використання ЕОМ і невдовзі, найімовірніше, займе лідерські позиції у цій категорії злочинів, ураховуючи курс країни на переведення всіх можливих сервісів в електронний вигляд. З одного боку, оцифровування всіх сфер діяльності більш зручне, а з іншого – чинне законодавство нині зовсім не досконало регулює всі процеси у сфері кіберпростору [43, с. 3].

Цей вид злочинів характеризується тим, що особа, яка має законний доступ до ЕОМ, наприклад до якогось реєстру чи бази, вчиняє у ньому певні несанкціоновані, всупереч установленому законом порядку, дії, спрямовані на зміну, видалення чи блокування інформації.

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, – *<…>.*

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, *– <…>.* [30].

Безпосередній об'єкт злочину – нормальне функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, комп'ютерної інформації.

Предмет злочину – інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах [43, с. 5].

Системами автоматизованих електронно-обчислювальних машин є операційні системи (MS-DOS, Windows та інші), які встановлюються на певній машині та за допомогою яких здійснюється її робота, а також різні прикладні системи (тобто інформаційні системи, у т. ч. системи управління), як встановлені для локальної роботи на певній машині, так і відкриті для доступу з інших машин через комп'ютерну мережу.

Комп'ютерна мережа – це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів іншої (інших) ЕОМ та до інформації, що зберігається в системі іншої (інших) ЕОМ.

Ознакою предмета цього злочину є те, що така інформація оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Оброблювання інформації – це виконання певних дій за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, які включають різні види маніпуляцій з такою інформацією згідно з відповідними комп'ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ тощо. Поняття «*оброблення комп'ютерної інформації*» включає в себе і зберігання такої інформації.

Об'єктивна сторона злочину полягає в несанкціонованих зміні, знищенні або блокуванні комп'ютерної інформації. Обов'язковими ознаками зміни, знищення або блокування комп'ютерної інформації є те, що ці дії є ***несанкціонованими***, тобто на вчинення таких дій особа, яка має доступ до цієї інформації, ***не має ні дійсного, ні передбачуваного права*** [43, с. 5].

Зміна інформації полягає в будь-якій модифікації інформації, що призводить до її перекручування, хоча при цьому інформація в цілому зберігається. До зміни інформації слід віднести і її доповнення

іншими, фальсифікованими даними. Причому йдеться про модифікацію змісту інформації. Тому не можна розглядати як ознаку вказаного злочину зміни, які ЕОМ здійснює автоматично, наприклад фіксацію часу і факту користування ЕОМ, активізацію (використання) певних файлів та ін.

Знищення інформації – це такий вплив на комп'ютерну інформацію, внаслідок якого власник позбавляється цієї інформації, тобто втрачає її повністю.

Незаконне втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж – це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини.

Комп'ютерна інформація – це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватися, змінюватися чи використовуватися за допомогою ЕОМ [43, с.6].

Ч. 1 ст. 361 КК України охоплюються як випадки проникнення (впливу) в ЕОМ, що працює, систему чи мережу (наприклад, проникнення до системи одного персонального комп'ютера, який працює, з іншого персонального комп'ютера), так і несанкціоноване увімкнення машини, що не працює, і проникнення до її системи (вплив на її роботу), якщо воно здійснюється за допомогою зазначених у цій статті знарядь.

Суб'єктивна сторона – умисна форма вини.

Мотив і мета значення для кваліфікації не мають, але якщо при цьому передбачається (як варіант, щоб уникнути повтору однакових слів) вчинення іншого злочину, то такі дії підлягають кваліфікації за сукупністю злочинів.

Суб'єкт злочину – спеціальний; ним може бути осудна фізична особа, яка досягла 16-річного віку і має право (на підставі трудових правовідносин або договору, або інших юридичних підстав) доступу до комп'ютерної інформації чи носіїв такої інформації.

Стаття 361[1]. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*, – <…>.*

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду*, – <…>.* [30].

Основним об'єктом цього злочину вважаються окремі суспільні відносини щодо встановленого порядку функціонування ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку.

Додатковим об'єктом злочину, передбаченого ст. 361-1 КК України, можуть бути суспільні відносини, пов'язані із забезпеченням власності на комп'ютерну інформацію, та відносини надання й отримання послуг електрозв'язку, виключно санкціонованого доступу до програмного і технічного забезпечення, комп'ютерної інформації, засобів мереж електрозв'язку, тобто право користувачів на доступ до зазначеної інформації та користування нею. Невід'ємною складовою зазначених правовідносин є:

- право власника (користувача) на безпеку конфіденційного чи таємного користування програмним і технічним забезпеченням, комп'ютерною інформацією, засобами мереж електрозв'язку;
- обов'язок осіб утримуватися від несанкціонованого втручання в роботу цих елементів. Право конфіденційності чи таємності в користуванні програмним і технічним забезпеченням, комп'ютерною інформацією, а також засобами мереж електрозв'язку є похідним від права власника (користувача) контролювати доступ до наявної інформації шляхом встановлення певного режиму, передбаченого ст. 28 Закону України «Про інформацію».

Потрібно зауважити, що специфіка механізму заподіяння шкоди цим суспільним відносинам у результаті вчинення означеного злочину

полягає в тому, що через створення, розповсюдження або збут шкідливих програмних чи технічних засобів створюється реальна загроза порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

Предмет злочину – шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку.

Шкідливі технічні засоби – це різні прилади, обладнання, устаткування тощо, за допомогою яких здійснюється несанкціонований доступ до ЕОМ чи АС. Причому ці засоби здатні призвести до витоку, втрати (знищення), підробки (фальсифікації), блокування інформації, спотворення процесу обробки інформації, що функціонує в ЕОМ, автоматизованих системах, комп'ютерних системах чи мережах електрозв'язку, або до порушення встановленого порядку її маршрутизації (ст. 361 КК України). Обов'язковою ознакою предметів зазначеного злочину є те, що їхнє призначення – це несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби як предмет злочину, передбаченого ст. 361-1 КК України [44, с. 9].

Автоматизована система (АС) – система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу та комплексу засобів автоматизації.

Комп'ютерна мережа – система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа – це система зв'язку через кабельне чи повітряне середовище.

Об'єктивна сторона злочину характеризується певними альтернативними діями:

1) створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку;
2) розповсюдження таких програмних чи технічних засобів;
3) збут указаних програмних чи технічних засобів.

Такий злочин (ч. 1 ст. 361-1 КК України) є злочином із формальним складом і для наявності його об'єктивної сторони не потрібне настання суспільно небезпечних наслідків.

Суб'єктивна сторона характеризується прямим умислом. Під час створення шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, необхідно встановити як обов'язкову ознаку, вказану в диспозиції ст. 361-1 КК України, *спеціальну мету* – ***використання, розповсюдження або збут цих шкідливих програмних чи технічних засобів*** [44, с. 10].

Використання шкідливих програмних чи технічних засобів як мета злочину означає, що під час створення зазначених засобів особа прагне застосовувати ці шкідливі предмети за їх призначенням, тобто для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Суб'єкт злочину – фізична, осудна особа, яка досягла 16-річного віку. У частині 2 ст. 361-1 КК України встановлено кримінальну відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду (поняття «значна шкода» визначена у примітці до ст. 361 КК України).

Стаття 361². 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

1. 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, створеної та захищеної відповідно до чинного законодавства, – *<…>.*

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – *<…>.* [30].

Безпосередній об'єкт – нормальне (безпечне) функціонування комп'ютерної інформації з обмеженим доступом.

Предмет злочину – інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або носіях такої інформації, створена та захищена відповідно до чинного законодавства.

Комп'ютерна інформація з обмеженим доступом, згідно зі ст. 30 Закону України «Про інформацію», за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація містить відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і можуть поширюватися лише за їх бажанням і згодою до встановлених умов, і мають відповідний правовий статус. Режим доступу до конфіденційної інформації громадян та юридичних осіб визначають самостійно та встановлюють для неї систему способів захисту компетентні державні органи або власники інформації.

До **таємної інформації** належить інформація, що містить відомості, які становлять державну та іншу, передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству або державі.

Перелік відомостей, що становлять державну таємницю, визначається Законом України «Про державну таємницю» в редакції від 21 вересня 1999 р. До іншої передбаченої законом таємниці належить комерційна, банківська, лікарська таємниці, таємниця листування та ін. Правовий режим цих видів таємниць (інформації) регламентується спеціальними законами. Проте зазначені види інформації розглядають також і як предмети інших (самостійних) злочинів. Так, кримінальну відповідальність за збут або розповсюдження вказаних видів інформації передбачено статтями 145, 121, 232, 328 та ін. (за умов відсутності ознаки злочинів проти основ національної безпеки України). Але якщо така інформація, що зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях інформації, несанкціоновано здобувається або розповсюджується, – усе вчинене має кваліфікуватися за сукупністю злочинів – за ст. 361-2 і відповідною статтею КК України, яка встановлює відповідальність за збут чи розповсюдження конкретного виду інформації з обмеженим доступом (таємниці).

Інформація з обмеженим доступом як предмет злочину має зберігатися в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних

мережах. Інформація, яка зберігається в мережах електрозв'язку, до предмета даного злочину не належить [45, с. 12].

Ознакою комп'ютерної інформації з обмеженим доступом є те, що вона повинна бути створена та захищена відповідно до чинного законодавства. При цьому в кожному випадку для з'ясування наявності цієї ознаки слід застосувати відповідні закони чи підзаконні нормативно-правові акти, у яких регламентується порядок створення і захисту такої інформації.

Об'єктивна сторона злочину полягає у вчиненні несанкціонованого збуту або розповсюдженні комп'ютерної інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації (ст. 361 КК України).

Несанкціонований збут інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, – це несанкціоноване розповсюдження такої інформації без згоди її власника на платній основі – шляхом купівлі-продажу, міни та ін.

Несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), АС, комп'ютерних мережах або на носіях такої інформації, – це вчинення будь-яких дій, якими без згоди власника інформації така інформація безпосередньо чи опосередковано надається іншим особам чи доводиться до їх відома, вводиться в обіг шляхом будь-якої, крім оплатної, форми. Тобто відбувається «передача права володіння» такою інформацією іншим особам, а так само розголошення інформації. Такий злочин (ч. 1 ст. 361-2 КК України) має формальний склад, і тому вважається закінченим з моменту вчинення суспільно небезпечних дій, зазначених у законі [45, с. 12].

Суб'єктивна сторона характеризується виною у формі прямого умислу.

Суб'єкт злочину – фізична, осудна особа, яка досягла 16-річного віку.

У частині 2 ст. 361-2 КК України встановлено кримінальну відповідальність за ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

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

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, *– <…>.*

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, *– <…>.*

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, **–** *<…>.* [30].

Безпосередній об'єкт злочину – нормальне функціонування ЕОМ (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, комп'ютерної інформації.

Предмет злочину – інформація, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах. Ознакою предмета цього злочину є те, що ця інформація обробляється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Оброблювання інформації – це виконання певних дій за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем чи комп'ютерних мереж, які включають у себе різні види маніпуляцій з такою інформацією згідно з відповідними комп'ютерними програмами, інструкціями, завданнями, технічними можливостями ЕОМ і т. ін. Поняття оброблення комп'ютерної інформації охоплює і зберігання такої інформації. Предметом цього злочину також є інформація, яка зберігається на носіях цієї інформації [45, с. 13].

Об'єктивна сторона злочину полягає у несанкціонованій зміні, знищенні або блокуванні комп'ютерної інформації.

Обов'язковими ознаками зміни, знищення або блокування комп'ютерної інформації є те, що ці дії є несанкціонованими, тобто на вчинення таких дій особа, яка має доступ до цієї інформації, не має ні дійсного, ні передбачуваного права.

Зміна інформації полягає в будь-якій модифікації інформації, що призводить до її перекручення, хоча при цьому інформація в цілому зберігається. До зміни інформації слід віднести і її доповнення іншими, фальсифікованими даними. Причому йдеться про модифікацію змісту інформації. Тому не можна розглядати як ознаку цього злочину зміни, які ЕОМ здійснює автоматично, наприклад фіксацію часу і факту користування ЕОМ, активізацію (використання) певних файлів тощо.

Знищення інформації – це такий вплив на комп'ютерну інформацію, внаслідок якого власник позбавляється цієї інформації, тобто втрачає її повністю.

Суб'єктивна сторона – умисна форма вини. Мотив і мета значення для кваліфікації не мають, але якщо при цьому метою є вчинення іншого злочину, то такі дії підлягають кваліфікації за сукупністю злочинів.

Суб'єкт злочину – спеціальний: ним може бути особа осудна, фізична, яка досягла 16-річного віку і має право (на підставі трудових правовідносин або договору, або інших юридичних підстав) доступу до комп'ютерної інформації або носіїв такої інформації, має право експлуатувати, використовувати за дорученням (і в межах доручення) власника ЕОМ, АС, комп'ютерні мережі чи носії комп'ютерної інформації.

У частині 2 ст. 362 КК України (додала) встановлено кримінальну відповідальність за перехоплення або копіювання інформації, яка оброблюється в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації.

Об'єктивну сторону цього злочину становлять дії, які полягають у несанкціонованому перехопленні або копіюванні інформації.

Перехоплення інформації – це протиправне заволодіння комп'ютерною інформацією, яка функціонує в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах. Ці дії можуть полягати у простому ознайомленні з інформацією, блокуванні такої інформації, затриманні передачі та її ненадходженні до адресата протягом певного часу й ін.

Копіювання інформації – це її відтворення в електронному вигляді, перенесення на інші носії інформації, наприклад, шляхом сканування-випромінювання монітора, спеціальними технічними засобами. Під час копіювання комп'ютерної інформації завжди відбувається відтворення інформації на певних носіях (створення копії) суб'єкта злочину, причому інформація як така залишається непорушеною, у розпорядженні власника (користувача). Копії ж такої інформації отримує суб'єкт злочину.

Перехоплення або копіювання комп'ютерної інформації повинно бути несанкціонованим, тобто незаконним, коли особа на вчинення вказаних дій не має ні дійсного, ні передбачуваного права.

Обов'язковою ознакою цього злочину (ч. 2 ст. 362 КК України) є те, що внаслідок несанкціонованого перехоплення або копіювання інформації, яка оброблюється в ЕОМ (комп'ютерах), АС чи комп'ютерних мережах та яка зберігається на носіях такої інформації, наявний витік комп'ютерної інформації як обов'язковий наслідок цього злочину.

Суб'єктивна сторона та суб'єкт злочину тотожні за ознаками складу злочину, передбаченого ч. 1 ст. 362 КК України. У частині 3 ст. 362 КК України встановлено кримінальну відповідальність за дії, вказані в частині 1 або 2 цієї статті, які вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

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

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, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, – <…> [30].

Безпосередній об'єкт – нормальне функціонування ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку.

Предмет злочину – ЕОМ (комп'ютери), АС, комп'ютерні мережі, мережі електрозв'язку, комп'ютерна інформація, а також інформація, що передається мережами електрозв'язку.

Об'єктивна сторона характеризується певними обов'язковими ознаками:

а) суспільно небезпечними діяннями (діями чи бездіяльністю) у формі: порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку або порушення порядку чи правил захисту інформації, яка в них обробляється;
б) суспільно небезпечними наслідками у вигляді значної шкоди, яка спричиняється вказаними діями;
в) причинним зв'язком між суспільно небезпечними діяннями та суспільно небезпечними наслідками [45, с. 14].

Стаття 363 КК України має бланкетну диспозицію. Отже, під час визначення правил, які порушуються суб'єктом злочину, слід застосувати відповідні закони чи підзаконні акти, у яких установлено правила експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, порядок і правила захисту інформації, яка обробляється у вказаних електронних і електротехнічних системах. Порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку може виражатися у невиконанні або неналежному виконанні уповноваженою особою обов'язків із дотримання правил експлуатації вказаних ЕОМ та мереж електрозв'язку. Ці порушення можуть виявлятися в порушенні як правил апаратного забезпечення, так і правил експлуатації їх програмного забезпечення.

Порушення порядку чи правил захисту інформації, яка обробляється ЕОМ (комп'ютерами), АС, комп'ютерними мережами чи мережами електрозв'язку, – це невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації, що обробляється у вказаних електронних системах особами, які мають здійснювати відповідні заходи із забезпечення захисту інформації.

Основними методами та видами технічного захисту комп'ютерної інформації є використання належних технічних засобів захисту, регламентація роботи користувачів програмних засобів, елементів і баз даних, носіїв інформації, пошук, виявлення та блокування додаткових пристроїв для контролю, приладів та ін., які надають можливість викрадати, копіювати інформацію чи знищувати її тощо.

Суспільно небезпечними наслідками порушення правил експлуатації ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку, порушення порядку чи правил захисту інформації, яка в них обробляється, можуть бути: витік (у тому числі викрадання, копіювання, повна чи часткова втрата інформації), модифікування, блокування інформації, підробка, а також порушення встановленого порядку її маршрутизації та ін.

Ознакою цих наслідків є те, що вказані дії повинні заподіяти значну шкоду власнику інформації (поняття «значна шкода» визначено в ст. 361 КК України). Між діями (в альтернативі), що утворюють об'єктивну сторону такого злочину, і суспільно небезпечними наслідками слід встановлювати необхідний причинний зв'язок.

Суб'єктивна сторона злочину характеризується умисною чи необережною формою вини щодо порушення правил експлуатації ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку або порядку чи захисту інформації і необережною формою вини щодо суспільно небезпечних наслідків – значної шкоди, яка спричинена власнику інформації.

Суб'єкт злочину – особа фізична, осудна, яка досягла 16-річного віку і відповідає за експлуатацію ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку або повинна забезпечувати правила захисту інформації, яка в них обробляється (спеціальний суб'єкт).

Стаття 363[1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

***1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**, – <…>.*

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, – <…> [30].

Безпосередній об'єкт – нормальне функціонування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Предмет злочину – ЕОМ (комп'ютери), АС, комп'ютерні мережі чи мережі електрозв'язку, комп'ютерна інформація, а також інформація, що передається засобами електрозв'язку.

Об'єктивна сторона характеризується:

а) суспільно небезпечними діями у вигляді масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів;
б) суспільно небезпечними наслідками у вигляді порушення або припинення роботи автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
в) причинним зв'язком зазначених дій із наслідками.

Масове розповсюдження повідомлень електрозв'язку – це надання значній кількості адресатів (досить широкому невизначеному колу осіб) без їх попередньої згоди як однакових, так і різних за змістом повідомлень. Передавання одного чи більше повідомлень одному адресатові або чітко визначеній їх кількості не може розглядатися як масове розповсюдження і не може становити складу цього злочину.

Повідомлення електрозв'язку – це певна інформація (відомості), що сповіщаються комусь і передаються мережами електрозв'язку. У цих повідомленнях можуть судження, які підтверджують певні факти або їх заперечують. Сигнали електрозв'язку, які не містять певних відомостей, не охоплюються цим поняттям. Під час учинення такого злочину повідомлення електрозв'язку розповсюджуються через систему ЕОМ (комп'ютери), АС, комп'ютерні мережі чи мережі електрозв'язку, у тому числі й через інтернет-систему. Як правило, це зайві для адресата, не запитувані ним і не бажані для нього нав'язливі електронні повідомлення рекламного, інформаційно-політичного або комерційного характеру. Ця інформація (відомості) стосується конкретних осіб, організацій, політичних діячів, окремих партій тощо.

Отримання адресатами повідомлень електрозв'язку (навіть коли воно має масовий характер) за їх попередньою згодою не містить складу злочину.

Суспільно небезпечними наслідками цього злочину є порушення або припинення роботи ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку.

Порушення роботи ЕОМ (комп'ютерів), АС, комп'ютерних систем чи систем електрозв'язку – це порушення повне чи часткове процесу функціонування вказаних ЕОМ або повна чи часткова втрата контролю над ними. Унаслідок порушення роботи мережі електрозв'язку втрачається також і здатність забезпечувати захист інформації, що передається нею, від знищення, перекручення, блокування, несанкціонованого витоку або від порушення встановленого порядку маршрутизації.

Припинення роботи ЕОМ (комп'ютерів), АС чи комп'ютерних мереж відбувається у разі, коли вони взагалі перестають працювати і не можуть виконувати операції зі або щодо збереження, введення, записування, фіксування, перетворення, зчитування, знищення, реєстрації інформації та ін.

Припинення роботи мережі електрозв'язку – це припинення виконання мережами електрозв'язку функцій із передавання або прийняття знаків, сигналів, письмового тексту, зображень та звуків або інших повідомлень по радіо-, проводових, оптичних або інших електромагнітних системах. Між суспільно небезпечними діями і суспільно небезпечними наслідками необхідно встановити причинний зв'язок.

Суб'єктивна сторона – умисна форма вини, мотиви і цілі для кваліфікації злочину значення не мають.

Суб'єкт злочину – будь-яка фізична особа, що досягла 16-річного віку.

У частині 2 ст. 363^1 КК України (додала) встановлено кримінальну відповідальність за ті самі дії, які вчинені повторно або за попередньою змовою групою осіб.

При цьому для наявності вказаних кваліфікованих ознак складу цього злочину слід обов'язково встановити, що такими діями завдано значної шкоди.

2.2. НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ В ДЕРЖАВНІ РЕЄСТРИ

Якщо йдеться безпосередньо про вказаний вид злочинів у сфері вчинення реєстраційних дій, то зазвичай у багатьох співробітників правоохоронних органів через незрозумілі причини сформувалася хибна думка про діяльність державних реєстраторів та переважно нотаріусів, які начебто повинні перевіряти тільки наявність документів та присутність сторін і все, більше до їх обов'язків нічого не належить. Це абсолютно помилкова позиція, яка спростовується Законом України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» та іншими нормативно-правовими актами, що регулюють вчинення реєстраційних дій [43, с. 8].

Державний реєстратор виконує згідно із законодавством свої основні обов'язки, які зазвичай ігноруються під час учинення протиправних дій, а саме:

1) встановлює відповідність заявлених прав і поданих отриманих документів вимогам законодавства, а також відсутність суперечностей між заявленими та вже зареєстрованими речовими правами на нерухоме майно та їх обтяженнями, зокрема:
   - відповідність повноважень особи, яка подає документи для державної реєстрації прав, *наприклад підроблена довіреність чи особа, яка не стосується певного товариства чи майна;*
   - відповідність відомостей про речові права на нерухоме майно та їх обтяження, що містяться у Державному реєстрі прав, відомостям, що містяться у поданих / отриманих документах;
   - наявність обтяжень прав на нерухоме майно;
2) перевіряє документи на наявність підстав для проведення реєстраційних дій, зупинення розгляду заяви про державну реєстрацію прав та їх обтяжень, зупинення державної реєстрації прав, відмови в державній реєстрації прав та приймає відповідні рішення. *Реєстратор не повинен одразу вчиняти реєстраційну дію, він має провести перевірку документів та з'ясувати або вирішити, чи дають ці документи підстави на заявлену реєстраційну дію;*

3) під час проведення державної реєстрації прав, що виникли в установленому законодавством порядку до 1 січня 2013 року, а також під час проведення державної реєстрації прав, які набуваються з прав, що виникли в установленому законодавством порядку до 1 січня 2013 року, обов'язково запитує від органів влади, підприємств, установ та організацій, які відповідно до законодавства проводили оформлення та/або реєстрацію прав, інформацію (довідки, засвідчені в установленому законодавством порядку копії документів тощо), необхідну для такої реєстрації, у разі відсутності доступу до відповідних носіїв інформації, що містять відомості, необхідні для проведення державної реєстрації прав, чи у разі відсутності необхідних відомостей в єдиних та державних реєстрах, доступ до яких визначено цим Законом, та/або у разі, якщо відповідні документи не були подані заявником, крім випадків, коли державна реєстрація прав, похідних від права власності, здійснюється у зв'язку із вчиненням нотаріальної дії та такі документи були надані у зв'язку з вчиненням такої дії. *На цю норму необхідно звертати увагу під час учинення реєстраційних дій, наприклад, щодо «земельних актів», які були видані до 2012 року, коли під один бланк документа, датований кінцем 90-х років, реєструється земля на праві власності за різними громадянами тощо;*
4) під час проведення реєстраційних дій обов'язково використовує відомості Державного земельного кадастру та Єдиного реєстру дозвільних документів, що дають право на виконання підготовчих та будівельних робіт і засвідчують прийняття в експлуатацію закінчених будівництвом об'єктів, відомостей про повернення на доопрацювання, відмову у видачі, скасування та анулювання зазначених документів, а також відомості інших реєстрів (кадастрів), автоматизованих інформаційних систем, держателем (розпорядником, володільцем, адміністратором) яких є державні органи, шляхом безпосереднього доступу до них чи у порядку інформаційної взаємодії з Державним реєстром прав, у тому числі відомості, що містять персональні дані особи, *наприклад*, *коли реєстрація новозбудованих об'єктів нерухомості відбувається без передбачених законом документів;*

5) виготовляє електронні копії документів, поданих у паперовій формі, та розміщує їх у реєстраційній справі в електронній формі у відповідному розділі Державного реєстру прав (у разі якщо такі копії не були виготовлені під час прийняття документів за заявами у сфері державної реєстрації прав). *Якщо в реєстрі відсутні сканкопії документів, це свідчить, що реєстраційна дія заслуговує на посилену увагу.*

Зважаючи на зазначений перелік обов'язків, убачається, що перевірку суб'єкти державної реєстрації повинні проводити не поверхневу за їх бажанням, а відповідно до конкретних норм законодавства.

