CRIMHUM
Co-funded by the Erasmus+ Programme of the European Union

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ

Посібник

598471-EPP-1-2018-1-AT-EPPKA2-CBHE-JP

Modernising Master's Training on Criminal Justice
CRIMHUM

CYBERCRIME AND DIGITAL EVIDENCE

Lviv
Ivan Franko National University of Lviv
2022

Authors:
Bohdan Holovkin, Olha Denkovych, Vasyl Lutsyk, Dmytro Tsekhan

Edited by:
Olha Denkovych, Gabriele Schmölzer

Удосконалення магістерської програми
з кримінальної юстиції

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ

Навчальний посібник

За редакцією
кандидата юридичних наук, доцента Ольги ДЕНЬКОВИЧ,
доктора права, професора Габріеле ШМЕЛЬЦЕР

Львів
ЛНУ ім. Івана Франка
2022

УДК [343.3/7:004](075.8)
К 39

Автори:
Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан

Рецензенти:
Олексій Гумін, доктор юридичних наук, професор,
завідувач кафедри кримінального права і процесу Національного
університету «Львівська політехніка»,
Тарас Созанський, кандидат юридичних наук, професор,
перший проректор Львівського державного університету
внутрішніх справ

Серія заснована в 2020 році

Видання підготовлено в рамках проєкту Програми Європейського Союзу ERASMUS+ «Модернізація магістерських програм для майбутніх суддів, прокурорів, слідчих з урахуванням європейських стандартів у сфері прав людини» (598471-EPP-1-2018-1-AT-EPPKA2-CBHI-JP), керівниця проєкту – *Габріеле Шмельцер*

К 39 **Кіберзлочинність та електронні докази** = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с. – (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

ISBN 978-617-10-0805-2 (серія)
ISBN 978-617-10-0807-6 (електрон. вид.)

У навчальному посібнику розглянуто поняття кіберзлочину та кіберзлочинності, особливості запобігання кіберзлочинності, особливості методики розслідування цієї категорії кримінальних правопорушень. Окрему увагу приділено поняттю та особливостям електронних доказів, способам їх збирання та правильного процесуального оформлення результатів процесуальних дій, спрямованих на їх збирання.

Нормативну базу і правозастосовну практику в посібнику проаналізовано станом на 1 жовтня 2022 року.

Навчальний посібник призначений для магістрів, що навчаються за спеціальністю 081 «Право».

УДК [343.3/7:004](075.8)

ISBN 978-617-10-0805-2 (серія)
ISBN 978-617-10-0807-6 (електрон. вид.)

ЗМІСТ

УМОВНІ ПОЗНАЧЕННЯ

АС	–	Автоматизована система
ВВП	–	Валовий внутрішній продукт
ВС	–	Верховний Суд України
ДКП	–	Департамент кіберполіції Національної поліції України
ЕОМ	–	Електронно-обчислювальна машина
Європол	–	Європейське поліцейське управління
ЄКПЛ	–	Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини)
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЄС	–	Європейський Союз
Інструкція	–	Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України № 114/1042/516/1199/936/1687/5 від 16 листопада 2012 року
КК, КК України	–	Кримінальний кодекс України від 5 квітня 2001 року
КПК, КПК України	–	Кримінальний процесуальний кодекс України від 13 квітня 2012 року

КТЕ	–	Комп'ютерно-технічна судова експертиза
МНІ	–	Матеріальний носій інформації
НДЕКЦ	–	Науково-дослідний експертно-криміналістичний центр
НДІСЕ	–	Науково-дослідний інститут судових експертиз
НП	–	Національна поліція України
НСРД	–	Негласні слідчі (розшукові) дії
ООН	–	Організація Об'єднаних Націй
ПЕОМ	–	Персональна електронно-обчислювальна машина
СНД	–	Співдружність Незалежних Держав
СТЗ	–	Спеціальні технічні засоби
США	–	Сполучені Штати Америки
DDoS	–	Distributed denial-of-service (Відмова в обслуговуванні)

Про проєкт
598471-EPP-1-2018-1-AT-EPPKA2-CBHI-JP
«Модернізація магістерських програм для майбутніх суддів, прокуроров,слідчих з урахуванням європейських стандартів у сфері прав людини»

Програма Європейського Союзу ERASMUS+ спрямована на підтримку діяльності у сфері освіти, перепідготовки, молоді та спорту. ERASMUS+ об'єднав існуючі раніше сім програм: програми безперервного навчання (Erasmus, Leonardo da Vinci, Comenius та Grundtvig), програму «Молодь у дії», 5 програм міжнародного співробітництва (Erasmus Mundus, Tempus, Alfa, Edulink, програма для співпраці з промислово розвиненими країнами). Раніше існуюча з 1990 року TEMPUS (Транс'європейська програма мобільності для навчання в університетах) підтримувала модернізацію вищої освіти і створювала простір для співробітництва в країнах – партнерах Європейського Союзупротягом більше 25 років.