Способи вчинення злочинів

1. Незаконне відчуження майна або юридичної особи

1.1. Державний реєстратор (нотаріус) вчиняє реєстраційні дії всупереч установленому законом порядку, зокрема незважаючи на положення (пропоную додати) Закону України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» (*приймає документи, на підставі яких вчиняється реєстраційна дія, у неуповноваженої особи або за підробленими рішенням суду, довіреностями, протоколами загальних зборів, не проводить перевірку достовірності документів за доступними реєстрами та інформаційними базами, не надає запити до органів державної влади щодо підтвердження видачі ними документів, датованих до 2013 року*).

1.2. Державний реєстратор вчиняє реєстраційні дії щодо відчуження юридичної особи, на балансі якої наявне майно, заводи, офісні приміщення тощо) або з метою доступу «зацікавлених осіб» до банківських рахунків усупереч Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань» [43, с. 10].

Коментар

Формально в таких діях убачаються ознаки кримінального правопорушення, передбаченого ч. 3 ст. 362 КК України,. Оскільки) здійснюється втручання в державні реєстри всупереч установленому законами порядку особою, що має доступ до такого реєстру, та в результаті призводить до нанесення шкоди потерпілому. Тому в описаних випадках необхідно насамперед брати до уваги матеріальну шкоду, тому що кримінальне провадження за ч. 1 ст. 362 КК України, кваліфікація якої не

передбачає наслідків, згідно зі ст. 477 КПК України (приватне обвинувачення) відкривається за заявою потерпілого.

ХАРАКТЕРНИЙ ПРИКЛАД

Фрагмент вироку

Відповідно до наказу № 2076-к начальника Головного управління юстиції в Одеській області від 30.12.2011 ОСОБА_1 була призначена на посаду головного спеціаліста відділу державної реєстрації речових прав на нерухоме майно реєстраційної служби Одеського міського управління юстиції, тобто маючи доступ до комп'ютерної інформації, яка знаходиться в Державному реєстрі речових прав на нерухоме майно, Реєстрі прав власності на нерухоме майно, Державному реєстрі іпотек, Єдиному реєстрі заборон відчуження об'єктів нерухомого майна, здійснила несанкціоновану зміну інформації в ньому.

12.03.2013 близько 12:00 годин невстановлена особа з метою скасування арешту на кв. АДРЕСА_3 , використовуючи підроблений паспорт громадянина України та ідентифікаційний код, видані на ім'я ОСОБА_2, знаходячись у приміщенні реєстраційної служби Одеського міського управління юстиції, розташованого за адресою: м. Одеса, вул. Старицького, 10/А подала до реєстраційної служби Одеського міського управління юстиції заповнену заяву про державну реєстрацію прав та їх обтяжень (штамп вих. № 496 від 07.02.2013), до якої долучила перелік документів, серед яких є підроблені, а саме: супровідний лист Київського районного суду міста Одеси № С-14 від 12.03.2012 року (штамп вих. № 496 від 07.02.2013), поверх якого поставлений штамп Державної реєстраційної служби Головного управління юстиції в Одеській області, у повноваження якої на 12.03.2012 року не входило припинення обтяжень, та завідомо підроблену копію ухвали Київського районного суду м. Одеси від 05.03.2011 у справі № 2-6712/2011 щодо скасування арешту на кв. АДРЕСА_3 , у якій дата її оголошення 05.03.2013, при цьому на штампі «Ухвала набрала законної сили 12.03.2012» та в резолютивній частині ухвали вказано, що ухвалу направити до державної реєстраційної служби Головного управління юстиції в Одеській області, яка почала здійснювати повноваження щодо припинення обтяження – арешту нерухомого майна лише з 01.01.2013 року.

За фактом подання невстановленою особою до Державної реєстраційної служби Головного управління юстиції в Одеській області завідомо

підроблених вищевказаних документів СВ Київського РВ ОМУ ГУМВС України в Одеській області 08.09.2015 до Єдиного реєстру досудових розслідувань були внесені відомості за № 12015160480004595 за ознаками кримінального правопорушення, передбаченого ч. 3 ст. 358 КК України (у редакції від 05.04.2001 року).

Так, 12.03.2013 о 12:08:37 годин, тобто через менше ніж 2 хвилини з моменту прийняття головним спеціалістом відділу державної реєстрації речових прав на нерухоме майно Реєстраційної служби Одеського міського управління юстиції Рубан М. О. заяви про державну реєстрацію прав та їх обтяжень (штамп вих. № 496 від 07.02.2013) були сформовані інформаційні довідки з Державного реєстру речових прав на нерухоме майно, Реєстру прав власності на нерухоме майно, Державного реєстру іпотек, Єдиного реєстру заборон відчуження об'єктів нерухомого майна.

Після чого, цього ж дня через менше ніж три хвилини з моменту формування інформаційних довідок, головний спеціаліст відділу державної реєстрації речових прав на нерухоме майно реєстраційної служби Одеського міського управління ОСОБА_1 12.03.2013 о 12:11:27 годин, знаходячись у службовому кабінеті відділу державної реєстрації речових прав на нерухоме майно Реєстраційної служби Одеського міського управління юстиції, розташованому по вул. Старицького, 10/А у м. Одесі, діючи умисно та усвідомлюючи протиправний характер своїх дій, встановивши ряд порушень вимог законодавства у поданих документах, у зв'язку з чим не маючи інформації про достовірність їх змісту, знаючи, що основним серед поданих документів є ухвала суду, визнаючи факт відсутності повноважень щодо припинення обтяжень у Державної реєстраційної служби Головного управління юстиції в Одеській області у 2011–2012 роках, оскільки вказані повноваження до них перейшли лише з 01.01.2013 з моменту вступу в законну силу ЗУ «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень», будучи достовірно обізнаною у здійсненні процедури реєстрації прав на нерухоме майно та їх обтяжень, в порушення вимог пункту 10 Порядку державної реєстрації прав на нерухоме майно та їх обтяжень, затвердженим постановою КМУ № 703 (у редакції від 01.01.2013), безпідставно прийняла незаконне рішення про державну реєстрацію прав та їх обтяжень № 820918, після чого, не маючи дійсного права на вчинення вказаних реєстраційних

дій, шляхом внесення запису до вказаного реєстру, здійснила на підставі фальсифікованих даних несанкціоновану зміну інформації, яка міститься в Державному реєстрі речових прав на нерухоме майно відносно об`єкта нерухомості у вигляді квартири АДРЕСА_3, тим самим скасувавши в Державному реєстрі речових прав на нерухоме майно, Реєстрі прав власності на нерухоме майно, Державному реєстрі іпотек, Єдиному реєстрі заборон відчуження об'єктів нерухомого майна діюче обтяження щодо вказаного об'єкта нерухомості [46].

2. Учинення реєстраційних дій для надання законності певним фактам усупереч встановленому законом порядку

Державний реєстратор приймає рішення про державну реєстрацію новозбудованого об'єкта (багатоквартирний будинок) без рішення органів місцевого самоврядування про присвоєння поштової адреси або без уведення в експлуатацію (*зазвичай це відбувається через ухилення забудовниками від сплати пайового внеску в розвиток інфраструктури, на що органи місцевого самоврядування повинні реагувати відмовою у наданні поштової адреси, що, у свою чергу, унеможливлює державну реєстрацію новобудови*) [43, с. 10].

3. Учинення реєстраційних дій неуповноваженою особою або доступ до інформації без наявних повноважень у контексті ст. 361 КК України

Доступ до реєстру, надання витягів, вчинення реєстраційних дій помічником нотаріуса.

ХАРАКТЕРНИЙ ПРИКЛАД

Фрагмент рішення

Обвинуваченій ОСОБА_2 повідомлено про підозру про вчинення несанкціонованого втручання в роботу автоматизованих систем, що призвело до підробки інформації; несанкціонованого втручання в роботу автоматизованих систем, що призвело до підробки інформації, вчиненого повторно; підроблення офіційного документа з метою його збуту, який видається приватним нотаріусом, а також підроблення офіційних документів з метою їх збуту, які видаються приватним нотаріусом, вчинені повторно.

Злочин вчинено за таких обставин. Так, між приватним нотаріусом Івано-Франківського міського нотаріального округу ОСОБА_3 та ОСОБА_2

укладено 2 трудових договори, а саме: від 23.06.2014 на період роботи з 23.06.2014 по 23.02.2015 та від 24.02.2015 по сьогодні, згідно з якими остання перебувала на посаді помічника нотаріуса.

Згідно зі ст. 46-1 Закону України «Про нотаріат» користування єдиними та державними реєстрами здійснюється безпосередньо нотаріусом, який вчиняє відповідну нотаріальну дію.

Однак помічник приватного нотаріуса Івано-Франківського міського нотаріального округу ОСОБА_3 – ОСОБА_2 у періоди часу з 06.09.2014 по 14.09.2014 та з 19.07.2015 по 07.08.2015, діючи умисно, достовірно знаючи про перебування приватного нотаріуса ОСОБА_3 за межами України, не маючи передбаченого Законом дозволу власника (Держателя), яким є Міністерство юстиції України, всупереч вимог ст.ст. 3, 13, 46-1 Закону України «Про нотаріат», п.п. 1.6, 2.3 Порядку ведення Єдиного реєстру спеціальних бланків нотаріальних документів, затверджених наказом Міністерства юстиції України № 2053/5 від 04.11.2009, та п.п. 1.5, 2.4 Положення про Єдиний реєстр довіреностей, затвердженого наказом Міністерства юстиції України № 111/5 від 28.12.2006, дев'яносто сім разів здійснила несанкціоноване втручання в роботу автоматизованих систем (електронних баз даних) державного підприємства «Національні інформаційні системи» (далі ДП «НІС»), що призвело до підробки інформації.

З метою отримання доступу та внесення змін до єдиних та державних реєстрів Міністерства юстиції України, адміністратором якого є ДП «НІС», ОСОБА_3 надано під персональну відповідальність посилений сертифікат відкритого ключа електронного цифрового підпису Акредитованого центру сертифікації ключів Інформаційно-довідкового департаменту Державної фіскальної служби із реєстраційним номером: 3EEE524F3BA9E8BB0400000092B90F009E431300, термін дії з 24.12.2013 по 24.12.2015 (відповідь Івано-Франківської філії ДП «НІС» вх. № 2452). При цьому для входу до Реєстру приватний нотаріус використовує свої особисті ідентифікатори доступу: логін користувача, пароль користувача, електронний цифровий ключ (ЕЦП), які він зобов'язаний зберігати в таємниці та не допускати їх використання третіми особами.

Згідно з отриманою інформацією, ОСОБА_3 за паспортом громадянина України для виїзду за кордон НОМЕР_2 неодноразово виїжджав за межі

України. Так, 19.05.2014 о 04:25 (повітряним транспортом, рейс WRC6061 «Львів – Хургада») покинув територію України, повернення зареєстровано 29.05.2014 о 13:40 (рейс WRC6062 «Хургада – Львів»); 06.09.2014 о 04:54 (рейс 4421 «Київ – Хургада», аеропорт «Бориспіль») здійснив виїзд за межі України, повернення зареєстровано 14.09.2014 о 21:13 (рейс 4424 «Хургада – Київ») та 19.07.2015 о 08:19 (автомобільним транспортом, д.н.з. НОМЕР_1, пункт пропуску «Угринів») покинув територію України, повернення зареєстровано 07.08.2015 о 01:49 (пункт пропуску «Краківець»).

26 липня 2015 року о 12:45 помічник приватного нотаріуса Івано-Франківського міського нотаріального округу ОСОБА_3 – ОСОБА_2, перебуваючи в приміщенні нотаріальної контори за адресою: АДРЕСА_2, достовірно знаючи, що ОСОБА_3 перебуває за межами території України, використовуючи особистий ключ приватного нотаріуса, носій ключової інформації, на якому він розміщений, і пароль доступу до єдиних і державних реєстрів інформаційної системи Міністерства юстиції України, що був виданий ОСОБА_3, діючи умисно, повторно, здійснила несанкціонований вхід в Єдиний реєстр спеціальних бланків нотаріальних документів та внесла в нього завідомо неправдиві відомості про виконання особисто приватним нотаріусом ОСОБА_3, спеціального бланку нотаріального документа серії НАО 134179, що був використаний для посвідчення заяви від ОСОБА_151 в органи нотаріату про згоду на продаж земельної ділянки ОСОБА_152.

27 липня 2015 року о 14:26 помічник приватного нотаріуса Івано-Франківського міського нотаріального округу ОСОБА_3 – ОСОБА_2 перебуваючи в приміщенні нотаріальної контори за адресою: АДРЕСА_2, достовірно знаючи, що ОСОБА_3 перебуває за межами території України, використовуючи особистий ключ приватного нотаріуса, носій ключової інформації, на якому він розміщений, і пароль доступу до єдиних і державних реєстрів інформаційної системи Міністерства юстиції України, що був виданий ОСОБА_3, діючи умисно, повторно, здійснила несанкціонований вхід в Єдиний реєстр спеціальних бланків нотаріальних документів та внесла в нього завідомо неправдиві відомості про виконання особисто приватним нотаріусом ОСОБА_3, спеціального бланку нотаріального документу серії НАО 134180, що був використаний для посвідчення заяви від ОСОБА_153 на ОСОБА_154 на розпорядження всім майном.

У подальшому, після здійснення оплати клієнтами за вчинення нотаріальних дій, ОСОБА_2, будучи обізнаною з Порядком вчинення нотаріальних дій нотаріусами України, затвердженим наказом Міністерства юстиції України від 22.02.2012 № 296/5, та діючи з метою надання правомірності своїм діям, встановлювала особу клієнта, перевіряла його дієздатність, встановлювала його волевиявлення, а також роз'яснювала наслідки вчинення правочину.

Крім того, ОСОБА_2, діючи на виконання свого злочинного умислу та притримуючись норм указаного вище Порядку, з метою внесення відомостей до довіреностей та заяв, перевіряла у зазначених осіб наявність підтверджуючих документів, після чого самостійно складала текст кожної з довіреностей та заяв.

У ході проведення досудового розслідування у вказаному кримінальному провадженні між прокурором, який здійснює процесуальне керівництво досудовим розслідуванням – прокурором відділу процесуального керівництва під час провадження досудового розслідування територіальними органами поліції та підтримання державного обвинувачення управління нагляду у кримінальному провадженні прокуратури Івано-Франківської області Романовським Іллею Олександровичем та підозрюваною ОСОБА_245 було укладено угоду про визнання винуватості від 27 липня 2017 року.

ОСОБА_2 визнати винною у вчиненні злочинів, передбачених ст.ст. 361 ч. 1, 361 ч. 2, 358 ч. 1, 358 ч. 3 КК України, та призначити покарання [47].

2.3. ДЖЕРЕЛА ОТРИМАННЯ ІНФОРМАЦІЇ ДЛЯ АНАЛІЗУ

1. Реєстр судових рішень

Для розуміння механізму документування вказаної категорії злочинів необхідно проаналізувати **Реєстр судових рішень**, що надасть загальне усвідомлення цього виду правопорушення, а також допоможе виявити недоліки й помилки, які допускалися правоохоронними органами під час документування зазначеної категорії злочинів, різницю в кваліфікації тощо.

Зокрема, щоб знайти необхідні рішення, незважаючи на величезні обсяги вироків щодо співробітників поліції чи банківських установ, касирів, прикордонників тощо, можна здійснювати пошук, так: у графу «Пошук за контекстом» уводимо, наприклад, «юстиції OR нотаріального» («OR» – логічний оператор, який здійснює пошук з альтернативою запитуваних параметрів). У розділі «Судова справа – Форма судочинства» необхідно ввести «Кримінальне». У розділі «Судове рішення –Форма судового рішення» вводимо «Вирок». Після цього вивчаємо всі рішення, що стосуються державних реєстраторів та нотаріусів. *Уведення вказаних пошукових параметрів є рекомендованим*. Для того, щоб зрозуміти проблематику, можливі недоліки документування та з'ясувати кваліфікацію, рекомендуємо вивчити повністю хоча б 50–100 рішень суду [48].

2. Офіційний сайт Міністерства юстиції України

На сьогодні є, імовірно, найкращим ресурсом, на якому можна знайти інформацію про протиправні дії державних реєстраторів чи нотаріусів – це архів рішень, прийнятих за результатами розгляду скарг **Колегією Міністерства юстиції України з розгляду скарг на рішення, дії або бездіяльність державного реєстратора, суб'єктів державної реєстрації, територіальних органів Міністерства юстиції України**.

З 2016 року кожного місяця Колегією Міністерства юстиції викладаються у загальний доступ копії рішень щодо всіх (можливо, не всіх) скарг на дії реєстраторів та нотаріусів. На сайті міститься інформація про незаконне втручання в ЕОМ (внесення змін, копіювання тощо), крім того, у рішеннях зазначено норми закону, які порушено, а також розкрито суб'єктів спору, що надасть змогу швидко ідентифікувати осіб та проводити подальшу перевірку. Основним завданням залишається ознайомитися з рішеннями стосовно необхідного регіону та надати правильну кваліфікацію (відрізнити дрібний проступок від діяння, у якому формально містяться ознаки кримінального правопорушення) [49].

Приклад розгляду скарги Колегією Міністерства юстиції з розгляду скарг на рішення, дії або бездіяльність державного реєстратора

Фрагмент

1. *Скаржником зазначено, що 09.08.2018 ТОВ «ПРАЙМ …» незаконно набуто право власності на будівлю, майнові права на яку належать ТОВ «Укрпром…» на підставі договору будівельного підряду від 24.05.2006 № 43, укладеного між ТОВ «Укрпром» та Акціонерним товариством закритого типу будівельною фірмою «Старатель», та які перебувають у заставі в Товариства з обмеженою відповідальністю «Фінансова Оферта».*

2. *Водночас з відомостей Державного реєстру прав установлено, що на підставі оскаржуваного рішення від 09.08.2018 № 42472689, прийнятого державним реєстратором «М», відкрито розділ Державного реєстру прав та здійснено державну реєстрацію права власності ТОВ «ПРАЙМ…» щодо будівлі. Оскаржуване рішення від 09.08.2018 № 424726895 прийнято державним реєстратором «М» за результатом розгляду заяви про державну реєстрацію права власності від 09.08.2018 № 29573861 (далі – Заява), до якої додано акт приймання-передачі від 08.08.2018 № 01-042016, укладений між ТОВ «ПРАЙМ…» та Мармурою Євгеном Петровичем, інформаційна довідка про показники об'єкта нерухомого майна від 08.08.2018 № 86, видана ТОВ «БТІ КОНСАЛТИНГ», та технічний паспорт, виданий ТОВ «БТІ-ПРОФІ», з яких державним реєстратором «М» не було виготовлено електронних копій з розміщенням їх у Державному реєстрі прав.*

3. *Крім того, до Заяви не додано документи, на підставі яких проводиться державна реєстрація права власності, перелік яких визначено частиною першою статті 27 Закону України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень».*

4. *Абзацом другим частини першої статті 16 Закону визначено, що при прийнятті заяви в паперовій формі обов'язково виготовляються електронні копії документів, поданих заявником для проведення реєстраційних дій. Електронні копії документів виготовляються шляхом сканування з подальшим їх розміщенням у Державному реєстрі прав.*

5. *Згідно з частиною першою статті 18 Закону державна реєстрація прав проводиться в такому порядку:*

1) прийняття / отримання документів для державної реєстрації прав, формування та реєстрація заяви в базі даних заяв;

2) виготовлення електронних копій документів, поданих для державної реєстрації прав, шляхом сканування (у разі подання документів у паперовій формі) та їх розміщення у Державному реєстрі прав;

3) встановлення черговості розгляду заяв, зареєстрованих у базі даних заяв;

4) перевіка документів та/або відомостей Державного реєстру прав, відомостей реєстрів (кадастрів), автоматизованих інформаційних систем на наявність підстав для зупинення розгляду заяви, зупинення державної реєстрації прав, відмови у проведенні державної реєстрації прав та прийняття відповідних рішень;

5) прийняття рішення про державну реєстрацію прав;

6) відкриття розділу в Державному реєстрі прав та/або внесення до відкритого розділу або спеціального розділу Державного реєстру прав відповідних відомостей про речові права на нерухоме майно та їх обтяження, про об'єкти та суб'єктів цих прав;

7) формування витягу з Державного реєстру прав про проведену державну реєстрацію прав для подальшого використання заявником;

8) видача / отримання документів за результатом розгляду заяви.

6. *Пунктом 7 частини третьої статті 10 Закону встановлено, що державний реєстратор виготовляє електронні копії документів та розміщує їх у реєстраційній справі в електронній формі у відповідному розділі Державного реєстру прав (у разі якщо такі копії не були виготовлені під час прийняття документів за заявами у сфері державної реєстрації прав).*

Згідно з частиною першою статті 23 Закону розгляд заяви про державну реєстрацію прав може бути зупинено державним реєстратором, зокрема у випадку подання документів для державної реєстрації прав не в повному обсязі, передбаченому законодавством.

Також на цьому порталі можна знайти перелік державних реєстраторів, яких позбавлено доступу до реєстру: https://minjust.gov.ua/spysok-der-reest-ta-not. Це надасть можливість провести додатковий аналіз стосовно діяльності певного суб'єкта, наприклад отримати інформацію для підвердження, що нотаріус, який має «оперативний»

інтерес для правоохоронних органів, уже пройшов перевірку щодо певного факту і притягнутий до дисциплінарної відповідальності. У подальшому за реквізитами наказу про стягнення можна відслідкувати в архіві рішень Колегії Міністерства юстиції України, щодо якої події накладено стягнення. Або ж, навпаки, припинити співпрацю з нотаріусом, який перебуває у необхідному окрузі, та визначити у зв'язку з чим його позбавлено доступу до Реєстрів (як правило, це відбувається через грубе порушення норм законів).

3. ІТС ІПНП «АРМОР»

Для отримання інформації щодо актуальних кримінальних проваджень чи заяв з приводу протиправних діянь державних реєстраторів або нотаріусів можна скористатися ІТС ІПНП «АРМОР». Також за допомогою вказаного ресурсу маємо змогу (як варіант, щоб уникнути повтору слова «можна») відслідкувати системність учинення протиправних дій одним і тим же реєстратором чи нотаріусом (встановлюємо дисциплінарне стягнення щодо протиправних дій особи на сайті Міністерства юстиції України (див. вище), здійснюємо пошук в «АРМОР», у разі якщо стосовно особи неодноразово зустрічаються заяви щодо її протиправних дій у сфері державної реєстрації, то є підстави провести більш детальний аналіз її діяльності) [43].

Приблизний порядок пошуку: «АРМОР» – розширений (аналітичний) пошук – єдиний облік – вкладка «Розширений пошук» – фабула – «неправдиві відомості» – застосувати – «нотаріус» – застосувати – «держреєстратор» – застосувати – «державний реєстратор» – орган (вказуємо орган) – дата та час реєстрації (вказуємо період) – вид документа (ЄО). Окремо можна ввести ст. 361 чи ст. 362 КК України в тій самій директорії, усе залежить від мети пошуку.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Ознаками злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, як правило, є: суспільна небезпечність, протиправність, винність та караність. Наявність зазначених характеристик (пропоную як варіант, щоб уникнути повтору з наступним реченням) є необхідною умовою для визнання скоєного злочином. У свою чергу, елементами складу злочину є: об'єкт, об'єктивна сторона, суб'єкт та суб'єктивна сторона. Ці елементи і є категоріями кримінального права, перелік яких за кримінальним законодавством є вичерпним. Характер й обсяг відповідальності за злочин визначається окремо, вони є наслідком наявних обставин у справі.

2. У багатьох співробітників правоохоронних органів через незрозумілі причини сформувалася хибна думка про діяльність державних реєстраторів та переважно нотаріусів, які начебто повинні перевіряти тільки наявність документів та присутність сторін, більше до їх обов'язків нічого не належить. Це абсолютно помилкова позиція, яка спростовується Законом України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» та іншими нормативно-правовими актами, що регулюють учинення реєстраційних дій.

РОЗДІЛ 3. КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

3.1. ПОЧАТОК ДОСУДОВОГО РОЗСЛІДУВАННЯ

Згідно зі ст. 214 КПК України [50] та вимогами Положення про порядок ведення Єдиного реєстру досудових розслідувань, затвердженого наказом Генерального прокурора України від 6 квітня 2016 року № 139, слідчий, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до ЄРДР та розпочати розслідування.

Прокурорам (процесуальним керівникам) слід ураховувати, що у кримінальних провадженнях щодо злочинів, учинених з використанням електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, основними джерелами інформації, у яких містяться відомості про вчинення кримінальних правопорушень, є:

- повідомлення фізичних або юридичних осіб, представників влади, громадськості або окремих громадян та самостійно виявлені слідчим або іншою службовою особою органів внутрішніх справ з будь-якого джерела відомості про вчинення кримінального правопорушення;
- повідомлення про вчинення кримінального правопорушення, опубліковані в засобах масової інформації, відомості, отримані засобами телефонного зв'язку, телеграфом або іншими засобами зв'язку, про вчинення кримінального правопорушення;
- узагальнені матеріали Державної служби фінансового моніторингу України, які містять відомості про вчинення кримінальних правопорушень;

- матеріали оперативно-розшукових справ оперативних підрозділів правоохоронних органів;
- матеріали, що надійшли від органів іноземних держав [51].

Однак на практиці найпоширенішими підставами для внесення до ЄРДР відомостей про кримінальне правопорушення є:

- самостійне виявлення фактів протиправних дій власниками або користувачами комп'ютерної мережі (бази даних);
- відомості про факти протиправних дій, які стали загальновідомими (наприклад, дані про порушення цілісності (конфіденційності) інформації в інформаційній системі стали загальновідомими, оскільки винна особа особисто про це заявила);
- виявлення ознак кримінального правопорушення правоохоронними органами (наприклад, у ході проведення оперативно-розшукових заходів у межах оперативного супроводження або щодо осіб, які готуються вчинити злочин);
- затримання злочинця на місці вчинення злочину в момент здійснення протиправних дій (наприклад, у момент несанкціонованого копіювання конфіденційної інформації або під час викрадення машинних носіїв з такою інформацією, передачі їх третім особам).

Слід зазначити, що за наявності зареєстрованого у встановленому законом порядку повідомлення про «комп'ютерний злочин» необхідно оцінювати вихідні дані, які утворюють змістовне наповнення елементів криміналістичної характеристики злочинів, зокрема:

1) ознаки злочину;
2) надійність засобів захисту комп'ютерної інформації;
3) спосіб, час та місце здійснення неправомірного доступу (копіювання, модифікація, знищення інформації, внесення шкідливих програм; незаконне втручання в роботу комп'ютерної мережі (пропоную додати) в самій організації або ззовні) і його ознаки;
4) засоби вчинення злочину (технічні, програмні носії інформації); способи подолання захисту (підбір логінів, викрадання паролів, відключення засобів захисту тощо);
5) особи, які вчинили злочин;
6) винність і мотив правопорушників;

7) обставини, які впливають на ступінь тяжкості злочину, а також обставини, що характеризують особу підозрюваного, пом'якшують та обтяжують покарання;
8) характер і розмір шкоди, завданої злочином [44].

До того ж істотним джерелом інформації про обставини, що свідчать про вчинення кримінального правопорушення у сфері інформаційних відносин, можуть бути матеріали оперативно-розшукової діяльності.

Загальному порядку проведення слідчих (розшукових) дій за фактом розповсюдження шкідливих програмних чи технічних засобів притаманний певний алгоритм:

1) отримання та внесення до Єдиного реєстру досудових розслідувань (ст. 214 КПК України) [50] заяв від фізичних осіб та повідомлення від юридичних осіб про вчинення кримінального правопорушення, пов'язаного з виявленням шкідливих програмних і технічних засобів, які незаконно втручаються в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку. Початок досудового розслідування та направлення письмового повідомлення про це прокурору (ст. 214 КПК України) [50];
2) розгорнутий допит заявника про відомі йому ознаки протиправного діяння;
3) витребування і вивчення матеріалів потерпілої сторони, що свідчать про вчинення протиправного впливу на її програмно-технічні засоби;
4) створення слідчо-оперативної групи для проведення обшуку (вважається, що саме із застосуванням цієї дії необхідно проводити огляд місця вчинення злочину) в потерпілої особи із визначенням включення в її склад залежно від обставин відповідних спеціалістів і працівників підрозділу протидії кіберзлочинності. Отримання відповідного рішення слідчого судді, суду на здійснення обшуку за місцем учинення злочину, в якому безпосередньо зазначаються електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку (ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку тощо), які можуть бути тимчасово вилучені для вивчення фізичних властивостей,

що мають значення для кримінального провадження. Виїзд СОГ на місце вчинення злочину та проведення там обшуку.

Варто зауважити, що відповідно до ч. 3 ст. 214 КПК України [50] у невідкладних випадках до внесення відомостей до ЄРДР може проводитися лише огляд місця події, який здійснюється в порядку, визначеному ст. 237 КПК України. Мета цієї слідчої (розшукової) дії полягає у виявленні та фіксації відомостей щодо обставин учинення кримінального правопорушення, а також огляду місцевості, приміщення, речей та документів.

Слід також наголосити, що у практиці правоохоронних органів виникає багато проблемних ситуацій, пов'язаних із посиленням кримінальної активності в комп'ютерній сфері, яка проникла у значну частину традиційно охоронюваних законом суспільних відносин. Останнє суттєво ускладнює кримінально-правову кваліфікацію досліджуваних діянь.

Зокрема, певні складнощі викликає кваліфікація такого діяння, як внесення до комп'ютерної системи неправдивої інформації (наприклад, під час внесення нотаріусом у реєстр незаконно оформленої довіреності). Кримінально-правова кваліфікація такого діяння може відбуватися за різними статтями КК України: 1) ст. 362 КК України; 2) ст. 361 КК України; 3) ч. 3 ст. 190 КК України [30].

3.2. ОСОБЛИВОСТІ ПРОЦЕСУАЛЬНОГО КЕРІВНИЦТВА В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ У СФЕРІ ІНФОРМАЦІЙНИХ (КОМП'ЮТЕРНИХ) ВІДНОСИН

З метою підвищення ефективності протидії злочинам, учиненим із використанням електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, якості досудового розслідування, а також взаємодії між слідчими та оперативними підрозділами прокурору (процесуальному керівнику) доцільно здійснювати такі *організаційні заходи:*

– скликати міжвідомчу робочу групу для розроблення та координації спільних заходів протидії комп'ютерній злочинності

між правоохоронними органами й операторами зв'язку, інтернет-провайдерами, контент-провайдерами, банківськими, фінансовими установами, державними та громадськими організаціями (оскільки результати внутрішніх розслідувань фінансових установ можуть розцінюватися як підстава для початку кримінального провадження та використовуватися під час доказування як на стадії досудового розслідування, так і в ході судового розгляду. Проте в певних випадках вони мають інше правове значення: зокрема, на підставі таких матеріалів можливе прийняття рішень про закриття кримінального провадження (ст. 284 КПК України), застосування до винуватої особи заходів дисциплінарної та матеріальної відповідальності);

– проводити моніторинг оперативної обстановки у сфері інформаційно-телекомунікаційних технологій (із міжнародного досвіду: спочатку створюється міжвідомча система моніторингу оперативної обстановки у сфері інформаційно-телекомунікаційних технологій, а після цього можна впроваджувати застосування ефективних механізмів реагування на повідомлення про можливі кримінальні правопорушення з використанням комп'ютерних технологій та мереж електрозв'язку);
– керівнику прокуратури доручати процесуальне керівництво досудовим розслідуванням кримінальних проваджень зазначеної категорії прокурорам, які володіють необхідними навичками у сфері інформаційних (комп'ютерних) технологій;
– доручати слідчому, органу досудового розслідування проведення у встановлений прокурором строк слідчих (розшукових) дій, негласних слідчих (розшукових) дій, інших процесуальних дій або давати вказівки щодо їх проведення чи брати участь у них, а за необхідності – особисто проводити слідчі (розшукові) та процесуальні дії в порядку, визначеному КПК України [44].

Слід зауважити, що швидкому, повному та неупередженому досудовому розслідуванню кримінальних правопорушень указаної категорії заважає, серед іншого, висока латентність. Основними причинами цього визначено такі: дуже високий рівень кваліфікації осіб, які вчинили злочини, їх уміння приховувати сліди; потерпілі не повідомляють

правоохоронні органи про те, що вони стали жертвами «комп'ютерних» злочинів, через небажання розголосу (розголошення може зашкодити їхньому авторитетові, знизити рівень довіри клієнтів – це насамперед стосується кредитно-фінансових та банківських установ) або через відсутність віри в можливість розкрити злочин; наслідки «комп'ютерних» злочинів пов'язують із збоями в роботі комп'ютерних систем, телекомунікаційних мереж, програмного забезпечення; розглядають наслідки окремих «комп'ютерних» злочинів (наприклад, викрадення комп'ютерної інформації) як шкоду, спричинену іншими видами суспільно небезпечних діянь; низький професійний рівень оперативних працівників, які не вміють виявляти й документувати вчинені злочини; складність розкриття злочинів і доведення вини, а як наслідок – відмова в реєстрації, щоб «не псувати показники».

Специфікою здійснення процесуального керівництва вказаної категорії кримінальних правопорушень є те, що з метою досягнення позитивних результатів, а також для відповідних комп'ютерно-технічних досліджень необхідне використання наукових, технічних та інших спеціальних знань, специфічних програмно-технічних засобів і методів.

Варто пам'ятати, що копіювання, зміна, модифікація, витік, пошкодження, знищення інформації можуть бути викликані не тільки умисними неправомірними діями, а й помилками, неумисною неправильною поведінкою персоналу організації – потерпілого.

Не слід також оминати увагою так звану «корпоративну віктимність», тобто віктимність юридичної особи, існування якої стає можливим завдяки законодавчому визнанню такої особи потерпілим у кримінальному провадженні (ч. 1 ст. 55 КПК України) [50]. Її специфіка полягає в тому, що юридичні особи володіють опосередкованою віктимністю, яка залежить від організації функціонування та безпеки діяльності юридичної особи. Варто зауважити, що тиск на юридичну особу як суб'єкта господарських відносин може чинитися через фізичних осіб (власників, засновників, робітників). Прояв злочинної агресії одночасно має подвійну спрямованість: на людину, від якої залежить діяльність організації, що вчиняється за допомогою застосування незаконного фізичного чи психологічного впливу; на юридичну особу, намагаючись спричинити їй певну шкоду за допомогою застосування економічної агресії [44].

Виявлення несанкціонованого втручання в роботу ЕОМ полягає у застосуванні спеціальних прийомів огляду і фіксації інформації, використанні спеціальних інженерних рішень, обов'язковому залученні фахівця оперативно-технічного підрозділу, тісній взаємодії з операторами зв'язку та провайдерами.

Слід наголосити, що на практиці отримання будь-якої інформації від операторів зв'язку та провайдерів майже неможливе без відповідної ухвали суду або слідчого судді.

Фактичні дані про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, можна визначити як достовірні відомості, отримані уповноваженим підрозділом правоохоронного органу у визначеному правовими актами порядку, про зміст та характер змін, пов'язаних із подіями злочинів у цій сфері як у фізичному (сліди, залишені на предметах та у свідомості людини), так і в електронному середовищі (електронні сліди), на підставі яких можна дійти висновку про наявність або відсутність у цих діяннях ознак конкретного складу злочину.

Тому з метою швидкого, повного та неупередженого розслідування процесуальному керівнику насамперед необхідно вжити заходів щодо встановлення:

- слідів злочину (традиційні та електронні);
- місця неправомірного проникнення в комп'ютерну мережу (зсередини організації, що постраждала, чи ззовні);
- способів здійснення неправомірного доступу (подолання програмних засобів захисту, вилучення засобів комп'ютерної техніки, маніпуляції з даними, керівними командами та інформацією, використання шкідливих програм, технічних прийомів);
- засобів, що використовувалися під час учинення злочину (технічні, програмні та інші);
- способів подолання інформаційного захисту (підбір ключів і паролів, крадіжка паролів, відключення засобів доступу тощо).

Особливості *електронних слідів*:

- місцезнаходження – окремий матеріальний носій комп'ютерної інформації, матеріальний носій в автоматизованій

(комп'ютерній) системі, яка реалізована на основі автономного комп'ютера, комп'ютерної або телекомунікаційної мережі;
- вигляд – кодований цифровий запис графічного, звукового, текстового та іншого характеру на магнітному або оптичному носієві, сукупність електронних імпульсів у мережі;
- необхідність дотримання певних технологічних процедур виявлення, фіксації та вилучення інформації (в електронному вигляді інформація легко піддається зміні, перекрученню, а інформація у вигляді електронних імпульсів узагалі існує лише в окремі моменти реального часу);
- необхідність використання наукових, технічних та інших спеціальних знань, а також програмно-технічних засобів і відповідних технологій, призначених для виявлення, фіксації та відтворення інформації у вигляді, придатному для сприймання людиною [44].

Матеріальними слідами злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна вважати:

- сліди-відображення зовнішнього фізичного впливу на комп'ютерні системи, периферійні пристрої та мережі (сліди рук, ніг, знарядь злому тощо);
- сліди-речовини у вигляді витратних матеріалів (тонерів, фарб, різних мастил, що використовуються в комп'ютерних системах, їх мережах та периферійних пристроях);
- сліди-предмети (змінні диски та стрічки, апаратно реалізовані закладні пристрої, пристрої дистанційного зняття інформації, роздруківки на паперових носіях і документи на електронних носіях, кабелі й роз'єми, пристрої фізичного знищення комп'ютерів та їх мереж) пропоную записати в дужках.

Зауважимо, що у разі вчинення конкретного комп'ютерного злочину треба мову вести про індивідуальну слідову картину. Але все ж таки можна виділити певну специфіку слідової картини цього виду комп'ютерних злочинів. Вона переважно чи здебільшого буде характеризуватися наявністю на носії комп'ютерної інформації зловмисника файлів, що вміщують інформацію з обмеженим доступом, яка стала

предметом злочину, програмні та технічні засоби подолання захисту, отримання інформації шляхом активного чи пасивного перехвату, її декодування, а також іншого спеціального обладнання і програмного забезпечення для отримання комп'ютерної інформації та виготовлення її носіїв, а також розповсюдження і збуту: сканерів, цифрових фотоапаратів, принтерів, пристроїв для запису компакт-дисків, відповідних заготовок, чистих носіїв інформації, засобів підключення до мережі локальної та глобальної (мережа Інтернет) тощо.

Залежно від характеру вихідних даних під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також інших злочинів у сфері інформаційних технологій на початковому етапі розслідування можуть виникати різноманітні слідчі ситуації, які умовно можна поділити на дві групи залежно від змісту вихідної інформації.

Першу групу формують ситуації вчинення зазначеного виду злочинів в умовах так званої «очевидності», коли вихідна інформація містить дані про конкретну особу, яка вчинила кримінальне правопорушення злочинця затримано на місці злочину в момент або безпосередньо після скоєння кримінального правопорушення; встановлено особу злочинця, але він зник з місця скоєння злочину, тощо).

До другої групи належать ситуації вчинення «комп'ютерних» злочинів в умовах «неочевидності», коли вихідна інформація не містить даних про злочин, а відомо лише факт його вчинення (інформації про спосіб учинення злочину й особу правопорушника немає, свідків не встановлено, матеріально фіксовані-их слідів не виявлені-о, місцезнаходження викрадених грошових коштів не встановлено; є дані про спосіб його вчинення, встановлено свідків, але немає матеріально фіксованих слідів учинення злочину та відомостей про особу злочинця).

Для слідчих ситуацій, що виникли *в умовах «очевидності»*, характерний такий алгоритм слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій:

1) огляд місця події із залученням відповідних спеціалістів (спеціаліста-криміналіста, спеціаліста з банківської справи, спеціаліста з інформаційних технологій тощо);

2) особисті обшуки затриманих, їх робочих місць та місць проживання;
3) аудіо-, відеоконтроль особи, накладення арешту на кореспонденцію, огляд і виїмка кореспонденції, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем як таких, що можуть надати істотну допомогу в розкритті зазначеного різновиду злочинів;
4) допит підозрюваних;
5) огляд документів, що характеризують ті виробничі операції, у процесі яких допущені порушення та вчинені злочинні дії;
6) допит осіб, зазначених або указаних у документах, переданих до органів досудового розслідування, як таких, що вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;
7) перевірка підозрюваних за обліками Національної поліції України (ОВС);
8) тимчасове вилучення:
– документів, що характеризують порядок й організацію роботи на підприємстві, в установі чи в організації – місці виявлення слідів злочину;
– документів, що відображають роботу суб'єкта з комп'ютерною інформацією, – журналу оператора ЕОМ, електронного журналу фіксації вчинених операцій, електронного реєстру з'єднань абонентів через ЕОМ або електрозв'язок;
9) допит осіб, причетних до відповідних електронних операцій або підозрюваних у зв'язках із особами, що вчинили злочинні дії;
10) аналіз одержаної інформації та вирішення питання про необхідність залучення до кримінального провадження відповідного експерта з метою проведення ревізії, документальної або іншої перевірки, зокрема повторної (з яких позицій, за який період і за участю яких фахівців).

У вирішенні ситуацій, що виникли в умовах «неочевидності», зазвичай планують та проводять такі початкові слідчі (розшукові), негласні слідчі (розшукові) й інші процесуальні дії:

1) допит заявника та осіб, на яких указано в початковій інформації як на можливих свідків;
2) огляд місця події із залученням відповідних спеціалістів (спеціаліста-криміналіста, спеціаліста з банківської справи, спеціаліста з інформаційних технологій тощо);
3) тимчасове вилучення і подальший огляд засобів комп'ютерної техніки, предметів, матеріалів і документів (зокрема тих, що знаходяться в електронній формі на машинних носіях), які характеризують електронну операцію, під час якої за наявними даними вчинені злочинні дії;
4) вирішення питання про необхідність проведення комп'ютерно-технічних, економічних та інших експертиз;
5) вирішення питання про можливість установлення особи злочинців і затримання злочинця на місці злочину та необхідні у зв'язку з цим заходи;
6) проведення негласних слідчих (розшукових) дій з метою виявлення осіб, винних у вчиненні злочину, а також слідів та інших речових доказів;
7) допити свідків (очевидців), установлених під час проведення розслідування;
8) допити підозрюваних (свідків), відповідальних за проведення операцій, пов'язаних з електронними розрахунками;
9) обшуки на робочих місцях і за місцем проживання підозрюваних у разі їх установлення.

Подальші дії процесуальний керівник, слідчий планують з урахуванням інформації, одержаної в процесі проведення вказаних вище слідчих (розшукових) та негласних слідчих (розшукових) дій.

Якщо у ході розслідування зібрано достатню кількість доказів для складання обвинувального акта стосовно певної особи, таку ситуацію прийнято вважати сприятливою. У цьому разі досудове розслідування визнається закінченим. У протилежному ж випадку наявна одна з проміжних ситуацій, яка, як і початкова, є вихідною для висування версій, планування розслідування, проведення слідчих (розшукових), негласних слідчих (розшукових) дій та оперативно-розшукових заходів.

3.3. ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Підготовка до проведення слідчих (розшукових) дій, спрямованих на збирання інформації в електронній формі

1. Потрібно погодити клопотання про провадження тимчасових доступів до речей і документів з метою фіксації (копіювання) інформації, що становить інтерес для кримінального провадження, або про проведення обшуку з метою фіксації інформації, що становить інтерес для кримінального провадження, або з метою вилучення електронних носіїв інформації (за необхідності подолання систем логічного захисту інформації на носії).

2. Слід володіти визначеною інформацією про об'єкт та предмет слідчої дії.

3. Створити та проінструктувати СОГ.

4. Забезпечити групу необхідними інструментами (або впевнитися в тому, що інструментів достатньо).

5. Забезпечити швидкий та безпечний шлях для проникнення в приміщення та переміщення в ньому [11].

6. У разі проведення обшуку в житлі чи нежитлових офісних приміщеннях, у яких власниками встановлено камери відеоспостереження, забезпечити їх вимкнення.

3.3.1. Огляд місця події

Відповідно до ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин учинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей та документів [50].

Зазначена слідча дія дає змогу встановити значну кількість доказів, які належать до складу злочину (об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони), однак потребує застосування певних тактичних прийомів і засобів криміналістичної техніки.

Для проведення огляду місця події під час здійснення процесуального керівництва та розслідування злочинів, учинених із використанням електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, до СОГ можуть залучатися:

- слідчий, прокурор, який спеціалізується на розслідуванні (процесуальному керівництві) кримінальних правопорушень цієї категорії;
- співробітники оперативних підрозділів (Національної поліції України), Служби безпеки України, Державної фіскальної служби України тощо;
- поняті (ураховуючи, що переважно або здебільшого зазначені злочини вчиняються у співучасті зі співробітниками установи, на території якої вчинено злочин, необхідно відмовитися від їх допомоги як понятих. Натомість запросити осіб, які розуміються на комп'ютерній техніці. Це не допустить розголошення відомостей досудового розслідування, і надалі, за необхідності, такі особи зможуть пояснити в суді перебіг слідчої (розшукової) дії та її результати);
- спеціаліст-криміналіст, що знає особливості роботи зі слідами злочинів цієї категорії;
- спеціаліст у роботі з банківським комп'ютерним обладнанням у сфері мережевих технологій (за наявності на місці події периферійного обладнання віддаленого доступу або локальної комп'ютерної мережі);
- спеціаліст із систем зв'язку (за умови використання для дистанційної передачі даних каналів електрозв'язку);
- інші категорії спеціалістів (інженери-електрики, спеціалісти супутникових систем зв'язку, оператори стільникових, пейджингових, мережі Інтернет).

Після прибуття на місце події члени СОГ з'ясовують обставини вчинення кримінального правопорушення, встановлюють свідків, прикмети осіб, які вчинили кримінальне правопорушення, та ймовірні шляхи їх відходу. За потреби вживають заходів для переслідування транспортних засобів, що використовувалися злочинцями.

Під час огляду місця події в установленому КПК України порядку фіксуються відомості щодо обставин учинення кримінального правопорушення, вилучаються речі та документи, які мають значення для кримінального провадження, і речі обмеженого доступу, у тому числі матеріальні об'єкти, придатні для з'ясування обставин, що підлягають доказуванню. Забезпечується їх належне зберігання з метою подальшого направлення для проведення експертного дослідження.

Прокурорам (процесуальним керівникам) слід мати на увазі, що огляд місця події може проводитися до внесення відомостей про вчинення злочину до ЄРДР. У таких випадках відповідно до ч. 2 ст. 168 КПК України тимчасове вилучення електронних інформаційних систем або їхніх частин, мобільних терміналів, систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, не здійснюється.

У разі необхідності вилучення таких систем потрібно у порядку ст. 160 КПК України звернутися до слідчого судді з клопотанням про надання тимчасового доступу до речей і документів [50].

Стадії огляду місця події доцільно розділити на два етапи:

1) огляд приміщення, де встановлено комп'ютер;
2) безпосередній огляд робочого місця та комп'ютера.

Під час огляду необхідно враховувати, що злочинець може вдаватися до інсценування некримінальної події або вчинення іншого злочину.

Серед інсценувань під час учинення злочинів у сфері комп'ютерної інформації найбільш розповсюджені такі:

1) створення уявлення того, що файли було пошкоджено в результаті невмілого поводження з ними осіб, котрі мають доступ до них на законних підставах;
2) зараження комп'ютерним вірусом користувачем з необережності;
3) пошкодження носія інформації через причини, не пов'язані з роботою користувача (перепади електричної напруги в мережі тощо);
4) інсценування іншого злочину [52, с. 307].