Програма ERASMUS+ створює для студентів, співробітників та волонтерів потенціал для мобільностей в інші країни з метою покращення своїх навичок та можливостей працевлаштування. Вона дозволяє організаціям працювати в транснаціональному партнерстві та ділитися інноваційними практиками в галузі освіти, професійної підготовки та підтримки молоді.

Спираючись на успіх програми в період 2014–2020 років, ERASMUS+ у період 2021–2027 років активізує зусилля на розширенні можливостей більшого кола учасників, приділяючи особливу увагу якісній взаємодії і сприяючи більш інклюзивним освіті та навчанню, які покликані формувати і розвивати компетенції, необхідні для динамічно змінюваних демократичних суспільств, згуртованих навколо цінностей

міжкультурного взаєморозуміння та розвитку горизонтів можливостей для особистісного та соціально-освітнього і професійного розвитку.

Проєкти зі створення потенціалу в галузі вищої освіти, яким є CRIMHUM, є транснаціональними проєктами співробітництва, на основі багатосторонніх партнерських відносин, насамперед між закладами вищої освіти держав ЄС і держав-партнерів.

Мета таких проєктів полягає у наданні підтримки державам-партнерам у:

- модернізації, інтернаціоналізації та розширенні доступу до вищої освіти;
- вирішенні проблем, з якими стикаються їх вищі інститути та система освіти;
- активізації співпраці з Європейським Союзом;
- добровільній конвергенції з розвитком Європейського Союзу в галузі вищої освіти, а також заохочення контактів між людьми та міжкультурного порозуміння.

Конкретна мета ERASMUS+-проєкту 598471-EPP-1-2018-1-AT-EPPKA2-CBHI-JP (CRIMHUM) полягає в тому, щоб створити комплексну, засновану на правах людини підготовку фахівців у сфері кримінального правосуддя шляхом модернізації спеціалізованих магістерських програм судово-прокурорсько-слідчої спеціалізації.

У межах реалізації спільної мети проєкту здійснюються такі завдання:

- структурна та концептуальна модернізація навчального плану спеціалізованих магістерських програм судово-прокурорсько-слідчої спеціалізації (профілізації), поєднана з поглибленням навичок викладання і навчання на основі європейських науково-освітніх методик та розробкою і впровадженням новітніх навчально-методичних посібників;

– підвищення професійної та дидактичної кваліфікації викладачів держав-партнерів;
– зміцнення ресурсної бази модернізованих магістерських програм.

Сталий розвиток проєкту в Україні забезпечується створенням на ґрунті CRIMHUM можливостей для вдосконалення існуючих та розробки нових магістерських програм за підтримки низки європейських університетів з Австрії, Німеччини, Литви, Франції і Хорватії в трьох українських університетах: Львівському національному університеті ім. Івана Франка, Національному юридичному університеті ім. Ярослава Мудрого, Національному університеті «Одеська юридична академія».

Координатори проєкту

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Підтримка Європейською Комісією виходу цієї публікації не означає підтримки змісту, який відображує позицію лише авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься у посібнику.

ПЕРЕДМОВА

Пропонований до уваги читача навчальний посібник підготовано в рамках ERASMUS+ проєкту CRIMHUM, метою якого є створення комплексної, заснованої на правах людини програми підготовки фахівців для кримінального правосуддя – майбутніх суддів, прокурорів, слідчих – шляхом модернізації спеціалізованих магістерських програм.

Через модернізацію магістерських програм освітній проєкт CRIMHUM має на меті формування у фахівців у сфері кримінальної юстиції навичок, які допоможуть їм ефективно реагувати на динамічно змінювані умови сучасних демократичних суспільств. Однією з таких умов є тенденція до все більш охоплюючої та стрімкої інформатизації, яка трансформує усі сфери життєдіяльності.

Можна з упевненістю констатувати, що левова частка життя кожної людини пов'язана з операціями, які здійснюються у кіберпросторі. Цифрова грамотність та кібергігієна стали невід'ємними складовими базових навиків сучасної людини. Окрім приватного життя, цифровізація все більш суттєво впливає на прийняття управлінських рішень та функціонування усіх суспільних інституцій, в тому числі державно-владних. Не є винятком і сфера кримінальної юстиції, яка стикнулася з необхідністю ефективних відповідей на нові виклики: динамічну появу нових видів кіберзагроз, і, як результат, потребу в адаптації існуючих та розробки нових методик розслідування кримінальних правопорушень, які вчиняються у кіберпросторі або з його використанням. Оскільки кіберзлочини вчиняються

як правило у віртуальному середовищі, специфіку мають сліди, які вони залишають, а отже виникають процесуальні особливості їх виявлення та фіксації та необхідність визначення місця нових форм представлення інформації у системі доказів та доказування.