Основними об'єктами, що підлягають огляду, є:

1) приміщення, де розташована комп'ютерна техніка;
2) окремі комп'ютери, які не підключені до мережі;

3) сервери;
4) периферійні телекомунікаційні пристрої;
5) магнітні та оптичні носії інформації;
6) роздруківки та записи;
7) технічна та інша документація [52, с. 307].

Під час огляду та описування слідів комп'ютерного (мережевого) обладнання та місця події варто звернути увагу на:

1) знаряддя вчинення злочинів у сфері комп'ютерної інформації, які за характером доступу поділяються на безпосередні та опосередковані (віддалені).

До знаряддя *безпосереднього* доступу можна віднести носіїв комп'ютерної інформації (USB-флеш-накопичувачі, лазерні диски, дискети, касети з магнітною стрічкою для стримера), різноманітне периферійне устаткування (друкувальний пристрій, CD-ROM-накопичувач, стример, дисководи), а також електронні ключі, особисті ідентифікаційні коди тощо. До знаряддя *опосередкованого* (віддаленого) доступу належать насамперед мережеве устаткування, а також засоби доступу до віддалених мереж (модеми, прилади телефонного та супутникового зв'язку);

2) застосовані способи доступу до комп'ютерної інформації, які також можна класифікувати на безпосередні та опосередковані [51].

Алгоритм дій під час огляду локального комп'ютерного засобу

1) після вмикання комп'ютера необхідно пересвідчитися в налаштуванні bios на завантаження з приводу оптичних дисків або з флеш-накопичувача (у процесі завантаження натиснути клавішу «Del», «Esc» або «F2» під час включення, у разі потреби внести необхідні зміни та перезавантажити);
2) завантажити операційну систему з робочого примірника спеціаліста;
3) підключити принтер, роздрукувати текст із правами й обов'язками учасників слідчої дії, ознайомити їх із цими документами під підпис;
4) приєднати носій, на який здійснюватиметься запис і на якому зберігатиметься інформація, отримана під час огляду, після чого його відформатувати;

5) за допомогою відповідної програми вивести на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, необхідну для його ідентифікації, зберегти її як окремий файл.
6) у разі потреби в перегляді файлів із відеограмами запустити програму запису зображення екрана монітора;
7) здійснити огляд вмісту носіїв інформації, демонструючи учасникам зміст та місцезнаходження (шлях розташування) файлів;
8) у разі потреби та наявності ресурсів здійснити побітове копіювання, створивши файловий образ носія;
9) скопіювати файли з відеограмою та скриншотами зображення екрана монітора;
10) вивести на екран монітора інформацію про контрольну суму кожного файла;
11) приєднати та відформатувати другий носій, після цього скопіювати на нього всю інформацію з контрольного носія;
12) інформацію про здійснений огляд внести до протоколу та роздрукувати його, після чого вирахувати його контрольну суму й обидва файли (протокол і файл з його контрольною сумою) зберегти на контрольному і робочому примірниках носіїв разом з каталогом із доказовою інформацією;
13) від'єднати носії з доказовою інформацією та упакувати.

До вказаного алгоритму дій можна додати додаткові пункти за умови огляду віддаленого ресурсу комп'ютерної мережі щодо встановлення IP-адреси сайта (ping), шляху проходження пакетів у процесі обміну інформацією з ним, скопіювати їх на носій, призначений для запису та зберігання доказової інформації.

Під час реалізації способів безпосереднього доступу інформація знищується, блокується, модифікується, копіюється, а також може бути порушено роботу ЕОМ, комп'ютерної системи або мережі шляхом передачі відповідних команд із комп'ютера, на якому інформація знаходиться. Безпосередній доступ мають особи, які працюють з інформацією, а також особи, котрі спеціально проникають у закриті зони та приміщення, де здійснюється обробка інформації. Іноді злочинець з метою вилучення інформації, залишеної користувачами після роботи ЕОМ, обстежує

робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування («прибирає сміття») або здійснює перегляд і відновлення стертих програм.

У процесі реалізації способів опосередкованого (віддаленого) доступу до комп'ютерної інформації відбувається: підключення до лінії зв'язку законного користувача (наприклад, до телефонної лінії) й одержання таким способом доступу до його системи; проникнення в чужі інформаційні мережі шляхом автоматичного перенабору абонентських номерів з подальшим з'єднанням із тим або іншим комп'ютером. Перенабір здійснюється доти, доки на іншому кінці лінії не «відповість» чужий комп'ютер.

Під час огляду слід дотримуватися таких специфічних умов:

1) не обробляти безпосередньо на місці виявлення пристрої магнітними порошками: використання їх і магнітних пензлів може пошкодити електронні складові та знищити ті сліди, які доцільно та ефективніше було б виявляти в лабораторних умовах (на внутрішньому боці банкомата можуть бути сліди пальців рук та інші сліди біологічного походження осіб, які збирали накладку як пристрій);
2) не вимикати електроживлення пристрою та механічно не роз'єднувати електричні ланцюги, не від'єднувати частини (крім випадків огляду SIM-карток);
3) з метою запобігання обміну інформації між накладкою на банкомат та іншими пристроями через безпровідний зв'язок за можливості поміщати об'єкти до пакетів, контейнерів чи інших пристроїв, що блокують (екранують) сигнал;
4) упаковувати пристрої так, щоб не допустити пошкодження, відокремлення частин, роз'єднання електричних ланцюгів та приклеювання матеріалу упаковки до накладки.

Застосування спеціальних знань у роботі з комп'ютерною технікою необхідне для:

1) визначення статусу об'єкта як машинних носіїв інформації, його стану, призначення та особливостей;
2) дослідження комп'ютерної інформації, включаючи її пошук та вилучення;

3) виявлення ознак і слідів впливу на машинні носії інформації та на саму інформацію;
4) здійснення допоміжних дій із виявлення, закріплення і вилучення доказів.

3.3.2. Обшук

Відповідно до ст. 234 КПК України обшук проводиться на підставі ухвали слідчого судді з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте в результаті його вчинення, а також установлення місцезнаходження розшукуваних осіб [50].

Під час підготовки або погодження клопотання про проведення обшуку прокурору (процесуальному керівнику) слід мати на увазі, що фактичною підставою для проведення вказаної слідчої дії є наявність достатніх відомостей, що вказують на можливість досягнення його мети. До них, зокрема, можна віднести достатні відомості про те, що знаряддя кримінального правопорушення або майно (речі й цінності), здобуті в результаті його вчинення, а також інші предмети та документи, які мають значення для розкриття правопорушення чи забезпечення цивільного позову, відомості про обставини вчинення кримінального правопорушення знаходяться в певному приміщенні або місці чи в якої-небудь особи [51].

Положення ч. 6 ст. 236 КПК України дає право слідчому, прокурору примусово проникати до приміщення, обстежувати його та встановлені на ЕОМ, що знаходяться в цьому приміщенні, програми, файли тощо [50].

Обшук доцільно розділити на три етапи: підготовчий (до виїзду на місцевість), робочий (дослідний) та заключний (фіксація результатів).

1. Підготовчий етап

До виїзду на місце слідчому, прокурору необхідно:

– з урахуванням слідчої ситуації, що виникла, визначити коло осіб, які візьмуть участь у слідчій (розшуковій) дії. Окрім учасників СОГ (прокурора, слідчого, працівників оперативних підрозділів

Національної поліції України, спеціаліста-криміналіста), можуть залучатися спеціалісти, які знають специфіку роботи об'єкта, що оглядається.;

- підготувати відповідну комп'ютерну техніку, програмне забезпечення, що буде використовуватися для зчитування та збереження вилученої інформації. Традиційно відповідні технічні засоби застосовують ІТ-спеціалісти, але це не знімає відповідальності зі слідчого (прокурора) за їх наявність і комплектність [44];
- запросити понятих. Бажано запрошувати таких осіб, які мають достатній рівень знань у галузі комп'ютерних технологій. Якщо немає можливості залучити кваліфікованих понятих, то дії слідчого (спеціаліста) з дослідження ЕОМ чи комп'ютерної інформації повинні пояснюватися. Це необхідно у разі допиту понятих у суді як свідків. Місцем проведення обшуку в указаних злочинах можуть бути: приміщення підприємств, установ, організацій, житлові будинки, квартири, дачі, кімнати, класи, зали, клуби, іноді нежитлові приміщення (кімнати в цокольних будовах, підвали, напівпідвали, гаражі, сараї, інші приміщення);
- пояснити мету проведення слідчої (розшукової) дії та завдання, що стоять перед її учасниками, їх права та обов'язки, а також необхідні заходи обережності під час пересування на місці обшуку або роботи зі слідами тощо;
- залежно від конкретного місця, території, кількості приміщень, засобів охорони, обсягу комп'ютерного оснащення, різновидів і технічних характеристик тощо слідчий разом із спеціалістом чи працівником підрозділу боротьби з кіберзлочинністю розробляє план з організації та ефективного проведення обшуку.

2. Робочий етап

Після прибуття на місце проведення обшуку слідчий, прокурор повинен:

- видалити з місця проведення слідчої (розшукової) дії сторонніх осіб та забезпечити його охорону, якщо це не було зроблено раніше. Обов'язковій охороні підлягають: територія місця події, затриманий, ЕОМ, у якій було виявлено сліди злочину,

сервер, пункти вимкнення живлення, якщо техніка знаходиться у ввімкненому стані, тощо;

- установити місцезнаходження ЕОМ, АС, комп'ютерних мереж та мереж електрозв'язку, які стали об'єктом посягання, їх кількість, а також програмне забезпечення, комп'ютерної інформації та документів, що використовувалися під час підготовки, здійснення і можливого приховування злочину, а також інших криміналістично значущих даних, які стосувалися вчинення протиправної дії. Визначити зміст комп'ютерної інформації, яка могла б бути об'єктом посягання;
- унеможливити вчинення сторонніми особами будь-яких дій із комп'ютерною технікою, їх користування іншими технічними засобами, що можуть за допомогою бездротових технологій вносити зміни в інформацію (видаляти її);
- визначити схематичний план місць проведення огляду, при цьому додатково можуть бути оглянуті інші ЕОМ, АС, комп'ютерні мережі та мережі електрозв'язку щодо наявності в них (впливу на них) шкідливих програмних і технічних засобів;
- установити власника чи користувача, осіб, які мають відповідний допуск до ЕОМ, АС, комп'ютерних мереж, мереж електрозв'язку та носіїв електронних даних, а також осіб, які перебувають на об'єкті, незалежно від їх пояснень щодо мети перебування;
- допитати як свідків потерпілого (заявника), інших осіб про те, що відбулося, зміни, які були внесені в обстановку, дії осіб до прибуття СОГ, види та технологічні операції, під час яких було виявлено ознаки злочину, та ін.;
- дати доручення учасникам СОГ на встановлення свідків, виявлення слідів, їх фіксацію тощо.

Пошук слідів комп'ютерного злочину необхідно розпочинати з виявлення мережевих підключень засобів комп'ютерної техніки, що знаходяться на місці події і в яких виявлені сліди злочину, та дослідження інформації, що пов'язана з цими підключеннями. З цією метою, враховуючи або зважаючи на інформацію, що міститься в записах підключень, слід визначити подальший план чи наступний пункт пошуку слідів аж

до встановлення ЕОМ, яка є предметом злочинного посягання і засобом вчинення злочину.

Найбільш специфічними залишаються сліди на машинних носіях у результаті впровадження, функціонування та впливу шкідливих програмних засобів, які можна розділити на кілька підгруп:

1) сліди зміни файлової структури, системних областей машинних носіїв інформації та постійної незалежної пам'яті;
2) сліди зміни налаштувань ЕОМ й окремих програм;
3) сліди порушення роботи ЕОМ й окремих програм;
4) сліди впливу на системи захисту й конфіденційність інформації;
5) інші прояви впливу та функціонування шкідливих програмних і технічних засобів, включаючи відеоефекти, повідомлення, що виводяться на пристрій для друку, аудіоефекти.

Тому пошук може завершитися встановленням ЕОМ, які є кінцевими точками маршруту. Усі сліди на точках маршруту фіксуються, за потреби досліджуються та вилучаються фахівцем [51].

3. Заключний етап

Фіксування результатів включає складання протоколу та додатків до нього, тобто (пропоную додати) виготовляються плани і схеми, до яких додаються матеріали фіксації процесу, зняття копій інформації та вилучення предметів, які мають значення для кримінального провадження. Залежно від властивостей шкідливого програмного засобу, можливостей його дослідження на місці чи в експертних установах слідчий за погодженням із спеціалістом може:

– зняти копію інформації, що міститься на ЕОМ, АС, інших електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку; (пропоную записати дії слідчого як перелік)
– вилучити ЕОМ, АС, інші електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, якщо вони безпосередньо зазначені в ухвалі суду на проведення обшуку.;
– вилучити в порядку, визначеному главою 16 КПК України, ЕОМ, АС, інші електронні інформаційні системи або їх частини,

мобільні термінали систем зв'язку, якщо вони безпосередньо не зазначені в ухвалі суду на проведення обшуку. Для цього необхідна нова ухвала слідчого судді, у якій зазначаються електронні інформаційні системи або їх частини, мобільні термінали систем зв'язку, що потребують додаткового вилучення [51].

3.3.3. Залучення експерта

Законодавець висвітлює значення поняття спеціальних знань у ст. 101 КПК України, яка регламентує право кожної сторони кримінального провадження надати суду висновок експерта, що ґрунтується на його наукових, технічних або інших спеціальних знаннях [53, с. 284].

Поняття «спеціальні знання» тлумачать як наукові, технічні або інші з позицій кримінального процесуального закону неюридичні знання, отримані внаслідок спеціальної підготовки та практики суб'єктом, процесуальний статус якого визначається як експерт або прирівнюється до спеціаліста [11, с. 27].

Відповідно до ст. 1 Закону України «Про судову експертизу» судова експертиза – це дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини справи, що перебуває у провадженні органів досудового та судового слідства [54].

Проведення експертизи включає:

1) залучення експерта або спеціаліста:
– *спеціаліста* – у формі консультації і технічної допомоги під час досудового розслідування та судового розгляду;
– *судового експерта* – у формі залучення до проведення судової експертизи;
2) проведення експертних досліджень;
3) подання експертом висновку з питань, які поставлені перед ним сторонами кримінального провадження, слідчим суддею чи судом.

Згідно зі ст. 242 КПК України експертиза проводиться експертом за зверненням сторони кримінального провадження або за дорученням

слідчого судді чи суду, якщо для з'ясування обставин, які мають значення для кримінального провадження, необхідні спеціальні знання. Не допускається проведення експертизи для з'ясування питань права [50].

Чинним КПК України не визначено форму юридичної підстави для проведення експертизи, однак на практиці це – постанова слідчого чи прокурора.

Залежно від наявності підстав слідчий, прокурор, як правило, на свій розсуд, з огляду на конкретні обставини справи й ті питання, на які має відповісти тільки фахівець із певної галузі знань, визначає, чи потрібно в кримінальному провадженні залучати експерта, проводити експертизу та яку саме.

З метою визначення, які об'єкти слід надати експерту в кожному конкретному випадку та як їх відбирати для дослідження, а також переліку питань, які необхідно вирішити, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки.

Завданнями, що вирішуються в межах проведення комп'ютерно-технічної експертизи, є:

- установлення виду (типу, марки), властивостей апаратного засобу, а також його технічних і функціональних характеристик;
- установлення фактичного стану і справності апаратного засобу;
- виявлення і дослідження функціональних властивостей, а також налаштувань програмного забезпечення, часу його інсталяції;
- виявлення потрібної інформації, установлення її властивостей та виду відображення в комп'ютерній системі;
- відновлення видаленої та зашифрованої інформації на різного виду носіях;
- виявлення ознак діяльності шкідливого програмного забезпечення;
- виявлення слідів активності в мережі Інтернет, змісту електронного листування, історії обміну повідомленнями у програмах для спілкування та ін. [54].

Об'єктами комп'ютерно-технічної експертизи є як апаратні засоби (системні блоки комп'ютерів та їх комплектуючі, сервери, ноутбуки, жорсткі диски, флеш-накопичувачі, модеми, маршрутизатори

та ін.), так і програмні продукти (комп'ютерні програми, бази даних тощо).

Слід зауважити, що порядок отримання зразків (об'єктів) експертизи, крім іншого (обшук, огляд), визначено у ст. 245 КПК України, а саме: шляхом постановлення ухвали слідчого судді про тимчасовий доступ до речей і документів.

Для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби – комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій).

Для забезпечення збереження наданих на дослідження носіїв інформації в робочому стані вони запаковуються окремо, зокрема, системні блоки персональних комп'ютерів мають бути запакованими так, щоб унеможливити доступ до носіїв інформації безпосередньо чи через (пропоную додати) підключення системного блока до мережі живлення.

Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій із копією досліджуваного програмного продукту або програмного коду.

Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них.

Орієнтовний перелік вирішуваних питань:

- Чи міститься на цьому носії інформація стосовно [зазначити, яка інформація цікавить] й у якому вигляді?
- Чи містить носій досліджуваного комп'ютера інформацію про певні [зазначити, які саме] дії користувача?
- Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?
- Чи могла бути створена зазначена інформація на цьому комп'ютері, чи вона перенесена з іншого носія?
- У який спосіб інформація [зазначити, яка саме] перенесена до досліджуваного комп'ютера (носія)?
- Яка технологія та хронологія створення електронного документа [зазначити електронний документ та певний зміст]?

- Чи містить накопичувач інформації досліджуваного комп'ютера певне [зазначити, яке саме: встановлене, невстановлене] програмне забезпечення?
- Які функціональні несправності мають комп'ютерне обладнання або його окремі складові та пристрої, як ці несправності впливають на роботу обладнання в цілому?
- Чи можливе виконання певних дій за допомогою цього або досліджуваного програмного продукту?
- Чи можливе вирішення певного завдання за допомогою цього або досліджуваного програмного продукту?
- Чи реалізовані у цьому або досліджуваному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Проведення цієї експертизи складається з таких стадій: попереднє дослідження; експертний експеримент; порівняльне дослідження; оцінка результатів проведеного дослідження та формулювання висновків; оформлення результатів проведеного дослідження [54].

Використання спеціальних знань під час розслідування кіберзлочинів має вагоме значення. Завдяки проведенню комп'ютерно-технічної експертизи маємо змогу вирішити різноманітні завдання, отримати нові фактичні дані, які є важливими доказами для притягнення до відповідальності винних у вчиненні кіберзлочинів. Цей вид експертизи постійно розвивається шляхом створення нових і вдосконалення наявних методик дослідження, використання сучасного обладнання, програмного забезпечення.

3.3.4. Допит свідка, потерпілого, підозрюваного

Допит щодо дослідження доказів на електронних носіях інформації, порівняно з іншими слідчими діями, має значне інформаційне навантаження. Для підтвердження або спростування доказової інформації в електронному вигляді необхідне проведення певного комплексу допитів осіб, визначених відповідно до мети допиту.

Вивчення кримінальних справ дає змогу встановити коло або сформулювати перелік (як варіант, на Ваш розсуд) осіб, що підлягають допиту як свідки:

а) службові особи та працівники установи-жертви, що можуть мати зв'язок з обставинами вчинення злочину;
б) представники та працівники юридичної особи, яка використовувалася під час учинення злочину тим чи іншим способом;
в) спеціалісти, що мають професійний досвід у галузі інформатики та комп'ютерної техніки, програмування, у тому числі особи, які брали участь як спеціалісти під час слідчих (розшукових) дій.

Свідки часто володіють спеціальною, професійною освітою (у сфері КТ, банківського електронного обігу коштів) або в цілому є обізнаними в питаннях використання інформаційних технологій та ІТ-технологіях. У теоретичному аспекті важко визначитися з послідовністю проведення допитів свідків, що пов'язано з конкретними обставини справи, певними результатами ознайомлення слідчого з документами, організацією роботи установи, зокрема розподілом обов'язків та її структурою.

Як доводить слідча практика, сприятиме дотриманню принципу послідовності дослідження доказів на електронних носіях інформації проведення допитів у такому порядку: від допиту осіб, яким відома більш повна інформація про обставини злочину (наприклад, це особи, які виявили злочин або проводили першочергову перевірку засобів комп'ютерної техніки), до тих, хто має орієнтовну інформацію у справі щодо КТ (всі інші).

У ході допитів підозрюваних необхідно встановити:

- наявність змови з іншими особами на вчинення злочину, хто ці особи;
- хто є ініціатором учинення злочину;
- час, місце та інші деталі злочинної домовленості;
- розподіл ролей між учасниками злочину (злочинів);
- конкретні дії з підготовки злочину (попереднє вивчення об'єкта злочинного посягання, підтвердження наявності співучасників, вжиття заходів щодо нелегального отримання логінів, паролів для доступу в мережу, відкриття фіктивного підприємства або рахунків у банках, що нині функціонують,

отримання кредитних / платіжних карток або ідентифікаційних даних про кредитні / платіжні картки для переказу викрадених грошових коштів і т. ін.);
- частку кожного із співучасників, яку він повинен був отримати в результаті вчинення злочину (злочинів) [44].

Під час допиту потерпілої сторони слід урахувати її умовний поділ на три групи: власники комп'ютерної системи; клієнти, що користуються їхніми послугами; інші особи, та обов'язково з'ясувати таке:
- установчі дані, посаду та функціональні обов'язки на робочому місці;
- яка інформація піддавалася неправомірному впливу;
- призначення і зміст інформації, що піддалася неправомірному втручанню;
- як здійснюється доступ до комп'ютерних ресурсів, систем, мереж, кодів, паролів та іншої комп'ютерної інформації;
- як організовано противірусний захист;
- у який спосіб ведеться облік користувачів комп'ютерної системи;
- хто і як виявив шкідливий програмний чи технічний засіб;
- коли та за яких умов це сталося.

У процесі допиту заявника додатково висвітлюються питання щодо:
- документального підтвердження шкоди, завданої несанкціонованим втручанням у роботу ЕОМ, АС або мережі;
- інтернет-провайдера, який забезпечує доступ до мережі Інтернет потерпілої сторони (технічне обслуговування, технічну підтримку сайту тощо), та угоди з провайдером щодо надання їй послуг;
- інтернет-технологій та програмних засобів, що використовуються під час обліку фінансової діяльності (чи є ресурс оригінальною розробкою);
- кола осіб, які мають доступ до паролів адміністративного інтерфейсу та доступ до ЕОМ;
- обсягу конфіденційної інформації, яка міститься у ЕОМ (мережі), можливості доступу до неї;
- останніх відомих випадків протиправного впливу на роботу ЕОМ, АС чи мережі, зміни, знищення або блокування інформації, яка міститься в зазначеній системі;

- того, чи збережені дані про вчинення протиправного впливу (в комп'ютері, сервері мережі тощо);
- того, чи був такий вплив єдиним або має системний характер;
- того, які організаційні, програмні та технічні засоби використовуються для забезпечення безпеки мережі [44].

Під час допиту провайдера або оператора зв'язку необхідно встановити відомості про:
- наявність інформації про здійснення доступу до ЕОМ, АС (мережі) потерпілого;
- IP-адреси користувача мережі Інтернет, з яких здійснювався вплив на роботу програмно-технічних засобів потерпілого, ім'я, яке ним використовувалося під час роботи в мережі;
- дані щодо реєстратора доменного імені правопорушника;
- наявність даних щодо користувача IP-адреси, з якої було здійснено протиправний вплив;
- номер телефону (стаціонарного, мобільного), з якого було здійснено доступ до мережі Інтернет, а також дані про його власника;
- місцезнаходження телефона (у тому числі мобільного);
- внесення будь-яких змін або здійснення несанкціонованих дій з інформацією, що міститься на сервері провайдера;
- системність учинення протиправного впливу з певних IP-адрес мережі;
- попередні спроби протиправного впливу на роботу певної ЕОМ, АС (мережі);
- програмні й технічні засоби, що були використані під час здійснення протиправного впливу [44].

3.3.5. Негласні слідчі (розшукові) дії

Під час підготовки або погодження клопотання про проведення негласної слідчої (розшукової) дії (далі – НСРД) прокурору (процесуальному керівнику) необхідно враховувати, що підставою для проведення конкретної негласної слідчої (розшукової) дії є наявність відомостей, які потребують перевірки, про вчинений злочин та особу, яка його

вчинила, з метою їх підтвердження або спростування, за умови, якщо в інший спосіб, крім проведення негласної слідчої (розшукової) дії, отримати інформацію неможливо.

Здебільшого негласні слідчі (розшукові) дії проводяться стосовно підозрюваних, однак на практиці існують випадки їх проведення щодо осіб, які не мають такого статусу.

Згідно зі ст. 246 КПК України до системи НСРД належить: аудіо-, відеоконтроль особи (ст. 260 КПК України), накладення арешту на кореспонденцію (ст. 261 КПК України), огляд і виїмку кореспонденції (ст. 262 КПК України), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), зняття інформації з електронних інформаційних систем (ст. 264 КПК України), обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України), установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України), спостереження за особою, річчю або місцем (ст. 269 КПК України), моніторинг банківських розрахунків (ст. 269-1 КПК України), аудіо-, відеоконтроль місця (ст. 270 КПК України), контроль за вчиненням злочину (ст. 271 КПК України), виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України), негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК України) [50].

Необхідно зауважити, що НСРД, передбачені ст.ст. 260, 261, 262, 263, 264 (стосовно дій, які потребують ухвали слідчого судді), та ст.ст. 267, 269, 269-1, 270, 271, 272, 274 цього Кодексу, проводяться лише у кримінальному провадженні щодо тяжких або особливо тяжких злочинів, класифікацію яких визначено у ст. 12 КК України. Слід зазначити, що НСРД, такі як зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем чи утримувачем або не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України), та установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) [50], проводяться незалежно від тяжкості злочину (п. 1.14 Інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затвердженої спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України,

Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листопада 2012 року № 114/1042/516/1199/936/1687/5» (далі – Інструкція)).

Також варто зазначити, що у кримінальних провадженнях вказаної категорії виникають проблеми щодо практичного застосування вимог ч. 3 ст. 370 КПК України та *відкриття стороні захисту матеріалів, які стосуються санкціонування проведених НСРД*, за наявності в них інформації з обмеженим доступом та можливості їх розсекречення на стадії судового розгляду.

Зокрема, Вищим спеціалізованим судом України з розгляду цивільних і кримінальних справ по-різному оцінюються результати НСРД як доказів у кримінальному судочинстві. Так, у разі їхнього невідкриття або неповного відкриття стороні захисту та недослідження судом матеріалів, які стосуються їхнього санкціонування (постанови прокурора та ухвали слідчого судді), результати застосування НСРД визнаються недопустимими. В інших випадках суди вважають, що докази, одержані внаслідок застосування НСРД, є допустимими, якщо до справи долучено лише інформацію, яка підтверджує факт винесення ухвали слідчого судді про зняття інформації з транспортних телекомунікаційних систем.

У зв'язку з цим, зважаючи на положення ст. 23 та ч. 3 ст. 370 КПК України, прокурор, який здійснює процесуальне керівництво досудовим розслідуванням, *кожного разу*, коли планує використати як доказ постанови прокурорів та ухвали слідчих суддів, що підтверджують допустимість результатів НСРД, *повинен ужити заходів щодо їх розсекречення.*

Відповідно до п. 5.9 Інструкції рішення про розсекречення постанови прокурора, якою санкціоновано контроль за вчиненням злочину, приймається прокурором, який здійснює процесуальне керівництво досудовим розслідуванням у конкретному кримінальному провадженні, з урахуванням обставин кримінального провадження у разі, якщо витік зазначених відомостей не завдасть шкоди національній безпеці України. Очевидно, що при цьому суд повинен брати до уваги довідку прокурора (суду), яка підтверджує законність санкціонування НСРД.

Згідно зі змістом п. 5.9 Інструкції розсекреченню підлягають не тільки результати НСРД у формі протоколу, а й відомості щодо їхнього

проведення, у тому числі ухвала слідчого судді, постанова прокурора про проведення відповідної НСРД.

Таким чином, відомості про термін дії дозволів на застосування НСРД, вид НСРД, особу (осіб), місце або річ, щодо яких необхідно провести НСРД, після використання їхніх результатів як доказів у кримінальному провадженні не є такими, розголошення яких створює загрозу національним інтересам та безпеці.

Слід зауважити, що *законодавством не врегульовано питання щодо розсекречення ухвал слідчих суддів апеляційних судів про надання дозволів на проведення НСРД*, у зв'язку з чим суди відхиляють відповідні письмові звернення прокурорів. Тому до моменту унормування цього питання в законодавстві, на нашу думку, суди мають брати до уваги довідки прокурора та суду, які підтверджують законність санкціонування НСРД, і за їх наявності відповідні матеріали НСРД повинні визнаватися допустимими доказами.

У разі, якщо в кримінальному провадженні у матеріалах НСРД є відомості, що становлять державну таємницю, і зняття з них грифа секретності неможливе, таке кримінальне провадження, на наш погляд, має здійснюватися в порядку, передбаченому главою 40 «Кримінальне провадження, яке містить відомості, що становлять державну таємницю» КПК України.

Необхідно зазначити, що Інструкцією передбачено можливість розсекречення постанов прокурора та ухвал слідчих суддів, якими санкціоновано здійснення НСРД, *лише на стадії досудового розслідування*.

Розсекречення таких постанов та ухвал на стадії судового розгляду вбачається неможливим, адже, якщо такі постанови та ухвали не відкривалися стороні захисту відповідно до вимог ст. 290 КПК України, вони не можуть досліджуватися в суді. До того ж указаною статтею КПК України встановлено, що прокурор або слідчий за його дорученням зобов'язаний надати доступ до матеріалів досудового розслідування, які є в його розпорядженні, у тому числі будь-які докази, самостійно або в сукупності з іншими доказами можуть бути використані для доведення невинуватості чи меншого ступеня винуватості обвинуваченого, або сприяти пом'якшенню покарання. Із документів, що надаються для ознайомлення, можуть бути вилучені відомості,

які не будуть розголошені під час судового розгляду. Їхнє вилучення повинно бути чітко позначено. За клопотанням сторони кримінального провадження суд має право дозволити доступ до відомостей, які були вилучені [51].

Зважаючи на викладене, якщо сторона обвинувачення не додала до матеріалів кримінального провадження копій ухвал слідчого судді про надання дозволів на застосування НСРД, у тому числі через наявність у них відомостей, що становлять державну таємницю, то це обмежує можливості використання результатів таких НСРД як доказів у кримінальному провадженні (Лист Генеральної прокуратури України від 29 лютого 2016 року № 09/2-117вих-16-92ОКВ).

Варто зауважити, що під час організації проведення негласних слідчих (розшукових) дій необхідно керуватися такими методичними рекомендаціями:

- з питань організації взаємодії прокурора, слідчого та оперативних підрозділів, особливості здійснення процесуального керівництва під час проведення негласних слідчих (розшукових) дій, схвалені науково-методичною радою при Генеральній прокуратурі України 10 квітня 2014 року (протокол № 1);
- щодо організації проведення негласних слідчих (розшукових) дій у провадженнях про кримінальні правопорушення, вчинені організованими злочинними угрупованнями, та використання їх результатів у кримінальному судочинстві, схвалені науково-методичною радою при Генеральній прокуратурі України 24 жовтня 2013 року (протокол № 7);
- «Організаційні та процесуальні аспекти розшуку підозрюваного слідчим та прокурором у кримінальному провадженні», схвалені науково-методичною радою при Національній академії прокуратури України 27 квітня 2016 року (протокол № 4).

Одним із видів такої НСРД, як зняття інформації з електронних інформаційних систем є ***зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту***. Ця дія як компонент тактичної операції «Персоналізація відомостей про особу/осіб злочинця/

ів» реалізується шляхом пошуку слідчим або інспектором кіберполіції (за дорученням слідчого) в різноманітних інтернет-спільнотах відкритої інформації про особу злочинця. Виконавець за результатами дії складає протокол, у якому фіксує: персоналізовані відомості про особу злочинця; ознаку, за якою об'єднують коло осіб, що потрапляють під підозру; інформацію про зв'язки особи, що потрапила під підозру; відомості, що можуть сприяти розв'язанню інших тактичних завдань (пошук свідків, потерпілих, забезпечення встановлення мотивів злочину тощо). До протоколу зняття інформації з електронних інформаційних систем або її частини додають відповідні носії електронної інформації, що містять файли з відеограмою та зображенням екрана монітора (англ. screenshot), створеними під час дослідження системи, а також їх роздруківки як додатків до протоколу [44].

Установлення місцезнаходження радіоелектронного засобу. Така НСРД, відповідно до ст. 268 КПК України, полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного термінала, систем зв'язку та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження. Фактично ж слідчий ініціює її проведення в кримінальних провадженнях різного ступеня тяжкості для визначення параметрів базових станцій операторів телекомунікацій, що забезпечують роботу в певному місці кінцевого обладнання систем зв'язку, і місцезнаходження інших радіовипромінювальних пристроїв, активованих у мережі операторів рухомого (мобільного) зв'язку.

Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача передбачено ст. 264 КПК України НСРД і має на меті одержання інформації, зокрема із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі. Цю НСРД ініціює слідчий виключно в кримінальному провадженні щодо тяжких або особливо тяжких злочинів, її проводять на підставі дозволу слідчого судді на втручання у приватне спілкування.

Проведення цієї дії потребує наявності спеціальних знань у галузі інформаційних технологій [44].

Контроль за вчиненням злочину є засобом криміналістичної тактики, шляхи оптимізації проведення якого доцільно визначати в контексті особливостей тактики його проведення під час розслідування злочинів окремої групи чи виду. Відсутність законодавчих критеріїв розмежування форм цієї НСРД зумовлює часто суб'єктивний характер обрання ініціатором у конкретній ситуації однієї з форм реалізації контролю за вчиненням злочину. Тому процес обрання тієї або іншої форми проведення контролю за вчиненням злочину розглянуто враховуючи тактичну обумовленість конкретної форми цієї НСРД під час розслідування кіберзлочинів. Це дозволило сформулювати певні тактичні рекомендації щодо оптимізації тактики його проведення стосовно обраної категорії злочинів. По-перше, тактичною метою проведення контролю за вчиненням злочину у формі спеціального слідчого експерименту є визначення кінцевого мотиву злочинної діяльності в кіберпросторі; за вчиненням злочину у формі імітування обстановки злочину – установлення замовника кіберзлочину; у формах контрольованої поставки, контрольованої та оперативної закупки – подолання засобів конспірації, які використовують учасники мережевої злочинної групи. У процесі розслідування конкретного кіберзлочину ініціатор, зважаючи на слідчу ситуацію, практичні міркування, формулює переважаючу в організаційно-тактичному плані мету проведення цієї НСРД та обирає конкретну форму проведення контролю за вчиненням злочину. По-друге, безпосереднє проведення цієї НСРД доручають оперативному підрозділу. По-третє, контрольована поставка, контрольована та оперативна закупка як форми НСРД обираються як тактичний засіб під час розслідування тяжких та особливо тяжких кіберзлочинів, зокрема придбання чи збут зброї, бойових припасів або вибухових речовин, незаконне придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів. Тактичні рекомендації, прийоми та методи проведення контрольованої поставки, контрольованої та оперативної закупки зумовлюються особливостями предмета їхнього здійснення.

3.4. ОСОБА ЗЛОЧИНЦЯ

Аналізуючи вивчення криміналістичної характеристики особи злочинця в контексті розслідування кіберзлочинів, наведемо приклади деяких класифікацій особи злочинця. О. А. Самойленко пропонує такі типи особи злочинця, що вчиняє злочин з використанням обстановки кіберпростору:

1) злочинець – користувач початкового рівня;
2) злочинець – користувач;
3) злочинець – впевнений користувач;
4) злочинець – досвідчений користувач;
5) злочинець – користувач професіонал [55, с. 200].

О. В. Курман виділяє декілька груп осіб, які здійснюють несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку:

1) працівники підприємств, установ, організацій-конкурентів;
2) працівники, які вчиняють незаконні дії з інформацією на замовлення, перебуваючи з її власником (уповноваженим органом) у трудових відносинах;
3) працівники, які збирають інформацію для себе (про всяк випадок);
4) особи, професійна або службова діяльність яких чи інші законні підстави обумовлюють виникнення певних правовідносин цивільно-правового характеру з власником інформації;
5) особи, які не перебувають у жодних цивільно-правових чи трудових відносинах з власником, але вчиняють незаконні дії через «спортивний інтерес», бажання заявити про себе, прорекламувати свої можливості та вміння, на замовлення сторонніх осіб (для передачі конкурентам чи вчинення шантажу) [56, с. 130].

Така класифікація особи злочинця може мати місце у процесі розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, де іншими елементами криміналістичної характеристики зазначеного злочину є: виток, утрата, підробка,

блокування інформації, спотворення процесу обробки інформації та порушення встановленого порядку маршрутизації інформації, а також обстановка, сліди, способи вчинення злочину та його приховування.

Вивчаючи обстановку скоєння злочину, треба обов'язково звернути увагу на наявність і спосіб підключення електронно-обчислювальної техніки (ЕОТ), у роботу якої було здійснено несанкціоноване втручання до комп'ютерних мереж і мереж електрозв'язку. Відразу ж можна виокремити три основні ситуації:

- ЕОТ не підключено до будь-яких мереж;
- ЕОТ підключено до локальної мережі [57, с. 215];
- ЕОТ підключено до глобальної мережі Інтернет. Беручи до уваги ці відомості, можна в деяких випадках значно (як варіант) звузити коло можливих підозрюваних і визначити типи осіб злочинців за способом здійснення несанкціонованого втручання:.

1. Злочинець мав безпосередній (фізичний) доступ до ЕОТ. Тоді доцільно було б з'ясувати коло осіб, які могли мати доступ до ЕОТ з урахуванням установлених часу та місця скоєння злочину (прикладом може бути ситуація, коли співробітник підприємства, якого, на його думку, незаслужено звільняють, пропоную пояснити що таке «дата-центр» та записати так: втручається в роботу центра збереження та обробки даних і, з помсти, використовуючи шкідливе програмне забезпечення, маючи безпосередній доступ до ЕОТ, знищує всю інформацію на серверах компанії).

2. Злочинець мав доступ до ЕОТ у локальній мережі та за допомогою цієї мережі здійснив несанкціоноване втручання в роботу ЕОТ, що міститься в тій же локальній мережі. У цьому разі є можливість з'ясувати в адміністратора локальної мережі обмежений список точок підключення ЕОТ, які які належать до мережі, а також фізичні (реальні) IP-адреси точок підключення до мережі. Використовуючи таку інформацію, можна встановити обмежене коло осіб, які працюють у локальній мережі наприклад, комірник на підприємстві, на якому комп'ютери об'єднані в закриту локальну мережу, для приховування нестачі товару підключається за допомогою одного з комп'ютерів у цій мережі до сервера із системою обліку товарообігу, за допомогою шкідливого програмного забезпечення зламує її захист і змінює дані про кількість товару на складі).

3. Злочинець здійснив несанкціонований доступ та втручання в роботу ЕОТ, що підключена до глобальної мережі Інтернет, за допомогою невстановленої ЕОТ, яка також підключена до глобальної мережі Інтернет. Така ситуація є найскладнішою для вирішення, оскільки теоретично несанкціонований доступ та втручання в роботу ЕОТ мало змогу здійснити необмежене коло осіб по всьому світу за наявності можливості підключення до глобальної мережі Інтернет як приклад, хакер розіслав електронною поштою шкідливе програмне забезпечення, за допомогою якого здійснив шифрування даних на жорстких дисках комп'ютерів підприємства, що призвело до блокування інформації, і тепер він вимагає гроші за відновлення можливості доступу до цієї інформації) [57, с. 215].

Якщо виникла така ситуація, треба розглянути особу злочинця, беручи до уваги слідову картину та спосіб учинення злочину. Потрібно з'ясувати, чи використовував злочинець шкідливе програмне забезпечення, бекдори (з англ. backdoor – «чорний хід», тобто дефекти в коді програмного забезпечення) або ж несанкціоноване втручання здійснили потерпілі чи користувачі ЕОТ через недотримання елементарних правил забезпечення кібербезпеки.

Отже, проаналізувавши отриману на початковому етапі розслідування інформацію, можна буде виокремити кілька типів особи злочинця, використовуючи знання у сфері комп'ютерних наук.

1. Злочинці, які мають базові навички у сфері комп'ютерних наук, використовують готове шкідливе програмне забезпечення, інструкції, уроки для вивчення техніки зламу мережі, що є в загальному доступі. У разі отримання від спеціаліста або експерта інформації про те, що було застосовано шкідливе програмне забезпечення, завдяки додатковим консультаціям з фахівцями та за допомогою особистого пошуку можна дізнатися яке шкідливе програмне забезпечення використовувалося для несанкціонованого втручання та маніпуляцій з інформацією. Такі відомості (щоб уникнути повтору) можуть стати корисними для доказування, якщо під час обшуків у осіб, які можуть бути причетні до скоєння злочину, у процесі огляду їхніх комп'ютерів буде встановлено, що вони послуговувалися інтернет-ресурсами, на яких можна завантажити це програмне забезпечення.

2. Злочинці, які мають навички у сфері комп'ютерних наук, що не володіють певним досвідом програмування, але здатні адаптувати готові програмні рішення відповідно до своїх потреб, уміють знаходити нові або використовувати відомі вразливості у програмному забезпеченні (наприклад, злочинець може використовувати готові програмні рішення для здійснення несанкціонованого доступу до ЕОТ на базі Kali Linux – дистрибутива на базі операційної системи Linux для проведення тестування на проникнення й аудиту безпеки). У цьому разі під час порівняння результатів комп'ютерно-технічної експертизи або інформації від фахівця про спосіб несанкціонованого втручання з можливостями, що надає зазначений дистрибутив, можна скласти уявлення про досвід злочинця, а також отримати відомості про те, на що треба звернути увагу під час проведення обшуків.

3. Злочинці, які мають фундаментальні знання у сфері комп'ютерних наук, зокрема й програмування, самостійно розробляють шкідливе програмне забезпечення й знаходять нові, складні в реалізації способи для здійснення несанкціонованого втручання в роботу ЕОТ. Наприклад, коли експерт не взмозі ідентифікувати шкідливе програмне забезпечення, що використовувалося під час несанкціонованого доступу до ЕОТ, а антивірусні бази ще не містять його сигнатури (від англ. signature – «підпис»; мається на увазі цифровий підпис, за допомогою якого антивірусне програмне забезпечення визначає шкідливе програмне забезпечення) або ці сигнатури були додані нещодавно й шкідливого програмного забезпечення немає в загальному доступі [57, с. 217].

Розкриття злочинів, учинених останнім типом злочинців, представляє особливу складність, оскільки вони знають, що роблять, роблять це добре й уміло приховують сліди.

3.5. СЛІДОВА КАРТИНА

У кримінальному праві обстановку розглядають як елемент кримінально-правової характеристики злочинів; у кримінології – з точки зору запобігання злочинності; у кримінальному процесуальному праві з точки зору доказування. У криміналістичній науці обстановку

визначають як складову криміналістичної характеристики, що вивчає середовище, у якому вчинюється злочин. Розслідування злочину органом досудового розслідування переважно розпочинається зі сприйняття і дослідження обстановки, у якій воно було вчинено. З'ясування обстановки вчинення злочину допомагає сформулювати слідчому уявлення про механізм здійснення злочину, імовірні місця пошуку слідів злочину, суб'єкта (суб'єктів) вчинення злочину, мотив та мету, а також деякі аспекти способу його вчинення [57, с. 360].

Зауважимо, що в юридичній літературі та в законодавчих актах не має точного визначення поняття «обстановка кіберзлочину». Однак, аналізуючи наукові праці українських вчених, ми можемо зазначити, що головна ознака обстановки вчинення кіберзлочину це те, що злочин здійснюються в віртуальному просторі, інакше кажучи у кіберпросторі [58, с. 83].

Ураховувати таку ознаку є цілком доречним, однак не слід забувати і про інші ознаки матеріального (реального) середовища, які є вагомими для розслідування та розкриття цих злочинів.

Зважаючи на особливості кіберзлочинів, на наш погляд, в обстановці кіберзлочину слід виокремлювати (як варіант, на Ваш розсуд):

1) кіберпростір – середовище, у якому здійснюється електронний процес до, у момент та після вчинення злочину, що характеризується місцем, часом, віртуальною взаємодією учасників злочину;
2) матеріальний (фізичний) простір – систему умов та обставин, що взаємодіють між собою до, у момент та після вчинення злочину об'єктів, процесів, що характеризують місце, час та реальну взаємодію учасників злочину, а також інші обставини скоєння кіберзлочину (соціально-психологічні, економічні, безпекові, політичні тощо) [57, с. 360].

Під час розслідування кіберзлочинів велике значення має інформація про ймовірне місце та час його вчинення. Для слідчого є важливим встановлення місця скоєння такого злочину. Насамперед, установлення місця вчинення злочину допомагає з'ясувати місцезнаходження можливих доказів та коло осіб, причетних до вчинення злочину. Час учинення кіберзлочину дає змогу встановити в якій саме послідовності здійснювалися злочинні дії та їхня тривалість.

Досліджуючи місце вчинення злочину, необхідно звернути увагу на те, що воно обирається суб'єктами злочину не випадково. Повністю оцінивши заздалегідь імовірне місце злочину, суб'єкт фактично використовує його як засіб реалізації свого злочинного наміру.

Місце вчинення злочину розглядається як визначена географічна точка (територія, приміщення тощо), яке тісно пов'язане з іншими елементами обстановки злочину [59, с. 744].

Аналізуючи час учинення злочину, доречно зауважити, що час не обмежується астрономічними властивостями (рік, місяць, дата, години, хвилини, секунди). Це може бути час, пов'язаний з сезонністю, з настанням темноти чи світлого часу доби, часом відпочинку та часом відсутності потерпілих у місцях проживання, годиною «пік», час, який пов'язаний з певною періодичністю тощо [59, с. 743–744].

Ураховуючи специфіку кіберзлочинів, можна виокремити місця їхнього вчинення: фізичне середовище (ділянки місцевості) та електронне середовище (вузли мережі), у яких розташовані:

- програмно-технічні засоби (носії інформації), що зазнали злочинного впливу, та точки їхнього доступу до певних мереж;
- програмно-технічні засоби, які злочинець використовував опосередковано, та точки їхнього доступу до певних мереж;
- мережеві вузли каналів зв'язку, з використанням яких відбувався обмін інформацією між програмно-технічними засобами злочинця та потерпілого [60, с. 72–73].

Щодо вибору фізичного середовища злочинцем, варто звернути увагу на думку О. І. Мотляха, що злочинці переважно обирають такі місця:

- адміністративні та службові приміщення різного типу суб'єктів господарювання (підприємств, організацій, компаній, фірм тощо), які використовують у своїй виробничій діяльності електронні пристрої;
- власні та орендовані житлові приміщення (офіси, квартири, кімнати та інше), у яких установлені електронні пристрої, що забезпечені виходом до всесвітньої мережевої системи Інтернет;
- приміщення комунальної власності або ж споріднені з ними (цокольні, напівпідвальні чи ті, що примикають до житлових

будинків, приміщення), котрі на правах власності чи оренди можуть використовуватися як комп'ютерні клуби, інтернет-кафе тощо [61, с. 64].

Враховуючи, що електронне середовище також є місцем вчинення кіберзлочину, це може бути:

- робоче місце, робоча станція – місце обробки інформації, яка стала предметом злочинного посягання;
- місце постійного зберігання або резервування інформації – сервер або стример (пристрій запису та зберігання даних на магнітній стрічці);
- місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що знаходиться в іншій точці, при цьому місце використання може збігатися з робочим, але перебувати поза організацією (наприклад у разі злому шляхом зовнішнього віддаленого мережевого доступу);
- місце підготовки злочину (розробка вірусів, програм злому, підбору паролів) чи місце безпосереднього використання інформації (копіювання, поширення, спотворення), отриманої в результаті неправомірного доступу до даних, що містяться на пристрої [62, с. 205].

Необхідно зазначити, що суттєвою особливістю кіберзлочинів є те, що для них відсутнє просторове обмеження і вчинення злочину може відбуватися за межами однієї держави. Злочин учиняється в одній державі, а негативні наслідки настають в іншій. Такі злочини набувають транснаціонального характеру. Тобто, для них є властивим наявність іноземного елемента в криміналістичній характеристиці та в кримінально-процесуальних відносинах під час його розслідування [63, с. 873–874].