У реаліях сьогодення кіберзлочини посягають вже не тільки на права і свободи окремих громадян чи заподіюють шкоду безпеці об'єктів критичної інфраструктури держави. В умовах сучасних глобалізаційних процесів та процесу інформатизації суспільства, кібербезпека стає пріоритетним напрямом національної безпеки кожної держави. Саме тому концептуальна модернізація процесу підготовки студентів-магістрів – майбутніх суддів, прокурорів, слідчих є неможливою без розвитку у студентів предметних компетентностей, спрямованих на попередження, виявлення і фіксацію, а також розслідування особливого виду кримінальних правопорушень – кіберзлочинів. Досягненню цієї мети сприяє цей навчальний посібник – «Кіберзлочинність та електронні докази».

Структуру цього навчального посібника побудовано так, щоб спрямувати студента у напрямку від оволодіння та засвоєння кримінологічних характеристик та особливостей кіберзлочину та кіберзлочинності до вивчення запобігання цій категорії кримінальних правопорушень та особливостей методики їх розслідування. У завершальному розділі цього посібника викладено матеріал, що стосується правової природи та поняття електронних доказів, способів їх збирання та правильного процесуального оформлення результатів процесуальних дій, спрямованих на їх збирання.

Ольга Денькович,
кандидат юридичних наук, доцент

РОЗДІЛ 1

КІБЕРЗЛОЧИННІСТЬ: ПОНЯТТЯ, ВИДИ ТА ЗАПОБІГАННЯ

1.1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів.
1.2. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.
1.3. Детермінанти та основні напрями запобігання кіберзлочинності.

1.1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів

Проаналізуйте наведені нижче ситуації та визначте, який з наведених проявів кримінально протиправної поведінки є кіберзлочином і чому?

КЕЙС 1. *Винний в Інтернеті знайшов програмне забезпечення, що призначене для віддаленого керування доступом до персонального комп'ютера, і завантажив його на свій комп'ютер. Потім за допомогою цього програмного забезпечення створив вірусне програмне забезпечення, що дозволяло у разі його завантаження отримати віддалений доступ до іншого комп'ютера та керування ним. Після чого він виклав це вірусне програмне забезпечення як додаток до інтернет-ігор у вигляді архівного файлу на одному із сайтів, який створив. У подальшому цей файл з вірусним програмним забезпеченням завантажив один із користувачів мережі Інтернет.*

КЕЙС 2. *Винний, з допомогою розрізаної двохсотгривневої купюри, нитки та клейкої стрічки, виготовив спеціальний пристрій, з допомогою якого він однією і тією ж купюрою неодноразово через термінал он-лайн платежів поповнював свій мобільний рахунок. Отримані в такий спосіб кошти він перераховував на електронні гаманці й банківські картки, а потім знімав з них готівку. У такий спосіб винний вчинив 50 кримінальних правопорушень і заподіяв матеріальну шкоду на суму 50 тисяч гривень.*

1 **Доктринальні підходи до визначення кіберзлочинності.** Кіберзлочинність є однією із основних проблем у правоохоронній сфері, яка турбує сучасні розвинуті держави. Така підвищена зацікавленість до явища кіберзлочинності невипадкова, а зумовлена, зокрема, поширеністю кримінальних правопорушень цього виду. У звіті Європейського поліцейського управління (Європол) "Оцінка загрози організованої злочинності в Інтернеті" за 2016 рік зазначено, що статистичні дані окремих держав-членів Європейського Союзу (ЄС) свідчать про те, що кількість зареєстрованих кіберзлочинів досягає або ж навіть перевищує кількість "традиційних" злочинів. За даними цього ж звіту Україна є лідером серед інших держав Європи, які не є членами ЄС, за кількістю розташованої на її території командної та управлінської інфраструктури кіберзлочинності.

2 За даними соціологічного опитування українських організацій про вплив економічних злочинів на бізнес під назвою "Всесвітній огляд економічних злочинів", яке всесвітньовідома міжнародна консалтингова компанія *PricewaterhouseCoopers* (*PwC*) проводить один раз на два роки, з 2011 року кіберзлочини входять у п'ятірку найпоширеніших економічних злочинів, які завдають матеріальних збитків українським компаніям. За даними цього дослідження у 2016 році кіберзлочини посідали друге місце, а у 2018 році – п'яте, серед інших економічних

злочинів, які вчиняються в економічній сфері. У 2020 році кіберзлочини входили у Топ 5 видів шахрайства.

Тенденції до зростання кількості кіберзлочинів 3
обумовлюють підвищену зацікавленість світового наукового співтовариства до вивчення проблем кіберзлочинності та напрямів боротьби з нею.