Встановлення часу вчинення кіберзлочинів не є суттєвою проблемою, оскільки операційна система електронного пристрою детально стежить практично за кожною важливою операцією, інформація про які відображається у статистичних файлах. За допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дасть змогу за відповідною командою відобразити на дисплеї інформацію про день, години, хвилини та секунди виконання тієї або іншої операції [63, с. 101].

Не можна не звертати увагу на випадки, коли час учинення злочину встановити неможливо. Це може бути зумовлено технічними причинами, зокрема під час перезавантаження електронного пристрою повністю або частково обнуляються чи стираються дані тощо. Тому за таких умов час учинення необхідно встановлювати шляхом проведення судової комп'ютерно-технічної експертизи. Крім того, час учинення кіберзлочину можна встановити за допомогою (пропоную додати) проведення слідчих (розшукових) дій.

Також слід звертати увагу чи час виставлений на електронному пристрою співпадає з поточним і чи не корегувався він. Варто зауважити, що віртуальну взаємодію учасників кіберзлочину треба розуміти як спільні дії цих учасників у кіберпросторі. Наприклад, особи домовилися вчинити DoS-атаку у відповідний день та час, використовуючи при цьому допоміжні програми, у яких узгоджують свої дії (Telegram, Viber, Discord тощо) [57, с. 362].

Реальна взаємодія учасників кіберзлочину – це їхній контакт у фізичному середовищі. Безумовно, елементи обстановки залишають різні сліди злочинної діяльності, які можуть бути виявлені під час криміналістичного аналізу злочину у процесі його розслідування [63, с. 68].

Сліди злочину – це результат взаємодії об'єктів живої і неживої природи, що опинилися у сфері злочинної діяльності [64, с. 89].

Прикладом електронних слідів можна вважати:

1) інформацію, яка є в журналах операційних систем та окремих програмних продуктів;
2) дані електронного листування, за допомогою яких можна встановити дату та час, адресу відправника тощо;
3) дії на різних сайтах (Facebook, Twitter тощо), які залишають електронні сліди у вигляді повідомлень, пошукових запитів, фотознімків тощо [65, с. 171].

Отже, «слідова картина» кіберзлочину становить сукупність матеріальних, ідеальних та електронних слідів кіберзлочину, які дають змогу слідчому встановити картину цього злочину. До того ж обстановка та «слідова картина» як криміналістичні елементи кіберзлочину взаємопов'язані між собою та мають певну специфіку, опанування якими має важливе як теоретичне, так і практичне значення для ефективного розслідування та розкриття злочинів цієї категорії.

3.6. ТИПОВІ СЛІДЧІ СИТУАЦІЇ ТА ЗАВДАННЯ ПОЧАТКОВОГО І НАСТУПНОГО ЕТАПІВ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Проблематика оцінювання прокурором правильності кваліфікації дій підозрюваної особи під час вчинення кіберзлочину та достатності доказів для складання обґрунтованого повідомлення про підозру призводить до розширення переліку основних завдань початкового етапу розслідування кіберзлочинів. Тому початковому етапу надається особливе значення в методиці розслідування таких злочинів [11].

Основні завдання початкового етапу розслідування кіберзлочинів:

1) установлення відсутності / наявності події кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);
2) з'ясування складу визначеного кримінального правопорушення (час, місце, спосіб, мета / мотив, повторність, учинення групою осіб / організованою групою, наслідки й інші обставини вчинення кримінального правопорушення);
3) установлення фактичних даних, які вказують на конкретну особу, що могла вчинити кримінальне правопорушення (форма вини, мотив і мета вчинення кримінального правопорушення особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру);
4) забезпечення здійснення кримінального провадження;
5) установлення злочинної діяльності в повному обсязі;
6) визначення характеру та тяжкості обвинувачення щодо кожного суб'єкта злочину.

Чинниками типізації слідчих ситуацій початкового етапу розслідування є: 1) характер (обсяг) інформації про особу злочинця; 2) форма початку кримінального провадження. Останній відображає специфіку типових слідчих ситуацій класифікаційних груп / підгруп злочинів, учинених у кіберпросторі. Існує певна система слідчих ситуацій.

1. Ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як ймовірного злочинця (розгорнуті анкетні дані особи).

2. Ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача як ймовірного злочинця.

3. Ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця. У межах кожної з груп таких слідчих ситуацій схарактеризовано три різновиди: 1) ситуація, коли кримінальне провадження розпочато на підставі отримання заяви / повідомлення особи про кримінальне правопорушення; 2) ситуація, за якої кримінальне провадження розпочато внаслідок перевірки оперативної інформації; 3) ситуація, коли кримінальне провадження розпочато в межах реалізації матеріалів оперативно-розшукової справи. Розгляд ситуацій у комплексі з основними тактичними завданнями та комплексом слідчих (розшукових) дій та інших заходів пізнання визначає специфіку розслідування класифікаційних груп / підгруп злочинів, учинених у кіберпросторі.

Основними завданнями наступного етапу розслідування кіберзлочинів є: установлення характеристик особи / осіб, яких обвинувачують, зокрема, ступеня та характеру сприяння підозрюваного / обвинуваченого у проведенні кримінального провадження щодо нього або інших осіб; визначення інших обставин, які враховує прокурор під час вирішення питання щодо укладення угоди про визнання винуватості (суспільного інтересу в запобіганні, виявленні чи припиненні більшої кількості кримінальних правопорушень або інших більш тяжких кримінальних правопорушень, у забезпеченні швидшого досудового розслідування, викритті більшої кількості кримінальних правопорушень) [11].

Ситуації наступного етапу розслідування злочинів, учинених у кіберпросторі, можна розглядати лише як орієнтири для слідчого, адже слідчу ситуацію в конкретному кримінальному провадженні зумовлює зміст обставин, викладених в акті повідомлення конкретній особі про підозру.

Типові ситуації наступного етап розслідування кіберзлочинів:

1) сприятлива ситуація наступного етапу розслідування (притаманна повнота виконання тактичних завдань початкового етапу розслідування та конкретизація зайнятих кожним із підозрюваних у кримінальному провадженні позицій);
2) несприятлива ситуація розслідування.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Підставою для порушення кримінальної справи про скоєний злочин, у тому числі й комп'ютерний, є достатні дані, що вказують на наявність ознак складу злочину. Зважаючи на зміст кримінально-правової характеристики, комп'ютер та його програмне забезпечення може бути як предметом злочину, так і засобом, за допомогою якого реалізується задум злочинця.

2. Криміналістична характеристика злочинів у сфері комп'ютерних технологій є узагальненою інформаційною моделлю, що являє собою систематизований опис типових криміналістично значущих ознак, які мають суттєве значення для виявлення та розслідування комп'ютерних злочинів.

Елементами криміналістичної характеристики злочинів є:

1) ознаки злочину;
2) надійність засобів захисту комп'ютерної інформації;
3) спосіб (копіювання, модифікація, знищення інформації, внесення шкідливих програм), час та місце (у межах організації або ззовні) здійснення неправомірного доступу і його ознаки;
4) засоби вчинення злочину (технічні, програмні носії інформації);
5) способи подолання захисту (підбір ключів і паролів, викрадення паролів, відключення засобів захисту тощо);
6) особи, які вчинили злочин;
7) винність і мотив правопорушників;
8) обставини, що впливають на ступінь тяжкості злочину, а також обставини, що характеризують особу підозрюваного, пом'якшують та обтяжують покарання;
8) характер та розмір шкоди, завданої злочином.

Способи скоєння злочинів:

1) способи безпосереднього доступу до комп'ютерної інформації або операційної системи;
2) способи виддаленого (опосередкованого) доступу;
3) способи виготовлення та розповсюдження на технічних носіях шкідливих програм для ЕОМ.

Слідова картина кіберзлочину становить сукупність матеріальних, ідеальних та електронних слідів кіберзлочину, які дають змогу слідчому встановити картину цього злочину:

1) слідова картина незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж;
2) слідова картина викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем;
3) слідова картина порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

Особа злочинця. Вік осіб, що вчиняють комп'ютерні злочини, становить від 15 до 45 років. За матеріалами експертних досліджень слід зауважити, що на момент учинення протиправних дій вік злочинців не перевищував 20 років.

Обстановка скоєння злочину. Особливістю комп'ютерних злочинів є те, що місце, звідки було скоєно протиправну дію (місце, де виконувалися дії об'єктивної сторони складу злочину), та місце настання шкідливих наслідків (місце, де наступив результат злочину) можуть не співпадати. Таким місцем може бути будь-яке приміщення різної форми власності, у якому знаходиться комп'ютерно-технічне оснащення, забезпечене виходом до глобальної мережі Інтернет. Час учинення протиправних дій з комп'ютерними технологіями завжди конкретно визначений.

ВИСНОВКИ

На основі результатів проведеного нами дослідження можна сформулювати певні висновки, рекомендації та пропозиції, що сприятимуть удосконаленню практичної діяльності щодо виявлення і розслідування злочинів, пов'язаних із використанням інформаційних комп'ютерних технологій.

1. Злочини у сфері комп'ютерних технологій є одним із складних явищ у суспільстві. Ефективне розслідування злочинів, зокрема протиправних дій, пов'язаних із використанням комп'ютерних технологій – одне з ключових питань для будь-якої держави, у тому числі й для України. Міжнародний характер протидії цьому феномену сучасності – запорука подальшої стабільності та розвитку всіх сфер людського буття.

2. За результатами проведеного аналізу теоретичні та практичні дослідження стосовно визначення поняття кіберзлочину, можна зробити висновок, що серед сучасних українських науковців немає єдиної позиції щодо визначення поняття кіберзлочину. До того ж наявні наукові бачення суттєво відрізняються, відсутність єдності та визначеності може призвести до неправильного трактування і, як наслідок, неправильної кваліфікації злочинних дій, а це, у свою чергу, створить проблеми не тільки на теоретичному, а й на практичному рівні.

3. Під час аналізу національної нормативно-правової бази щодо протидії кіберзлочинам установлено, що на сьогодні законодавцем приділено значну увагу питанню кібербезпеки в нашому суспільстві. Законодавцем напрацьовано певну нормативно-правову базу кібернетичної безпеки України, яку становлять Конституція України, Закони України «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згоду на обов'язковість яких надано Верховною Радою України.

Однак, попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення. У Законі України про кримінальну відповідальність немає усіх тих

необхідних термінів, що повністю пояснюють суть поняття «кіберзлочинність». Загалом Кримінальний кодекс України не містить понять із префіксом кібер-, є лише узагальнене визначення злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку. Уважаємо за доцільне акцентувати увагу й на тому, що Кримінальний кодекс України повинен бути оновлений сучасними термінами, які б розкривали суть кіберзлочинів, зокрема, у розділі, що передбачає відповідальність за них.

4. Відкриті можливості людей використовувати кіберпростір обумовлюють виникнення нових загроз. Кіберзлочини мають велику кількість різноманітних видів та форм, які постійно трансформуються, удосконалюються та створюють нові загрози для інтересів особи й суспільства в цілому.

5. Ознаками злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, як правило, є: суспільна небезпечність, протиправність, винність та караність. Наявність зазначених характеристик є необхідною умовою для визнання скоєного злочину. У свою чергу, елементами складу злочину є: об'єкт, об'єктивна сторона, суб'єкт та суб'єктивна сторона. Ці елементи і є категоріями кримінального права, перелік яких за кримінальним законодавством є вичерпним. Характер й обсяг відповідальності за злочин визначається окремо і є наслідком наявних обставин у справі.

6. У багатьох співробітників правоохоронних органів через незрозумілі причини виникла хибна думка про діяльність державних реєстраторів та переважно нотаріусів, які начебто повинні перевіряти тільки наявність документів та присутність сторін. Це абсолютно неправильна позиція, яка спростовується Законом України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» та іншими нормативно-правовими актами, що регулюють учинення реєстраційних дій.

7. Підставою для порушення кримінальної справи про скоєний злочин, у тому числі й комп'ютерний, є достатні дані, що вказують на наявність ознак складу злочину. Зважаючи на зміст кримінально-правової характеристики, комп'ютер та його програмне забезпечення може бути як предметом злочину, так і засобом, за допомогою якого реалізується задум злочинця.

8. Криміналістична характеристика злочинів у сфері комп'ютерних технологій є узагальненою інформаційною моделлю, що становить систематизований опис типових криміналістично значущих ознак, які мають суттєве значення для виявлення та розслідування комп'ютерних злочинів.

Елементи криміналістичної характеристики злочинів:

1) ознаки злочину;
2) надійність засобів захисту комп'ютерної інформації;
3) спосіб (копіювання, модифікація, знищення інформації, внесення шкідливих програм), час та місце (у самій організації або ззовні) здійснення неправомірного доступу та його ознаки;
4) засоби вчинення злочину (технічні, програмні носії інформації); способи подолання захисту (підбір ключів і паролів, викрадення паролів, відключення засобів захисту тощо);
5) особи, які вчинили злочин;
6) винність і мотив правопорушників;
7) обставини, що впливають на ступінь тяжкості злочину, а також обставини, що характеризують особу підозрюваного, пом'якшують та обтяжують покарання;
8) характер та розмір шкоди, завданої злочином.

Способи скоєння злочинів:

1) способи безпосереднього доступу до комп'ютерної інформації або операційної системи;
2) способи віддаленого (опосередкованого) доступу;
3) способи виготовлення, розповсюдження на технічних носіях шкідливих програм для ЕОМ.

Слідова картина кіберзлочину становить сукупність матеріальних, ідеальних та електронних слідів кіберзлочину, які допомагають слідчому встановити картину цього злочину:

1) слідова картина незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж;
2) слідова картина викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем;

3) слідова картина порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

Особа злочинця. Вік осіб, що вчиняють комп'ютерні злочини, сягає від 15 до 45 років. За матеріалами експертних досліджень визначено, що на момент учинення протиправних дій вік злочинців не перевищував 20 років.

Обстановка скоєння злочину. Особливістю комп'ютерних злочинів є те, що місце, звідки було скоєно протиправну дію (місце, де виконувалися дії об'єктивної сторони складу злочину), та місце настання шкідливих наслідків (місце, де настав результат злочину) можуть бути абсолютно різними. Місцем скоєння злочину може бути будь-яке приміщення різної форми власності, у якому знаходиться комп'ютерно-технічне оснащення, забезпечене підключенням до мережі Інтернет. Час учинення протиправних дій із комп'ютерними технологіями завжди конкретно визначений.

9. Розслідування комп'ютерних злочинів включає такі етапи: підготовчий (до виїзду на місцевість), робочий (дослідний) та заключний (фіксація результатів) етапи. Кожен з етапів має свою особливість:

1) *підготовчий етап* має складатися з двох стадій: до виїзду на слідчий огляд та дії на місці події до початку робочого етапу. Особливу роль на цьому етапі має оперативно-розшукова діяльність правоохоронних органів та, зокрема, формування складу робочої групи, яка виїжджатиме на слідчу дію;
2) *робочий етап* повинен передбачати загальний огляд (він є статичним) та детальну (динамічну) дію. Важливою на цьому етапі є робота спеціалістів з електронними документами, які можуть зберігати доказову інформацію про скоєний злочин;
3) на *заключному етапі* проведення слідчої дії має відбуватися не лише грамотне оформлення відповідних процесуальних документів, а й правильне вилучення виявлених речей і предметів доказового значення та належне поводження з електронними носіями інформації.

10. Для ефективного проведення процесуальних слідчих заходів слідчо-оперативна група повинна мати необхідне технічне оснащення. На нашу думку, доцільно до традиційних криміналістичних валіз додати

ще й спеціалізоване науково-технічне спорядження для виявлення, фіксації та відбору інформаційних слідів на місці скоєння злочину.

11. Логічне завершення розслідування злочину у сфері інформаційних комп'ютерних технологій залежить від своєчасного і грамотного проведення необхідних експертиз. Окрім традиційних експертиз документів (дактилоскопічної, трасологічної, фоноскопічної, фінансово-економічної, техніко-криміналістичної тощо), важливе значення має й судова комп'ютерно-технічна експертиза, різновид класу інженерно-технічних експертиз. Основним завданням цього виду експертиз є вирішення діагностичних та ідентифікаційних питань. Вони сприяють вирішенню таких розшукових завдань, як установлення факту знаходження необхідної інформації на технічних носіях, які представлені на експертизу; отримання розшукової інформації про професійні якості злочинця.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дзяна Г. О, Дзяний Н. Р. Реалізація національної політики у сфері кібербезпеки. *Ефективність державного управління*. 2016. Вип. 3 (48). С. 123–130. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=efdu_2016_3_14 (дата звернення: 14.07.2021).

2. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ»*. 2016. URL: http://visnyk-psp.kpi.ua/article/view/140496/137578 (дата звернення: 14.07.2021).

3. Gibson W. Neuromancer. London : HarperCollins, 1994.

4. David K. Djavaherian. Reno v. ACLU. Berkeley Technology Law Journal. 1998. Vol. 13, № 1. Pp. 371–378.

5. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству от 15.10.2003 г. *Организация Объединенных Наций* URL: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml (дата звернення: 20.07.2021).

6. Чубенко А. Г., Лошицький М. В., Павлов Д. М., Бичкова С. С., Юнін О. С. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції. Київ : Ваіте, 2018. С. 332.

7. Кіберпростір. *Wikideck*. URL: https://wp-uk.wikideck.com/Кіберпростір (дата звернення: 20.07.2021).

8. Манжай О. В. Використання кіберпростору в оперативно розшуковій діяльності. *Право і безпека.* 2009. № 4. С. 142–149.

9. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник*. 2018. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/muvnudp_2018_1-2_46.pdf (дата звернення: 14.07.2021).

10. Про основні засади забезпечення кібербезпеки України : проєкт Закону України від 05.10.2017 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.07.2021).

11. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса. 2020. 112 с.

12. Ричка Д. О. Історичні аспекти кіберзлочинності. *Сучасний стан і перспективи розвитку держави і права* : матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених, м. Дніпропетровськ, 4–5 груд. 2015 р. Дніпропетровськ : Дніпропетровський національний університет імені Олеся Гончара, 2015. С. 293–295.

13. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем

та комп'ютерних мереж і мереж електрозв'язку. Університет державної фіскальної служби України. Ірпень, 2019. 212 с.

14. Діордіца І. В. Поняття та зміст кіберзлочинності. 2017. URL: https://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/ (дата звернення: 10.08.2021).

15. Притула В. О. Поняття кіберзлочинності. *Українське Право та ГО «Європейська Асоціація Студентів Права Львів».* 2017. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_prytula_cybercrime/ (дата звернення: 03.08.2021).

16. Конвенція про кіберзлочинність : Міжнародний документ від 23.11.2001 р. № 65. *Рада Європи*. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 14.07.2021).

17. Русецький А. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78.

18. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. № 3. С. 129–136.

19. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини : навч. посіб. Харків : Право, 2014. 513 с.

20. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. … канд. юрид. Наук : 12.00.08. Харків, 2016. 16 с.

21. Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. Кропивницький : КНТУ, 2016. С. 33–34.

22. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. Київ. : «Аванпост-Прим», 2012. 214 с.

23. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-chinnoi-vitchiznyanoi-normativno-pravovoi-bazi-u-sferi (дата звернення: 14.07.2021).

24. Стратегія забезпечення кібернетичної безпеки України (2021–2025 роки) : Проєкт URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 14.07.2021).

25. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. № 994_687. *Офіційний вісник України*. 2010 .

26. Computer Misuse Act. 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents/enacted (дата звернення: 14.07.2021).

27. Шості харківські кримінально-правові читання «Україна на кримінально-правовій карті світу» : тези доп. та наук. повідомл. учасників міжнар. наук. конф. студентів та аспірантів. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2017. 166 с.

28. Уголовный кодекс Грузии. *Парламент Грузии*. 1999. URL: https://matsne.gov.ge/ru/document/view/16426?publication=229 (дата звернення: 14.07.2021).

29. Кримінальний кодекс України. *Відомості Верховної Ради України*. 2001. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.07.2021).

30. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 20.07.2021).

31. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. URL:https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 20.07.2021).

32. Про Національну програму інформатизації : Закон України від 04.02.1998 р. № 74/98-ВР. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (дата звернення: 20.08.2021).

33. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 03.08.2021).

34. Про телекомунікації : Закон України від 18.11.2003 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (дата звернення: 14.07.2021).

35. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 14.07.2021).

36. Про захист персональних даних : Закон України від 01.06.2010 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.08.2021).

37. Про електронні довірчі послуги : Закон України від 05.10.2017 р. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 15.08.2021).

38. Форос Г. В. Правове регулювання протидії кіберзлочинам. *Правова держава*. 2016. № 24. С. 164–169. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Prav_2016_24_29.pdf (дата звернення: 15.08.2021).

39. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні : Указ Президента України від 31.07.2000 р. № 928/2000 База даних «Законодавство України». *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text (дата звернення: 03.08.2021).

40. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 р. № 96/2016. Відомості Верховної Ради України. URL:http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 20.07.2021).

41. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII (дата оновлення: 12.12.2020). Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 14.07.2021).

42. Методичні рекомендації щодо виявлення злочинів вчинених державними реєстраторами та нотаріусами під час виконання реєстраційних дій в державних реєстрах у розрізі ст.ст. 361, 362 КК України. Департамент кіберполіції. Київ. 2020. 16 с.

43. Вакуленко О. Ф. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів : методичні рекомендації. Київ., 2016. 55 с.

44. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Одеський державний університет внутрішніх справ. 2017. 26 с.

45. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. 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 : вирок № 520/15032/15-к. від 22.09.2020 р. Малиновський районний суд м. Одеси. URL: https://reyestr.court.gov.ua/Review/89689424(дата звернення: 30.07.2021).

46. Кримінальні справи (до 01.01.2019); Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку : вирок № 344/9746/17 від 23.09.2017 р. Івано-Франківський міський суд Івано-Франківської області. URL: https://reyestr.court.gov.ua/Review/68468677 (дата звернення: 20.07.2021).

47. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/ (дата звернення: 20.08.2021).

48. Міністерство Юстиції. URL: https://minjust.gov.ua/ (дата звернення: 20.08.2021).

49. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № № 4651-VI. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.08.2021).

50. Амелін О. В. Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Київ, 2017. 66 с.

51. Курман О. В. Тактичні та організаційні особливості початку досудового розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. №4. 2019. С. 303–308.

52. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса : ТЕС, 2020. 372 с.

53. Про судову експертизу : Закон України від 25 лютого 1994 року № 4038-XII (дата оновлення: 03.07.2020). URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 11.08.2021).

54. Самойленко О. А. Типизація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). *Підприємництво, господарство і право*. 2018. № 8. С. 195–201.

55. Курман О. В. Криміналістична характеристика несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. Випуск 4. Том 2. 2017. С. 127–130.

56. Бородай О. В. Особа злочинця як елемент криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*, 2018. № 4 (84), С. 212–220. https://doi.org/10.33766/2524-0323.84.212-220

57. Неділько Я. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право.* 2020. № 7. С. 359–364.

58. Довженко О. П. Поняття кіберзлочину з криміналістичної позиції. *Юридичний вісник*. 2018. № 3. С. 79-83.

59. Бутузов В. М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : науково-практичний посібник. Київ., 2010. 245 с.

60. Пряхіна Є. В. Криміналістика : підручник. Львів, 2016. 948 с.

61. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 221 с.

62. Ісмайлов К. Ю. Сучасні проблеми дослідження криміналістичних особливостей кіберзлочинів. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції (м. Львів, 23 грудня 2016 року). Львів: ЛьвДУВС, 2017. С. 202-206.

63. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія. Запоріжжя, 2003. 250 с.

64. Салтевский М. В. Криміналістика (у сучасному викладі) : підручник. Київ. 2006. 588 с.

65. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. URL: http://dspace. nlu.edu.ua/bitstream/123456789/13283/1/ Avdeeva_168-175.pdf (дата звернення: 19.07.2021).

ДОДАТКИ

КОНСТИТУЦІЯ УКРАЇНИ

(Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141)

Стаття 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

(Із змінами та доповненнями станом на 2021 рік)

Розділ XVI
КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. Значною шкодою у статтях 361-363^{-1}, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 361^{1}. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів,

призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк до п'яти років.

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

1. 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, створеної та захищеної відповідно до чинного законодавства, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від двох до п'яти років.

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

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

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

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, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363[1]. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

ЗАКОН УКРАЇНИ
ПРО НАЦІОНАЛЬНУ ПРОГРАМУ ІНФОРМАТИЗАЦІЇ

(Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст. 181)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Основні терміни та поняття

У цьому Законі наведені нижче терміни та поняття вживаються у такому значенні:

база даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній області;

база знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами;

засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій;

інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

інформаційний суверенітет держави – здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави;

локалізація програмних продуктів – приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, нормами і правилами, що діють в Україні;

нерезиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням за межами України, які створені й діють відповідно до законодавства іноземної держави, у тому числі юридичні особи та інші суб'єкти підприємницької діяльності, створені за участю юридичних і фізичних осіб;

окреме завдання – комплекс проєктів інформатизації, взаємопов'язаних і взаємопогоджених за термінами реалізації, складом виконавців та спрямованих на досягнення конкретних цілей;

проєкт інформатизації – комплекс взаємопов'язаних заходів, як правило, інвестиційного характеру, що узгоджені за часом, використанням певних матеріально-технічних, інформаційних, людських, фінансових та інших ресурсів і мають на меті створення заздалегідь визначених інформаційних і телекомунікаційних систем, засобів інформатизації та інформаційних ресурсів, які відповідають певним показникам якості;

резиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням на території України, які здійснюють свою діяльність відповідно до законодавства України.

ЗАКОН УКРАЇНИ
ПРО ІНФОРМАЦІЮ

(Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

суб'єкт владних повноважень – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Розділ II
ВИДИ ІНФОРМАЦІЇ

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:
– інформація про фізичну особу;
– інформація довідково-енциклопедичного характеру;
– інформація про стан довкілля (екологічна інформація);
– інформація про товар (роботу, послугу);
– науково-технічна інформація;
– податкова інформація;
– правова інформація;
– статистична інформація;
– соціологічна інформація;
– інші види інформації.

Стаття 11. Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та

захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних.

Стаття 12. Інформація довідково-енциклопедичного характеру

1. Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

2. Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-телекомунікаційними системами.

3. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 13. Інформація про стан довкілля (екологічна інформація)

1. Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про:
- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;
- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);
- стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
- інші відомості та/або дані.

2. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Стаття 14. Інформація про товар (роботу, послугу)

1. Інформація про товар (роботу, послугу) – відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

2. Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

3. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 15. Науково-технічна інформація

1. Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проєктно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Правовий режим науково-технічної інформації визначається Законом України «Про науково-технічну інформацію», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Стаття 16. Податкова інформація

1. Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

2. Правовий режим податкової інформації визначається Податковим кодексом України та іншими законами.

Стаття 17. Правова інформація

1. Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. Джерелами правової інформації є Конституція України, інші законодавчі та підзаконні нормативно-правові акти, міжнародні договори й угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

3. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Стаття 18. Статистична інформація

1. Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

3. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

4. Правовий режим державної статистичної інформації визначається Законом України «Про державну статистику», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 19. Соціологічна інформація

1. Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

2. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 20. Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Стаття 21. Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;
2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;
3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення,

а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;
5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;
5[1]) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;
6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

ЗАКОН УКРАЇНИ ПРО ЕЛЕКТРОННІ ДОКУМЕНТИ ТА ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ

(Відомості Верховної Ради України (ВВР), 2003, № 36, ст. 275)

Розділ I ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

адресат – фізична або юридична особа, якій адресується електронний документ;

дані – інформація, яка подана у формі, придатній для її оброблення електронними засобами;

посередник – фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;

обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

автор електронного документа – фізична або юридична особа, яка створила електронний документ;

суб'єкти електронного документообігу – автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Стаття 2. Сфера дії Закону

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Стаття 3. Законодавство про електронні документи та електронний документообіг

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про телекомунікації», «Про обов'язковий примірник документів», «Про Національний архівний фонд та архівні установи», цим Законом, а також іншими нормативно-правовими актами.

Розділ II ЕЛЕКТРОННИЙ ДОКУМЕНТ

Стаття 5. Електронний документ

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Стаття 6. Електронний підпис

Для ідентифікації автора електронного документа може використовуватися електронний підпис.

{Частина перша статті 6 в редакції Закону № 1206-VII від 15.04.2014}

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням удосконалених та кваліфікованих електронних підписів, регулюються Законом України «Про електронні довірчі послуги».

{Частина третя статті 6 в редакції Закону № 2155-VIII від 05.10.2017}

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Стаття 7. Оригінал електронного документа

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги».

{Частина перша статті 7 із змінами, внесеними згідно із Законом № 1206-VII від 15.04.2014; в редакції Законів № 675-VIII від 03.09.2015, № 2155-VIII від 05.10.2017}

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Стаття 8. Правовий статус електронного документа та його копії

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;
2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;
3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

ЗАКОН УКРАЇНИ
ПРО ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ

(Відомості Верховної Ради (ВВР), 2017, № 45, ст. 400)

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі терміни вживаються в такому значенні:

1) автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;
2) блокування сертифіката відкритого ключа – тимчасове зупинення чинності сертифіката відкритого ключа;
3) вебсайт – сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу;
4) відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;
5) відокремлений пункт реєстрації – представництво (філія, підрозділ, територіальний орган) надавача електронних довірчих послуг або юридична чи фізична особа, яка на підставі наказу надавача електронних довірчих послуг (його керівника) або договору, укладеного з ним, здійснює реєстрацію підписувачів з дотриманням вимог цього Закону та законодавства у сфері захисту інформації;
6) Довірчий список – перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються;
7) електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;
8) електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;
9) електронна печатка – електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних;

10) електронна позначка часу – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;
11) електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему;
12) електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;
13) електронні дані – будь-яка інформація в електронній формі;
14) засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;
15) засіб електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки;
16) засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;
17) засіб кваліфікованого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам цього Закону;
18) засіб удосконаленого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення вдосконаленого електронного підпису чи печатки, та/або перевірки вдосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа вдосконаленого електронного підпису чи печатки;
19) ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;
20) ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;
21) інтероперабельність – технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою;
22) кваліфікована електронна печатка – удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;

23) кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;
24) кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;
25) кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам цього Закону;
26) компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;
27) користувачі електронних довірчих послуг – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону;
28) надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг;
29) особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;
30) пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;
31) перевірка – процес засвідчення справжності і підтвердження того, що електронний підпис чи печатка є дійсними;
32) підписувач – фізична особа, яка створює електронний підпис;
33) поновлення сертифіката відкритого ключа – відновлення чинності попередньо заблокованого сертифіката відкритого ключа;
34) програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг (далі – програмно-технічний комплекс), – апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг;
35) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів – електронна база даних, у якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;

36) реєстрована електронна доставка – послуга, яка дає змогу передавати електронні дані між третіми сторонами за допомогою електронних засобів, засвідчувати обробку переданих електронних даних, у тому числі підтверджувати відправлення та отримання електронних даних, та захистити відправлені електронні дані від втрати, крадіжки, пошкодження або несанкціонованих змін;
37) самопідписаний сертифікат відкритого ключа – сертифікат відкритого ключа, який формується центральним засвідчувальним органом або засвідчувальним центром з використанням особистого ключа центрального засвідчувального органу або засвідчувального центру;
38) сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію вебсайту;
39) скасування сертифіката відкритого ключа – зупинення чинності сертифіката відкритого ключа;
40) створювач електронної печатки – юридична особа, яка створює електронну печатку;
41) схема електронної ідентифікації – система електронної ідентифікації, у якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб;
42) технологічна нейтральність національних технічних рішень – невтручання органів, що здійснюють державне регулювання у сфері електронних довірчих послуг, у процес розроблення програмно-технічних комплексів, засобів електронного підпису чи печатки та засобів криптографічного захисту інформації, який не перешкоджатиме досягненню інтероперабельності між ними;
43) удосконалена електронна печатка – електронна печатка, створена за результатом криптографічного перетворення електронних даних, з якими пов'язана ця електронна печатка, з використанням засобу удосконаленої електронної печатки та особистого ключа, однозначно пов'язаного із створювачем електронної печатки, і який дає змогу здійснити електронну ідентифікацію створювача електронної печатки та виявити порушення цілісності електронних даних, з якими пов'язана ця електронна печатка;
44) удосконалений електронний підпис – електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис.

2. Інші терміни вживаються у значеннях, наведених у Цивільному кодексі України, законах України «Про електронні документи та електронний

документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про стандартизацію», «Про технічні регламенти та оцінку відповідності», «Про наукову і науково-технічну експертизу», «Про Національний банк України».

Розділ III
ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ

Стаття 14. Засоби електронної ідентифікації

1. Електронна ідентифікація здійснюється за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України.

2. Міжнародні договори України щодо електронних довірчих послуг повинні передбачати порядок подання повідомлень та визнання схем електронної ідентифікації (із зазначенням рівня довіри для засобів електронної ідентифікації).

Стаття 15. Схеми електронної ідентифікації

1. Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Схема електронної ідентифікації визначається Кабінетом Міністрів України.

2. Низький, середній та високий рівні довіри до засобів електронної ідентифікації повинні відповідати таким критеріям:

- низький рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;
- середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності;
- високий рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи.

3. Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до схем електронної ідентифікації.

Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації.

Розділ IV
ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ

Стаття 16. Вимоги до електронних довірчих послуг

1. Електронні довірчі послуги надаються, як правило, на договірних засадах надавачами електронних довірчих послуг.

2. До складу електронних довірчих послуг входять:

– створення, перевірка та підтвердження удосконаленого електронного підпису чи печатки;
– формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки;
– формування, перевірка та підтвердження чинності сертифіката автентифікації вебсайту;
– формування, перевірка та підтвердження електронної позначки часу;
– реєстрована електронна доставка;
– зберігання удосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності.

3. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок зі спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку зі спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш як 1000 мінімальних розмірів заробітної плати.

4. Розподіл ризиків збитків, що можуть бути заподіяні користувачам електронних довірчих послуг та третім особам фізичними або юридичними особами, не внесеними центральним засвідчувальним органом до Довірчого списку, визначається суб'єктами правових відносин на договірних засадах.

Стаття 17. Використання електронних довірчих послуг

1. Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях не повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в інформаційних системах, у яких здійснюється обробка таких електронних даних, можуть здійснюватися з використанням електронних довірчих послуг або без отримання таких послуг, за умови попередньої домовленості між учасниками взаємодії щодо порядку електронної ідентифікації учасників таких правових відносин.

2. Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в складових частинах інформаційних систем, в яких здійснюється обробка таких електронних даних та володільцями інформації в яких є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, повинні здійснюватися з використанням кваліфікованих електронних довірчих послуг.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори, нотаріуси та інші суб'єкти, уповноважені державою на здійснення функцій державного реєстратора, для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа, а для реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону, застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

3. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності встановлюється Кабінетом Міністрів України.

4. Нотаріальні дії з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняються в порядку, визначеному головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері нотаріату.

5. Здійснення правосуддя з використанням кваліфікованого електронного підпису чи печатки або інших засобів електронної ідентифікації вчиняється в порядку, встановленому законом.

6. Використання електронних довірчих послуг не змінює порядку вчинення правочинів, встановленого законом.

Правочини, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, встановлених законом, вчиняються в електронній формі виключно із застосуванням кваліфікованих електронних довірчих послуг та у встановленому порядку.

7. Результати надання кваліфікованих електронних довірчих послуг повинні визнаватися в усіх державних установах та іншими користувачами цих послуг.

Стаття 18. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки

1. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки надається кваліфікованим постачальником електронних довірчих послуг та включає:

надання користувачам електронних довірчих послуг засобів кваліфікованого електронного підпису чи печатки для генерації пар ключів та/або створення кваліфікованих електронних підписів чи печаток, та/або перевірки кваліфікованих електронних підписів чи печаток, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки;

технічну підтримку та обслуговування наданих засобів кваліфікованого електронного підпису чи печатки.

2. Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо:

перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису чи печатки;

перевіркою встановлено, що відповідно до вимог цього Закону на момент створення кваліфікованого електронного підпису чи печатки був чинним кваліфікований сертифікат електронного підпису чи печатки підписувача чи створювача електронної печатки;

за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача чи створювача електронної печатки;

під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки;

під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов'язаний цей кваліфікований електронний підпис чи печатка.

3. Електронний підпис чи печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки.

4. Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

5. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

6. Обов'язкові вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

7. Випуск та обіг засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що посвідчують особу, регулюються законодавством.

Вимоги до кваліфікованих електронних довірчих послуг, які надаються з використанням засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що посвідчують особу, встановлюються цим Законом та іншими актами законодавства.

Стаття 19. Засоби кваліфікованого електронного підпису чи печатки

1. Засоби кваліфікованого електронного підпису чи печатки повинні забезпечувати:

належний рівень унікальності пари ключів, що ними генеруються;

конфіденційність особистих ключів під час їх генерації, зберігання та створення кваліфікованого електронного підпису чи печатки;

захист від доступу до особистих ключів сторонніх осіб.

Засоби кваліфікованого електронного підпису чи печатки не повинні змінювати електронні дані, з якими пов'язаний цей кваліфікований електронний підпис чи печатка, або перешкоджати доступу до них підписувача чи створювача (уповноваженого представника створювача) електронної печатки.

2. Засоби кваліфікованого електронного підпису чи печатки під час перевірки кваліфікованого електронного підпису чи печатки повинні надавати користувачеві електронних довірчих послуг результат процесу перевірки та виявляти всі події, що стосуються порушень захисту інформації.

3. Вимоги до засобів кваліфікованого електронного підпису чи печатки встановлюються Кабінетом Міністрів України.

Відповідність засобів кваліфікованого електронного підпису чи печатки зазначеним вимогам підтверджується документами про відповідність або позитивними експертними висновками за результатами їх державної експертизи у сфері криптографічного захисту інформації.

4. Встановлення обов'язкових вимог до засобів кваліфікованого електронного підпису чи печатки, а також перевірка їх дотримання здійснюються відповідно до вимог, установлених Кабінетом Міністрів України.

Стаття 20. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає:

створення умов для генерації пари ключів особисто підписувачем чи створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки;

формування кваліфікованих сертифікатів електронного підпису чи печатки, що відповідають вимогам цього Закону, та видачу їх користувачу електронної довірчої послуги;

скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису чи печатки у випадках, передбачених цим Законом;

перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки шляхом надання третім особам інформації про їхній статус та відповідність вимогам цього Закону;

надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток шляхом їх розміщення на офіційному вебсайті

кваліфікованого надавача електронних довірчих послуг, за умови згоди підписувача чи створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

2. Формування та видача кваліфікованих сертифікатів електронного підпису чи печатки, що не відповідають вимогам цього Закону, заборонені.

3. Обов'язкові вимоги до кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Стаття 21. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту включає:

формування кваліфікованого сертифіката автентифікації вебсайту, що відповідає вимогам цього Закону, та передачу його користувачу електронної довірчої послуги;

створення умов для генерації пари ключів особисто користувачем цієї електронної довірчої послуги за допомогою засобу кваліфікованого електронного підпису чи печатки;

скасування, блокування та поновлення кваліфікованого сертифіката автентифікації вебсайту у випадках, передбачених цим Законом;

перевірку та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту шляхом надання третім особам інформації про його статус та відповідність вимогам цього Закону;

надання доступу до кваліфікованого сертифіката автентифікації вебсайту шляхом розміщення його на офіційному вебсайті кваліфікованого надавача електронних довірчих послуг, за умови згоди особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті автентифікації вебсайту, на публікацію кваліфікованого сертифіката автентифікації вебсайту.

2. Обов'язкові вимоги до кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації вебсайту, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Стаття 22. Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа

1. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

2. Ідентифікація фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний

реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

3. Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться в раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

4. Ідентифікація іноземців здійснюється відповідно до законодавства.

5. Під час перевірки цивільної правоздатності та дієздатності юридичної особи кваліфікований надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

6. Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог цього Закону, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, кваліфікованому надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

Стаття 23. Кваліфіковані сертифікати відкритих ключів

1. Під час надання кваліфікованих електронних довірчих послуг використовуються кваліфіковані сертифікати електронного підпису, кваліфіковані сертифікати електронної печатки та кваліфіковані сертифікати автентифікації вебсайту.

2. Кваліфіковані сертифікати відкритих ключів обов'язково повинні містити:

1) позначку, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;
2) позначку, що сертифікат відкритого ключа виданий в Україні;
3) ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа (далі – суб'єкти, які видали сертифікат), у тому числі обов'язково:

для юридичної особи: найменування та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено її державну реєстрацію;

для фізичної особи-підприємця: прізвище, ім'я, по батькові (за наявності) та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та

повідомили про це відповідний податковий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), за якими здійснено її державну реєстрацію;

4) ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, у тому числі обов'язково:

прізвище, ім'я, по батькові (за наявності) підписувача та унікальний номер запису в Єдиному державному демографічному реєстрі або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний податковий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

найменування або прізвище, ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з Єдиним державним реєстром підприємств та організацій України, за якими здійснено його державну реєстрацію, або унікальний номер запису в Єдиному державному демографічному реєстрі, або реєстраційний номер облікової картки платника податків, або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний податковий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

5) місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;
6) значення відкритого ключа, який відповідає особистому ключу;
7) відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;
8) серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;
9) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені суб'єктом, який видав сертифікат;
10) відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;
11) відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;
12) відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
13) відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
14) ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації вебсайту).

{Частина друга статті 23 із змінами, внесеними згідно із Законом № 440-IX від 14.01.2020}

3. Кваліфіковані сертифікати відкритих ключів можуть містити інші ідентифікаційні дані фізичних або юридичних осіб, необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

4. Обов'язкові вимоги до кваліфікованих сертифікатів відкритих ключів, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

5. Правочин, вчинений в електронній формі, може бути визнаний судом недійсним у разі, коли під час його вчинення використовувався кваліфікований електронний підпис чи печатка, кваліфікований сертифікат якого/якої не містить відомостей, передбачених частиною другою цієї статті, або містить недостовірні відомості.

Стаття 24. Чинність кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа вважається чинним у разі, якщо на момент перевірки чинності:

строк дії, зазначений у кваліфікованому сертифікаті відкритого ключа, не закінчився;

суб'єктом, який видав сертифікат, статус кваліфікованого сертифіката відкритого ключа не змінено на скасований або блокований з підстав, визначених цим Законом;

за попередніми двома ознаками був чинним кваліфікований сертифікат відкритого ключа суб'єкта, який видав сертифікат.

2. Суб'єкти, які видають сертифікати відкритих ключів, не повинні видавати кваліфіковані сертифікати відкритих ключів із строком дії, що перевищує строк дії їх власних кваліфікованих сертифікатів відкритих ключів.

3. Інформація про статус кваліфікованих сертифікатів відкритих ключів надається суб'єктами, що видали сертифікати, засобами їх інформаційно-телекомунікаційної системи цілодобово.

4. Доступ до кваліфікованих сертифікатів відкритих ключів надається суб'єктами, що видали сертифікати, з урахуванням вимог законодавства у сфері захисту персональних даних.

Стаття 25. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів

1. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин скасовується суб'єктом, який видав сертифікат, у разі:

1) подання користувачем електронних довірчих послуг заяви про скасування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;
2) надходження до суб'єкта, який видав сертифікат, документа, що підтверджує:

– смерть фізичної особи-підписувача;
– припинення діяльності створювача електронної печатки;
– зміни ідентифікаційних даних користувача електронних довірчих послуг;
– факт державної реєстрації припинення підприємницької діяльності фізичної особи-підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;
– надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;
– факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;
– набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

2. Самопідписаний сертифікат електронної печатки центрального засвідчувального органу не пізніше ніж протягом 24 годин скасовується центральним засвідчувальним органом у разі:

підтвердження факту компрометації особистого ключа центрального засвідчувального органу, виявленого ним самостійно або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішенням суду про скасування самопідписаного сертифіката електронної печатки центрального засвідчувального органу.

3. У разі подання повідомлення про прийняття кваліфікованим надавачем електронних довірчих послуг рішення про припинення діяльності з надання кваліфікованих електронних довірчих послуг центральний засвідчувальний орган або засвідчувальний центр на основі відповідного рішення скасовує кваліфікований сертифікат відкритого ключа, виданий цьому надавачу відповідно до вимог цього Закону.

4. Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на скасований.

5. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

6. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин блокується суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг заяви про блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;

повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг;

набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;

порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг.

7. Кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також блокується у разі прийняття рішення контролюючим органом про блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача електронних довірчих послуг за результатами здійснення державного нагляду (контролю) відповідно до вимог цього Закону.

8. Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на заблокований.

9. Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

10. Заблокований кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин поновлюється суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);

повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру;

надходження до суб'єкта, який видав сертифікат, повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили.

11. Заблокований кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також поновлюється відповідно до вимог цього Закону в разі:

відновлення статусу кваліфікованого надавача електронних довірчих послуг;

набрання законної сили рішенням суду на користь надавача електронних довірчих послуг.

12. Кваліфікований сертифікат відкритого ключа, який був заблокований, відновлює свою чинність з моменту його поновлення.

13. Кваліфікований сертифікат відкритого ключа вважається поновленим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на поновлений.

14. Суб'єкт, який видав кваліфікований сертифікат відкритого ключа, повинен забезпечити доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа.

Стаття 26. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу

1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає:

формування кваліфікованої електронної позначки часу;

передачу кваліфікованої електронної позначки часу користувачеві електронної довірчої послуги.

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов'язані.

2. Кваліфікована електронна позначка часу повинна забезпечувати:

зв'язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;

точність часу в програмно-технічному комплексі кваліфікованого надавача електронних довірчих послуг, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

3. До кваліфікованої електронної позначки часу додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка.

4. Використання кваліфікованої електронної позначки часу для постійного зберігання електронних даних є обов'язковим.