Будь-якому видовому поняттю, відповідно до правил 4
формальної логіки, властиві усі ознаки родового поняття, з якого воно виділене. Родовим до кіберзлочинності є злочинність як така, а тому загальні ознаки злочинності властиві і кіберзлочинності як її виду. Окрім того, кіберзлочинність характеризується властивими лише їй ознаками, які відрізняють її від інших видових до «злочинності» понять.

Сучасна кримінологія характеризується плюралізмом 5
методологічних підходів до визначення тих чи інших понять, у тому числі і злочинності. Можна виділити біологічний, соціальний, психологічний та статистичний підходи[1]. Саме останній із названих – статистичний підхід, домінує в українській кримінології. У межах цього підходу злочинність визначається як сукупність кримінальних правопорушень, вчинених у певний період часу в певному суспільстві. Як наслідок, саме статистичний підхід є найбільш поширеним у вітчизняній кримінології в інтерпретації видового до злочинності поняття – кіберзлочинність.

Зокрема, у Великій українській юридичній енциклопедії, 6
яка є систематизованим зводом знань і досягнень сучасних наук, у тому числі кримінології, під кіберзлочинністю пропонують розуміти сукупність злочинів, що вчиняються за допомогою комп'ютерної мережі чи мережі електрозв'язку,

---

[1] *Куц В.* Поняття злочинності. *Науковий часопис Національної академії прокуратури України*. 2016. № 2 С. 34–39. URL : http://www.chasopysnapu.gp.gov.ua/ua/pdf/10-2016/02/kuts.pdf

у межах комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку, чи проти комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку[2].

7 Під кіберзлочинністю М. О. Кравцова пропонує розуміти 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[3].

8 Зокрема, Г. М. Чернишов кіберзлочинність визначає як «явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку»[4].

9 Окрім відсутності єдності підходів до змісту поняття кіберзлочинність, у науці кримінології не досягнуто консенсусу і щодо терміна, яким позначається це явище. Так, кіберзлочинність застосовують поряд із такими термінами, як комп'ютерна злочинність, злочини у сфері високих технологій, інформаційні злочини, злочини у сфері комп'ютерної безпеки, злочини у сфері комп'ютерної інформації тощо. У вітчизняній кримінології переважно як синонім до слова «кіберзлочинність» використовують термін «комп'ютерна злочинність». Однак є й інші підходи до співвідношення цих понять. Н. В. Савчук уважає,

---

[2] *Бабанін С. В.* Кіберзлочинність, Комп'ютерна злочинність. *Велика українська юридична енциклопедія* : у 20 т. Харків, 2019. Том 18. С. 207.

[3] *Кравцова М. О.* Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. … канд. юрид. наук: 12.00.08. Харків, 2016. С. 12.

[4] *Чернишов Г. М.* Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. № 3. С. 160.

що кіберзлочинність є ширшим поняттям, ніж комп'ютерна злочинність. На думку цього автора, кіберзлочинність охоплює «комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо»[5]. Такої ж позиції дотримується І. В. Діордіца[6].

Законодавче визначення поняття кіберзлочинності. Спробу поставити крапку у зазначених дискусіях зробив законодавець. Зокрема, Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року № 2163-VIII у національне законодавче поле були введені такі поняття, як «кіберзлочинність», «кіберзлочин», «комп'ютерний злочин». Зокрема, законодавець сприйняв домінуючий у кримінології статистичний підхід до розуміння злочинності і визначив кіберзлочинність як сукупність кіберзлочинів (п. 9 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року № 2163-VIII), а терміни «кіберзлочин» та «комп'ютерний злочин» використав як взаємозамінні та однакові за змістом. Тож, відповідно до чинного законодавства, поняття кіберзлочинність та комп'ютерна злочинність є синонімічними.

Водночас недоліком вказаного законодавчого визначення кіберзлочинності (так само як і визначення злочинності в межах статистичного підходу) є те, що воно відображає НЕ сутність та зміст поняття (тобто сукупність його істотних, необхідних і достатніх ознак), а його обсяг (тобто вказує на об'єкти, які цим поняттям охоплюються). Вказане законодавче та схожі

---

[5] *Савчук Н. В.* Кіберзлочинність: зміст та методи боротьби. С. 338. URL : http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf

[6] *Діордіца І. В.* Поняття та зміст кіберзлочинності. URL : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/

за методологічними підходами доктринальні кримінологічні визначення кіберзлочинності виходять з того, що цей вид злочинності є сукупністю кримінальних правопорушень, їх арифметичною сумою. Різняться вони у тому, які саме кримінальні правопорушення потрібно включати в обсяг цього поняття, тобто якими ознаками характеризується кіберзлочин як одиничний елемент вказаної суми, чим він відрізняється від інших видів кримінальних правопорушень.

12 **Ознаки кіберзлочину.** В основу належності кримінального правопорушення до кіберзлочину (комп'ютерного кримінального правопорушення) закладають, зокрема, такі критерії:

- комп'ютерними називають ті кримінальні правопорушення, які законодавець об'єднав у Розділі XVI Особливої частини КК (С. В. Бабанін, М. О. Кравцова[7]). Умовно цей підхід можна назвати позитивістським, а ознакою, яка відрізняє кіберзлочини від інших та об'єднує їх у певну групу є родовий об'єкт цих кримінальних правопорушень;
- комп'ютерним є кримінальне правопорушення, яке вчиняється з використанням ЕОМ, телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку (П. Д. Біленчук, М. А. Зубань[8], О. М. Литвинов та М. О. Кравцова[9]). Тобто, на думку цих авторів, кіберзлочин відрізняється від інших видів кримінальних правопорушень знаряддям вчинення, яким є певна

[7] *Кравцова М. О.* Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 157. URL : http://dspace.univd.edu.ua/xmlui/handle/123456789/3848

[8] *Біленчук П. Д., Зубань М. А.* Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посібник. Київ : Українська академія внутрішніх справ, 1994. С. 6.

[9] *Кравцова М. О., Литвинов О. М.* Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. С. 19.

комп'ютерна система, комп'ютерна мережа чи мережа електрозв'язку;
- комп'ютерним є кримінальне правопорушення, предметом якого є комп'ютерна інформація, що обробляється в ЕОМ, АС, комп'ютерних мережах чи мережах електрозв'язку (А. А. Музика, Д. С. Азаров);
- кіберзлочином є кримінальне правопорушення, в якому комп'ютер є або предметом кримінального правопорушення, або знаряддям, або способом його вчинення (Н. В. Савчук[10]);
- кіберзлочини – це кримінальне правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення (Г. М. Чернишов[11]);
- кіберзлочин (комп'ютерне кримінальне правопорушення) – це 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 (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року № 2163-VIII).

Недоліки законодавчого визначення кіберзлочину в Україні. У вказаному вище законодавчому визначенні кіберзлочину відображені окремі загальні ознаки кримінального правопорушення, названі у ст. 11 КК України (суспільна небезпечність, діяння, винність, кримінальна протиправність), а також специфічні ознаки, які відрізняють цей вид кримінальних

13

[10] *Савчук Н. В.* Кіберзлочинність: зміст та методи боротьби. С. 338. URL : http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf

[11] *Чернишов Г. М.* Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. № 3. С. 158–162.

правопорушень від інших: до кіберзлочинів належать ті, які вчиняються у кіберпросторі та/або з його використанням. Водночас вказана законодавча інтерпретація кіберзлочину містить низку недоліків: по-перше, не охоплює такої загальної ознаки кримінального правопорушення, як вчинене суб'єктом кримінального правопорушення; по-друге, суперечить ч. 3 ст. 3 КК України в частині такої ознаки, як кримінальна протиправність; по-третє, це визначення не враховує змін, внесених до КК України Законом № 2617-VIII від 22.11.2018 року «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень». Зокрема, ч. 3 ст. 3 КК України є законодавчим відображенням однієї зі складових принципу законності – *nullum crimen, nulla poena, sine lege*, яка полягає у тому, що немає кримінального правопорушення без вказівки про це в законі. У ч. 3 ст. 3 КК України визначено, що кримінальна протиправність діяння визначається лише КК. Однак у законодавчому визначенні кіберзлочину вказано, що до них належать як ті діяння, відповідальність за які передбачена у КК, так і ті, що визнані злочином міжнародними договорами України. Тобто законодавець НЕ обмежує кіберзлочини лише злочинами, які є в Розділі XVI Особливої частини чи в КК загалом. До кіберзлочинів належать також і ті, які є злочинами відповідно до міжнародних договорів України. По-третє, законодавче визначення кіберзлочину не враховує того факту, що до цієї групи кримінальних правопорушень належать не тільки злочини, а ті, які з огляду на санкцію відповідної статті КК України є кримінальними проступками.

14 Визначення кіберзлочину, яке є у Законі України «Про основні засади забезпечення кібербезпеки України», обмежує кіберзлочини лише тими, які вчиняються у кіберпросторі та/або з його використанням, і, як наслідок, необґрунтовано звужує

обсяг поняття кіберзлочин та кіберзлочинність. Законодавче визначення кіберзлочину обумовлене метою, з якою прийнято вказаний законодавчий акт, – регулювання порядку кіберзахисту визначених цим Законом об'єктів. Об'єктами такого кіберзахисту, відповідно до ч. 2 ст. 4 Закону, є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
2) об'єкти критичної інформаційної інфраструктури;
3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Цей Закон не поширюється на:

1) відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;
2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;
3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші вебресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;
4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними

мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем) (ч. 1 ст. 2 Закону).