5. Обов'язкові вимоги до процедур надання кваліфікованої електронної довірчої послуги надання кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

ЗАКОН УКРАЇНИ ПРО ТЕЛЕКОМУНІКАЦІЇ

(Відомості Верховної Ради України (ВВР), 2004, № 12, ст. 155)

Глава I ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні:

абонент – споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

абонентна плата – фіксований платіж, який може встановлювати оператор телекомунікацій для абонента за доступ на постійній основі до своєї телекомунікаційної мережі незалежно від факту отримання послуг;

абонентський номер – сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі;

адреса мережі Інтернет – визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

адресний простір мережі Інтернет – сукупність адрес мережі Інтернет;

безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) – електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися зі збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру;

взаємозв'єднання телекомунікаційних мереж – встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією;

власник (володілець) кабельної каналізації електрозв'язку – суб'єкт господарювання, у власності (володінні) якого перебувають уся інфраструктура кабельної каналізації електрозв'язку або окремі її елементи, набуті на належній правовій підставі, призначені для забезпечення доступу до телекомунікаційної мережі загального користування;

голосова телефонія – обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж;

дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

домен – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

домен.UA – домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет;

домен другого рівня – частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

електрозв'язок – див. «телекомунікації»;

загальнодоступні (універсальні) телекомунікаційні послуги – мінімальний набір визначених цим Законом послуг нормованої якості, доступний усім споживачам на всій території України;

Інтернет – всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

інформаційна система загального доступу – сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних;

інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації;

інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

кабельна каналізація електрозв'язку – обладнання та споруди, призначені для прокладання, монтажу та експлуатаційного обслуговування кабелів телекомунікацій, що включають трубопроводи (канали кабельної каналізації), закладні та оглядові пристрої в колодязях, кабельних шафах, шахтах, колекторах, мостах, естакадах, тунелях, будівлях, а також приміщення для вводу кабелів і розміщення лінійного обладнання;

канал електрозв'язку – сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі;

канал кабельної каналізації електрозв'язку – окремо виділені місця в колекторах, телекомунікаційних колодязях, тунелях, акведуках, шляхопроводах, на мостах, мостових переходах, естакадах, трубопроводах, а також інші надземні та підземні інженерні споруди, що призначені для прокладання або використовуються для прокладання магістральних, з'єднувальних та розподільних проводових і оптоволоконних кабелів електрозв'язку, а також розміщення супутніх лінійних технічних засобів телекомунікацій;

кінцеве обладнання – обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг;

монопольний (домінуючий) оператор телекомунікацій – оператор, який відповідно до законодавства України займає монопольне (домінуюче) становище на ринку певних телекомунікаційних послуг на території держави чи певного регіону;

Національний план нумерації – нормативно-правовий акт, який визначає структуру, регламентує розподіл та умови використання номерного ресурсу в телекомунікаційних мережах;

номерний ресурс – сукупність цифрових знаків, що використовуються для позначення (ідентифікації) мереж, послуг, пунктів закінчення мережі в телекомунікаційних мережах загального користування;

оператор телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

оператор, провайдер телекомунікацій з істотною ринковою перевагою на ринку телекомунікаційних послуг – оператор, провайдер телекомунікацій, частка доходу якого на визначеному національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, ринку певних телекомунікаційних послуг протягом року, що передує проведенню аналізу ринку, перевищує 25 відсотків сумарного доходу всіх операторів, провайдерів телекомунікацій, отриманого на цьому ринку за той самий період часу, або якщо внаслідок технологічного процесу надання послуги іншому оператору, провайдеру телекомунікацій її може бути надано тільки в мережі певного оператора, провайдера телекомунікацій;

передавання даних – передавання інформації у вигляді даних з використанням телекомунікаційних мереж;

перенесення абонентського номера – телекомунікаційна послуга, що надається абоненту за його заявою, яка полягає у збереженні за абонентом наданого йому оператором телекомунікацій абонентського номера з метою використання цього номера для отримання телекомунікаційних послуг у мережі іншого оператора телекомунікацій, що надає телекомунікаційні послуги на території України;

персональний номер – абонентський номер, що присвоюється зареєстрованому абоненту за його заявою у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, централізовано адмініструється і може використовуватися цим абонентом для отримання відповідно до договору телекомунікаційних послуг незалежно від географічного регіону України і типу цих послуг;

послуга пропуску трафіка – телекомунікаційна послуга щодо здійснення термінації та/або транзиту трафіка, що надається оператором телекомунікацій іншим операторам;

провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

проводовий електрозв'язок – передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконнооптичними жилами;

пропуск трафіка – проходження трафіка між елементами однієї або різних телекомунікаційних мереж;

пункт закінчення телекомунікаційної мережі – місце стику (з'єднання) мережі телекомунікацій та кінцевого обладнання;

ресурси телекомунікаційних мереж – наявні в телекомунікаційних мережах кількість номерів (номерний ресурс), кількість і пропускна спроможність проводових ліній з металевими жилами, оптичними волокнами, радіоліній, каналів, трактів для передавання інформації, комутаційних станцій та вузлів, радіочастотний ресурс;

ринок телекомунікаційних послуг – сфера обігу визначених телекомунікаційних послуг, на які протягом певного часу і в межах певної території є попит і пропозиція;

розподіл номерного ресурсу – виділення номерного ресурсу з визначеного діапазону номерів для надання телекомунікаційних послуг;

розрахункова такса – сума, що визначає розмір оплати за доступ до технічних та технологічних ресурсів мереж операторів телекомунікацій (здійснення доступу) для пропуску одиниці трафіка і застосовується для операторів, які є суб'єктами господарської діяльності на території України;

розрахункова такса за послугу пропуску трафіка – розмір плати за термінацію або транзит одиниці трафіка між телекомунікаційними мережами операторів;

роумінг національний - телекомунікаційна послуга, яка забезпечує можливість абонентам одного оператора телекомунікацій, що надає послуги рухомого

(мобільного) зв'язку на території України, отримувати телекомунікаційні послуги в телекомунікаційній мережі іншого оператора (операторів) у межах України;

рухомий (мобільний) зв'язок – електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного зі споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції;

споживач телекомунікаційних послуг (споживач) – юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб;

споруди електрозв'язку – будівлі, вежі, антени, що використовуються для організації електрозв'язку;

сталість телекомунікаційної мережі – властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників;

суб'єкти ринку телекомунікацій – оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій;

телекомунікації (електрозв'язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

телекомунікаційна мережа загального користування – телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів;

телекомунікаційна мережа доступу – частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно;

телекомунікаційна послуга (послуга) – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій;

телемережі – телекомунікаційні мережі загального користування, що призначаються для передавання програм радіо- та телебачення, а також інших телекомунікаційних і мультимедійних послуг і можуть інтегруватися з іншими телекомунікаційними мережами загального користування;

термінація трафіка – встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіка між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання;

технічні вимоги – (технічний) документ, що встановлює вимоги, які повинні бути виконані під час побудови та функціонування телекомунікаційних

мереж, застосування технічних засобів та об'єктів телекомунікацій чи отримання телекомунікаційних послуг;

технічні засоби телекомунікацій – обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж;

транзит трафіка – встановлення, підтримка телекомунікаційною мережею оператора фізичного та/або логічного з'єднання, пропуск трафіка між двома іншими телекомунікаційними мережами;

транспортна телекомунікаційна мережа – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу;

трафік – сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію;

фіксований зв'язок – телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання.

2. Термін «благодійне телекомунікаційне повідомлення» вживається в цьому Законі у значенні, наведеному в Законі України «Про благодійну діяльність та благодійні організації».

Стаття 9. Охорона таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпека телекомунікацій

1. Охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України.

2. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом.

3. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Глава VI
СПОЖИВАЧІ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

Стаття 32. Права споживачів телекомунікаційних послуг

1. Споживачі під час замовлення та/або отримання телекомунікаційних послуг мають право на:

1) державний захист своїх прав;
2) вільний доступ до телекомунікаційних послуг;
3) безпеку телекомунікаційних послуг;
4) вибір оператора, провайдера телекомунікацій;
5) вибір виду та кількості телекомунікаційних послуг;

6) безоплатне отримання від оператора, провайдера телекомунікацій вичерпної інформації щодо змісту, якості, вартості та порядку надання телекомунікаційних послуг;
7) своєчасне і якісне одержання телекомунікаційних послуг;
8) отримання від оператора, провайдера телекомунікацій наявних відомостей щодо наданих телекомунікаційних послуг;
9) обмеження оператором, провайдером телекомунікацій доступу споживача до окремих видів послуг на підставі його власної письмової заяви;
10) повернення від оператора, провайдера телекомунікацій невикористаної частини коштів у разі відмови від передплачених телекомунікаційних послуг у випадках і порядку, визначених правилами надання і отримання цих послуг, а також договором приєднання щодо виконання благодійного телекомунікаційного повідомлення (у разі укладення такого договору);
11) відмову від телекомунікаційних послуг у порядку, встановленому договором про надання телекомунікаційних послуг;
12) відшкодування збитків, заподіяних унаслідок невиконання чи неналежного виконання оператором, провайдером телекомунікацій обов'язків, передбачених договором із споживачем чи законодавством;
13) оскарження неправомірних дій операторів, провайдерів телекомунікацій шляхом звернення до суду та уповноважених державних органів;
14) відмову від оплати телекомунікаційної послуги, яку вони не замовляли;
15) отримання відомостей щодо можливості та порядку відмови від замовленої телекомунікаційної послуги;
16) безоплатне отримання від оператора, провайдера телекомунікацій рахунків за надані телекомунікаційні послуги. За особистим зверненням споживача з урахуванням технічної можливості обладнання телекомунікаційної мережі нарахована до оплати сума за надані послуги повинна бути розшифрована тільки за той розрахунковий період, до якого споживач має претензії, із зазначенням номера абонента, якого викликав споживач, виду послуги, часу початку і закінчення кожного сеансу зв'язку, обсягу наданих послуг, суми коштів до сплати за кожний сеанс зв'язку. Телекомунікаційні послуги, які надаються знеособлено (анонімно), розшифровці не підлягають;
16[1]) перенесення абонентського номера, користування персональним номером та отримання послуг національного роумінгу;
17) інші права, визначені законодавством України та договором про надання телекомунікаційних послуг.

2. Абонент, який отримує телекомунікаційні послуги без укладення договору в письмовій формі, може зареєструватися в оператора, надавши йому персональні дані відповідно до закону в порядку, установленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Стаття 33. Обов'язки споживачів телекомунікаційних послуг

1. Споживачі телекомунікаційних послуг зобов'язані дотримуватися Правил надання та отримання телекомунікаційних послуг, що затверджує Кабінет Міністрів України, зокрема:
1) використовувати кінцеве обладнання, що має документ про підтвердження відповідності;
2) не допускати використання кінцевого обладнання споживача для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку;
3) не допускати дій, що можуть створювати загрозу для безпеки експлуатації мереж телекомунікацій, підтримки цілісності та взаємодії мереж телекомунікацій, захисту інформаційної безпеки мереж телекомунікацій, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливлювати надання послуг іншим споживачам;
4) не допускати використання на комерційній основі кінцевого обладнання та абонентських ліній для надання телекомунікаційних послуг третім особам;
5) виконувати умови договору про надання телекомунікаційних послуг у разі його укладення, у тому числі своєчасно оплачувати отримані ними телекомунікаційні послуги;
6) виконувати інші обов'язки відповідно до законодавства.

2. У разі використання абонентами лічильників обліку тривалості телекомунікаційних послуг, що встановлюються на кінцевому обладнанні для перевірки правильності нарахування плати за отримані послуги, абоненти зобов'язані:
1) використовувати лічильники, що мають документ про підтвердження відповідності згідно із законодавством України;
2) періодично здійснювати метрологічну повірку лічильників як засобів вимірювальної техніки в порядку, визначеному законодавством України.

3. Споживачі телекомунікаційних послуг зобов'язані виконувати інші обов'язки відповідно до цього Закону та законодавства України.

Стаття 34. Захист інформації про споживача

1. Оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

2. Призначені для оприлюднення телефонні довідники, у тому числі електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім'я, по батькові, найменування, адресу та номер телефону абонента в разі, якщо в договорі про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації. Під час автоматизованої обробки інформації про абонентів оператор телекомунікацій забезпечує її захист відповідно до закону. Споживач має право на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб.

3. Інформація про споживача та про телекомунікаційні послуги, що він отримав, може надаватись у випадках і в порядку, визначених законом. В інших випадках зазначена інформація може поширюватися лише за наявності письмової згоди споживача.

Стаття 35. Захист інтересів споживачів у разі припинення діяльності оператором, провайдером телекомунікацій з надання телекомунікаційних послуг

1. Оператор, провайдер телекомунікацій, який припиняє діяльність з надання телекомунікаційних послуг, зобов'язаний попередити споживачів не пізніше ніж за три місяці до припинення надання телекомунікаційних послуг.

2. У разі вилучення номерного та/або радіочастотного ресурсу внаслідок порушення оператором, провайдером телекомунікацій законодавства такий оператор, провайдер зобов'язаний відшкодувати абоненту витрати, пов'язані з припиненням надання телекомунікаційних послуг, у встановленому законом порядку.

Стаття 36. Відповідальність споживачів телекомунікаційних послуг

1. Споживачі телекомунікаційних послуг несуть відповідальність за порушення норм цього Закону, Правил надання та отримання телекомунікаційних послуг відповідно до закону.

2. У разі затримки плати за надані оператором, провайдером телекомунікаційні послуги споживачі сплачують пеню, яка обчислюється від вартості неоплачених послуг у розмірі облікової ставки Національного банку України, що діяла в період, за який нараховується пеня.

3. Сплата споживачем пені, правомірне припинення чи скорочення оператором, провайдером переліку телекомунікаційних послуг не звільняє споживача від обов'язку оплатити надані йому телекомунікаційні послуги.

4. У разі виявлення пошкодження телекомунікаційної мережі, що сталося з вини споживача, усі витрати оператора телекомунікацій на усунення пошкодження, а також відшкодування інших збитків (у тому числі неотриманий прибуток) покладаються на споживача.

ЗАКОН УКРАЇНИ ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

(Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403)

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;
2) інформація про інцидент кібербезпеки – відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали

кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;
4) кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;
5) 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;
6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;
7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
8) кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність – сукупність кіберзлочинів;
10) кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;
11) кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;
12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами в кіберпросторі або з його використанням;
13) кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
14) кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;
15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;
16) критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;
17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою в мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;
18) національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Електронні інформаційні ресурси розуміють як будь-яку інформацію, що створена, записана, оброблена або збережена в цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;
19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;
20) система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;
21) системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, у якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Терміни «національна безпека», «національні інтереси», «загрози національній безпеці» вживаються в цьому Законі у значенні, визначеному Законом України «Про основи національної безпеки України».

ЗАКОН УКРАЇНИ ПРО НАЦІОНАЛЬНУ ПОЛІЦІЮ

(Відомості Верховної Ради (ВВР), 2015, № 40–41, ст. 379)

Розділ I ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 2. Завдання поліції

1. Завданнями поліції є надання поліцейських послуг у сферах:

1) забезпечення публічної безпеки і порядку;
2) охорони прав і свобод людини, а також інтересів суспільства та держави;
3) протидії злочинності;
4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

Розділ IV
ПОВНОВАЖЕННЯ ПОЛІЦІЇ

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення

1. Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом.

2. Поліція в рамках інформаційно-аналітичної діяльності:
1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;
2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;
3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;
4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями;
5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів в електронній формі та в обсягах даних, зазначених у статтях 7, 14 Закону України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів», відомості, необхідні для забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів.

3. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

4. Діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

5. Поліція зобов'язана письмово інформувати митні органи про виявлення нецільового використання та/або передачі транспортних засобів особистого користування, тимчасово ввезених на митну територію України чи поміщених у митний режим транзиту, у володіння, користування або розпорядження особам, які не ввозили такі транспортні засоби на митну територію України або не поміщували в митний режим транзиту, а також про виявлення розкомплектування таких транспортних засобів.

Стаття 26. Формування інформаційних ресурсів поліцією

1. Поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:
1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;
2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;
3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;
4) розшуку осіб, зниклих безвісти;
5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;
6) зареєстрованих в органах внутрішніх справ кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;
7) осіб, затриманих за підозрою у вчиненні правопорушень (адміністративне затримання, затримання згідно з дорученнями органів правопорядку, затримання осіб органами досудового розслідування, адміністративний арешт, домашній арешт);
8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією;
9) зареєстрованих кримінальних та адміністративних правопорушень, пов'язаних з корупцією, осіб, які їх учинили, та результатів розгляду цих правопорушень у судах;
10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;
11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;
12) викрадених (втрачених) документів за зверненням громадян;
13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;
14) викрадених транспортних засобів, які розшукуються у зв'язку з безвісним зникненням особи, виявлених безгосподарних транспортних засобів, а також викрадених, втрачених номерних знаків;
15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;
16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;
17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї із числа тієї, що незаконно зберігалася;

18) бази даних, що формуються у процесі здійснення оперативно-розшукової діяльності відповідно до закону.

2. Під час наповнення баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (дактилокартки, зразки ДНК).

3. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримання таких відомостей в актуальному стані в межах, визначених законодавством.

Стаття 27. Використання поліцією інформаційних ресурсів

1. Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних».

2. Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано.

3. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України.

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Стаття 28. Відповідальність за протиправне використання інформаційних ресурсів

1. Поліція вживає всіх заходів для недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації.

2. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

3. Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами (банками) даних у порядку, визначеному у статтях 26, 27 цього Закону.

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ

1. Зберігання та передача даних

Недотримання окремих правил безпеки під час здійснення службових обов'язків працівниками органів виконавчої влади місцевого самоврядування, посадовими особами державних підприємств, установ, організацій може призвести до втрати чи крадіжки мобільних телефонів, персональних ноутбуків, магнітних носіїв інформації тощо. Указане ставить під загрозу збереження персональних даних та може призвести до розголошення інформації з обмеженим доступом.

Сприятливі умови для реалізації кіберзагроз виникають через порушення вимог законодавства про захист інформації в інформаційно-телекомунікаційних системах (далі – ІТС), а також внаслідок таких чинників:

- здійснення несанкціонованого доступу до баз даних;
- копіювання та передача через незахищений канал мережі Інтернет документальних матеріалів, що містять службову інформацію;
- використання особистих технічних засобів у складі виробничих автоматизованих систем (USB-флеш накопичувачі);
- підключення до комп'ютерних систем технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;
- незахищеність ІТС за допомогою актуальних версій антивірусного програмного забезпечення.

З метою уникнення негативних наслідків у разі втрати або викрадення носіїв інформації необхідно:

- установити паролі на всі пристрої, що перебувають у користуванні, а також паролі / коди на доступ до всіх облікових записів;
- систематично здійснювати резервне копіювання важливих файлів;
- блокувати пристрої щоразу після закінчення роботи з ними.

2. Соціальні мережі

Для того, щоб уникнути (щоб уникнути повтору) несанкціонованого доступу до персональних акаунтів, зареєстрованих у соціально-орієнтованих ресурсах мережі Інтернет, необхідно:

- установити надійний пароль для входу в обліковий запис. При цьому рівень захищеності акаунту та інформації, яка в ньому міститься, залежить від складності встановленого пароля;
- використовувати функцію подвійної авторизації. Щоб увійти до профілю з незнайомого пристрою, сервіс вимагатиме пройти додаткову ідентифікацію як власника акаунту. У цьому разі на вказаний номер

телефону чи на поштову скриньку буде надіслано повідомлення з кодом підтвердження або треба буде ввести один із паролів, які попередньо були збережені через інший обраний спосіб підтвердження;
- здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованого доступу до ресурсів з невідомого пристрою або інтернет-браузера;
- під час створення акаунтів у соціальних мережах використовувати як логін поштову адресу надійного сервісу (наприклад «Google», «Yahoo») або українських поштових сервісів. Не рекомендується користуватися російськими сервісами;

не здійснювати авторизацію особистих чи робочих, корпоративних профілів із незнайомих чи незахищених пристроїв. Існує імовірність, що після завершення роботи не буде здійснено вихід з облікового запису або пристрій запам'ятає вказаний під час входу логін та пароль. Крім того, існує можливість ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;
- не відкривати вкладень у підозрілих повідомленнях від адресатів, щодо яких виникають сумніви;
- пам'ятайте, що саме фішинг є найпоширенішим способом отримання зловмисниками паролів до поштових скриньок та сторінок у соціальних мережах.

Також слід ураховувати, що під час гібридної агресії з боку Російської Федерації соціальні мережі активно використовуються для збору додаткових відомостей щодо місць регулярного перебування особи, її родичів, колег, особистих уподобань та іншої приватної інформації.

З метою недопущення отримання зацікавленими особами додаткової (приватної) інформації стосовно особи, членів її сім'ї, колег рекомендується:
- не публікувати в соціальних мережах інформацію, що може загрожувати особистому життю особи, життю членів її сім'ї та інших осіб;
- обмежити доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі. Обрати налаштування, які найбільше захищають додаткові відомості про власника акаунту. Зокрема, не зазначати геолокацію (місцерозташування);
- періодично переглядати список «друзів» у соціальній мережі. Якщо серед них є незнайомі або підозрілі акаунти, необхідно їх видалити, оскільки статус «друга» відкриває доступ до більшого обсягу приватної інформації про особу. У подальшому необхідно бути уважними під час додавання до списку «друзів» нових користувачів;
- не використовувати російські соціальні мережі «Вконтакте» та «Одноклассники», а також російські пошукові системи «Mail.ru» та «Yandex» (у т. ч. із застосуванням сервісів VPN), доступ до яких обмежено відповідно до Указу Президента України № 184/2020, оскільки відповідно до федеральних законів Російської Федерації власники вказаних ресурсів можуть передавати російським спецслужбам відомості щодо персональних даних

користувачів акаунтів (e-mail, номер мобільного телефону, дата та IP-адреса реєстрації, дата та IP-адреса останнього відвідування тощо).

Слід зазначити, що за розповсюдження через соціальні мережі матеріалів із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також зміни меж території чи державного кордону України на порушення порядку, установленого Конституцією України, передбачена кримінальна відповідальність,

Також варто звернути увагу на те, що окремі публікації, розміщені посадовими особами органів виконавчої влади на їх персональних сторінках у соціальних мережах, можуть слугувати інформаційним приводом, який у подальшому буде використаний для підриву авторитету державної влади в цілому, штучного загострення суспільно-політичної ситуації в державі та здійснення інших деструктивних дій, що можуть завдати шкоди державним інтересам України.

3. Використання додатків до смартфонів

Під час встановлення тих чи інших додатків на власний телефон ці програмні продукти можуть вимагати доступу до певної інформації на використовуваному пристрої, насамперед геолокації, списку контактів, акаунтів у соціальних мережах та поштових скриньок.

За наявними даними більшість шпигунських програм додаються саме до мобільних додатків, які цікавлять конкретну аудиторію. Тому необхідно бути уважним під час установлення додатків, особливо якщо робити це з невідомих та неперевірених сервісів.

З метою унеможливлення завантаження на особистий пристрій програм-шпигунів необхідно дотримуватися таких правил:
- інсталювати додатки лише з офіційних та перевірених сервісів («Chrome Store», «Google Play Store» для Android, «App Store» для iOS);
- заборонити операційній системі смартфона автоматично встановлювати додатки з невідомих джерел у відповідних налаштуваннях пристрою;

періодично здійснювати видалення додатків, які не використовуються.

4. Електронне листування

Щоб уникнути зламу електронної поштової скриньки, необхідно:
- підключити двофакторну аутентифікацію за допомогою мобільного пристрою. У такому разі, як тільки сторонні особи робитимуть спробу отримати доступ до поштової скриньки, буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу доступу;
- використовувати надійний пароль;
- не використовувати цей пароль для доступу до інших сервісів;
- періодично змінювати пароль;
- не використовувати для відновлення пароля російські сервіси («Yandex.ru», «Mail.ru» тощо);

- не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.doct», «.xlst» тощо;
- державні службовці повинні пам'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

5. Доступ до мережі «Інтернет»

Одним із найпоширеніших способів доступу до мережі Інтернет в публічних місцях є підключення до відкритих точок Wi-Fi. Зазвичай вони безоплатні та доступ до них здійснюється без введення паролів. Саме відсутність контролю доступу робить їх вразливими для використання зацікавленими особами, які мають на меті отримати персональні дані та відомості, що зберігаються на телефоні, планшеті тощо.

Щоб уникнути перехоплення інформації сторонніми особами, необхідно:

- під час здійснення доступу до мережі використовувати лише ті точки Wi-Fi, які мають протоколи безпеки для захисту безпровідного з'єднання WPA-2 та WPA-3;
- у публічних місцях найкраще користуватися особистим модемом Wi-Fi або здійснювали доступ до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора, або використовувати захищене VPN підключення;
- на мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».

6. Рекомендації посадовій особі органу виконавчої влади

Рекомендовано:

- підрозділам комунікації з громадськістю державних органів, під час суспільно-політичних подій у країні необхідно надавати коментарі та роз'яснення рішень для того, щоб уникнути спотворених інтерпретацій інформації у процесі обговорення тієї чи іншої ситуації в загальнодоступних та соціально-орієнтованих ресурсах інтернет-мережі;
- державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками підрозділів комунікації з громадськістю інформації у разі виникнення резонансних інцидентів, офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої важливої інформації від суспільства може знизити рівень довіри до них як представників державної влади;
- представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;

- органам державної влади необхідно розробити правила використання офіційних сторінок та акаунтів у соціальних мережах для уникнення непорозумінь з користувачами та окреслення формату комунікації через соціальні мережі. Крім того, вважається за доцільне здійснити верифікацію офіційних представництв органів державної влади та установ, які у своїй діяльності використовують акаунти в соціальних мережах, насамперед сервісів «Meta» (Facebook, Instagram), «Twitter» та канали у відеохостингу «Youtube»;
- держслужбовцям, а також іншим особам, які відповідно до своїх функціональних обов'язків працюють з інформацією з обмеженим доступом, варто пам'ятати, що у процесі оформлення допуску до державної таємниці (під час заповнення відповідних анкет) необхідно вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних електронних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах.

Наукове видання

О. В. Ковальова

ПРОТИДІЯ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ З НЕСАНКЦІОНОВАНИМ ВТРУЧАННЯМ У ДЕРЖАВНІ РЕЄСТРИ

НАУКОВО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

Підготовлено до друку ВД «Дакор»
Друкується в авторській редакції

Підписано до друку __.__.2022. Гарнітура Cambria. Формат 60×84 1/16.
Папір офсетний. Друк офсетний. Ум.-друк. арк. 8,85. Обкл.-вид. арк. 8,23. Наклад ___ прим.

ТОВ «ВД «Дакор»
Свід. ДК № 4349 від 05.07.2012
(044) 461-85-06; vd_dakor@ukr.net www.dakor.kiev.ua
04073, м. Київ, просп. Степана Бандери, 8