16 Тож, кримінальні правопорушення, які вчиняють у межах вказаних суспільних відносин чи проти вказаних об'єктів зі застосуванням інформаційних технологій, не належать до кіберзлочинів. Наприклад, не можна розглядати як кіберзлочин у сенсі вказаного Закону незаконне одержання доступу до інфраструктури компанії *SoftServe*, яке відбулося 01 вересня 2020 року, в результаті якого декілька серверів компанії перестали працювати, а в мережі згодом з'явилися репозиторії проєктів, які *SoftServe* розробляла для своїх клієнтів, персональні дані працівників та клієнтів компанії[12]. Вчинити вказане кримінальне правопорушення без застосування інформаційних технологій – неможливо, а тому, очевидно, таке кримінальне правопорушення має входити в обсяг поняття кіберзлочинність. Вказане дає підстави стверджувати, що кримінологічне визначення кіберзлочину має бути ширшим, ніж те, яке передбачене у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України». Окрім кримінальних правопорушень, які вчиняються у кіберпросторі та/або з його використанням, воно повинно охоплювати інші кримінальні правопорушення, які пов'язані з іншими способами застосуванням корисних властивостей інформаційних технологій для заподіяння шкоди об'єкту кримінально-правової охорони. Більш детально розглянемо це питання згодом у межах цього підрозділу.

17 **Історія зародження поняття кіберзлочину.** Зрештою, відсутність єдності розуміння понять кіберзлочинності та кіберзлочину ілюструє загальносвітові тенденції. Зародження окремої категорії кіберзлочинів пов'язане з розвитком

[12] Хакери «злили» дані клієнтів великої української ІТ-компанії. *Економічна правда*. URL : https://www.epravda.com.ua/news/2020/09/17/665235/

комп'ютерних технологій. Запровадження та поширення комп'ютерів на основі транзисторів у 1960-х роках створило передумови для появи нового виду злочинності. На цьому ранньому етапі кіберзлочини не виділялись в окрему групу, а обговорювались у контексті кримінальних правопорушень проти власності як правопорушення, які заподіюють фізичну шкоду комп'ютеру або розміщеній у ньому інформації.

18 Однак вже у 1970-х роках акценти у визначенні кіберзлочину зміщуються. Незаконне використання комп'ютерних систем, маніпуляції з цифровими даними та перші шахрайські дії, вчинені з використанням комп'ютера, спричинили жваві дискусії у науковому середовищі щодо кримінально-правової оцінки таких діянь. У 1977 році у США було прийнято Федеральний закон про захист комп'ютерних систем, а пізніше інші держави також намагалися привести своє законодавство у відповідність до нових реалій та криміналізувати суспільно-небезпечні діяння, які вчинялися з використанням комп'ютерної системи чи мережі або у ній. Поява глобальної мережі Інтернет ще більше загострила проблему кіберзлочинності й у 1989 році Європейський комітет з проблем злочинності Ради Європи надав низку рекомендацій національним законодавцям з приводу того, які діяння з комп'ютерними системами варто криміналізувати. А у 1994 році у межах ООН був розроблений Посібник щодо попередження та контролю за комп'ютерними злочинами, у якому констатовано, що міжнародного визначення поняття комп'ютерного злочину наразі не досягнуто. І хоча з моменту видання цього підручника минуло більше 20-ти років, єдиного уніфікованого міжнародного визначення поняття кіберзлочину досі немає.

19 **Поняття кіберзлочину у зарубіжній кримінології.** У 2000 році X Міжнародний конгрес ООН з боротьби зі злочинністю та поводження з правопорушниками сформулював вузький

та широкий підходи до визначення поняття кіберзлочину. Згідно із першим – вузьким – поняття кіберзлочину охоплює будь-яку незаконну поведінку, яка реалізується за допомогою електронних операцій і спрямована проти безпеки комп'ютерних систем та інформації, яка обробляється у них. Під кіберзлочином у широкому розумінні Конгрес запропонував розуміти будь-яку незаконну поведінку, яка здійснюється за допомогою або щодо комп'ютерної системи чи мережі, включаючи такі злочини, як незаконне заволодіння, пропозиція або поширення інформації через комп'ютерну систему або мережу.

20 Найбільш поширеним, простим і часто вживаним у сучасній зарубіжній кримінології є визначення кіберзлочину як будь-якого незаконного діяння, у якому комп'ютерна система чи мережа є знаряддям, ціллю або місцем злочинної діяльності. В Оксфордському словнику під кіберзлочином запропоновано розуміти будь-яку злочинну діяльність, яка здійснюється за допомогою комп'ютерів або ж Інтернету. В іншому кримінологічному дослідженні акцентовано на тому, що кіберзлочином може бути лише така злочинна діяльність, у якій комп'ютер або комп'ютерна мережа є основним засобом вчинення злочину чи порушення спеціальних правил (*Nir Kshetri. The Global Cybercrime Industry*). Однак цілком заслужено такі широкі визначення поняття кіберзлочину піддаються критиці. У такому розумінні кіберзлочином доцільно визнавати, наприклад, тілесні ушкодження, знаряддям вчинення яких є клавіатура до комп'ютера.

21 Автори іншого, вужчого підходу до розуміння поняття кіберзлочину намагаються врахувати об'єкт та/або засоби цього кримінального правопорушення і пропонують, наприклад, такі визначення кіберзлочину: опосередкована комп'ютером діяльність, яка є або незаконною або вважається незаконною певними сторонами і яка здійснюється через глобальні електронні

мережі; будь-які злочинні діяння, які вчиняються за допомогою комп'ютера і посягають на інформацію, яка обробляється з комп'ютерній системі. Але знову ж такі визначення далекі від досконалості, адже не охоплюють усіх можливих проявів злочинної діяльності у сфері комп'ютерних технологій. Критики вузького підходу аргументують свою позицію тим, що поза його межами залишаються ті види кіберзлочинів, які визначені такими міжнародними договорами, зокрема Конвенцією Ради Європи про кіберзлочинність від 23.11.2001 року. Саме ця Конвенція є ключовою у сфері діяльності правоохоронних органів та співпраці держав щодо боротьби з кіберзлочинністю. Підтвердженням цьому є факт її підписання та ратифікації також і тими державами, які не є членами Ради Європи (наприклад, Канада, Ізраїль, Південна Африка, США).

Конвенція про кіберзлочинність не містить визначення 22
поняття кіберзлочину, однак наводить перелік та класифікацію кіберзлочинів, за які на національному рівні пропонується встановити кримінальну відповідальність. Саме цей перелік є вихідним у визначенні поняття кіберзлочину у зарубіжній кримінології. Зокрема, у вказаному міжнародному документі до кіберзлочинів запропоновано віднести такі групи посягань:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем (наприклад, незаконний доступ, нелегальне перехоплення);
2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами);
3) правопорушення, пов'язані зі змістом (наприклад, дитяча порнографія, расизм і ксенофобія);
4) правопорушення, пов'язані з порушенням авторських та суміжних прав.

Використана у Конвенції про кіберзлочинність класифікація 23
відповідних злочинів теж не є досконалою, адже групи

виділяються за різними критеріями. Однак попри всі недоліки важливість цього документа є беззаперечною, а належну імплементацію його положень до національного законодавства держав-підписантів цієї Конвенції віднесено до основних рекомендацій державам за результатами дослідження Європолу у 2016 році.

24 На підставі наведеного можна стверджувати, що у зарубіжній кримінології домінує функціональний підхід до визначення поняття кіберзлочину, тобто вчені концентруються не на формулюванні визначення цього поняття, а на формулюванні переліку кібердіянь, які є суспільно небезпечними і, відповідно, мають бути криміналізовані. Такий самий підхід використано й у Конвенції про кіберзлочинність: основний акцент зроблено не на роз'ясненні змісту понять «кіберзлочин» та «кіберзлочинність», а на встановленні їх обсягу – тих конкретних діянь, які належать до кіберзлочинів і, відповідно, формують обсяг поняття кіберзлочинності. З огляду на міжнародний характер положень Конвенції про кіберзлочинність така тенденція є виправданою й обумовлена необхідністю ефективної відповіді правоохоронних органів на національному та міжнародному рівнях на динамічно зростаючу кількість кіберзлочинів, налагодженню співпраці щодо розслідування цих злочинів та притягнення винних до кримінальної відповідальності.

25 **Доктринальні підходи до питання про кримінологічну однорідність кіберзлочинів.** У кримінології відсутній єдиний критерій для поділу злочинності на види. Кримінологічні класифікації злочинності проводяться за різними критеріями: за соціальним змістом мотивації злочинної поведінки, за критерієм спрямованості заходів запобігання, за сферою вчинення, за формою вини, за змістом злочинної діяльності тощо. Підставою для виділення виду злочинності є кримінологічна однорідність злочинної поведінки.

Б. М. Головкін слушно стверджує, що класифікація злочинності може бути природною, яка проводиться за якісними (найбільш істотними) ознаками, та штучною, яка допускає використання неістотних ознак, кількість яких може бути доволі великою. Як стверджує цей автор, при проведенні природної класифікації використовуються критерії, що дають змогу розподілити явище на великі однорідні групи, окреслити сферу його існування, показати форми прояву, виразити соціальний зміст, розкрити зв'язки з іншими спорідненими явищами і поняттями одного класу[13]. Отже, природна класифікація злочинності є первинною до штучної. Кримінологічна однорідність проявів кримінально протиправної поведінки у межах природної класифікації злочинності обумовлюється спільністю найбільш загальних ознак кримінальних правопорушень, їх взаємозв'язків і залежностей. Це, до прикладу, може бути мотивація кримінально протиправної поведінки, зміст такої поведінки тощо. Кримінологічна однорідність проявів кримінально протиправної поведінки є передумовою схожості їх детермінуючого комплексу та, відповідно, системи заходів запобігання певному виду злочинності.

У кримінології відсутній єдиний підхід до того, чим схожі кіберзлочини та в чому полягає їх кримінологічна однорідність. Частина вчених пов'язує кіберзлочини зі специфічним предметом кримінально протиправної поведінки та зі способом вчинення кримінальних правопорушень, якими є комп'ютер чи комп'ютерні дані[14], інші – з місцем їх вчинення (зокрема,

26

[13] *Головкін Б. М.* Види злочинності. *Журнал східноєвропейського права*. 2015. №. 18. С. 14–21. URL : http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

[14] *Савчук Н. В.* Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки : зб. наук. праць. Київ : Вид. поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338. URL : http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf

віртуальним простором)[15], зі сферою злочинних проявів (вчиняються у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку)[16], з родовим об'єктом цих кримінальних правопорушень[17], зі знаряддям вчинення кримінальних правопорушень (комп'ютерна техніка) та середовищем їх вчинення[18], зі середовищем (кіберпростір), предметом (метою) посягання та/або способом вчинення[19]. Кіберзлочин також називають видом економічних злочинів[20].

27 Наведені підходи можна об'єднати у три групи. Першу групу утворюють ті, відповідно до яких об'єднуючою ознакою кіберзлочинів є те, що комп'ютерна система є предметом, знаряддям або способом вчинення кримінально протиправного діяння. До другої групи належать підходи, за якими кіберзлочини відрізняються від інших за сферою їх вчинення (якою називають кіберпростір або віртуальний простір). До третьої групи належать підходи, які інтегрують

---

[15] *Буяджи С. А.* Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : автореф. дис. ... канд. юрид. наук: 12.00.01 – Теорія та історія держави і права; історія політичних і правових учень. Івано-Франківськ, 2018. С. 6.

[16] *Головкін Б. М.* Види злочинності. *Журнал східноєвропейського права*. 2015. №. 18. С. 17. URL : http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

[17] *Кравцова М. О.* Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 157. URL : http://dspace.univd.edu.ua/xmlui/handle/123456789/3848

[18] *Бутузов В.* Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія]. Київ : КИТ, 2010. С. 119.

[19] *Чернишов Г. М.* Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. № 3. С. 160.

[20] *Васильковський І. І.* Поняття "кіберзлочинність" та "кіберзлочини": стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2 (10–11). С. 278.

перші два підходи, і стверджують, що кримінологічну однорідність кіберзлочинів обумовлює сукупність двох ознак: сфера їх вчинення та знаряддя чи способи, які використовує злочинець. Спробуємо дати відповідь на питання про те, яка з позицій правильна, проаналізувавши механізм вчинення конкретних кіберзлочинів та виявивши спільні ознаки цих проявів кримінально протиправної поведінки.

Отже, спільною, інтегруючою та, одночасно, найбільш 28
істотною ознакою проявів кримінально протиправної поведінки, які належать до кіберзлочинів, є те, що у процесі їх вчинення задіяні інформаційні (комп'ютерні) системи. Ці системи є або об'єктом кримінально протиправної поведінки, тим, проти чого спрямоване конкретне діяння винного, або використовуються у процесі кримінально протиправної діяльності, як, зокрема, знаряддя, засіб, місце, спосіб вчинення суспільно небезпечного діяння. Ця ознака відрізняє їх від інших видів кримінально протиправної поведінки, та, відповідно, дозволяє виділити цю групу кримінально протиправної поведінки в окремий вид злочинності – кіберзлочинність. Тобто у процесі вчинення (скоєння) кіберзлочину злочинець використовує особливі можливості, властивості, якими наділені інформаційні (комп'ютерні) системи для реалізації свого кримінально протиправного умислу.

Види кіберзлочинів. Сфера вчинення (якою у вітчизняній 29
кримінології називають кіберпростір, віртуальне середовище) кримінально протиправних діянь, які належать до кіберзлочинів, не може виконувати роль кримінологічно однорідної ознаки, адже окремі кіберзлочини вчиняються і поза кіберпростором, але в межах інформаційної (комп'ютерної) системи. Слушним є зауваження М. О. Кравцової, що визначення кіберзлочинності через поняття кіберпростір не є достатнім для позначення її

обсягу[21]. Адже кіберпростір – це 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 (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»). Тому якщо кіберпростір визнавати об'єднуючою ознакою кіберзлочинів, то вчинення кримінально протиправних діянь з використанням інформаційних (комп'ютерних) систем, які під'єднані до локальних мереж, або ж не під'єднані до жодної мережі, не є кіберзлочинами. Тобто за цим підходом втручання в інформаційну систему (наприклад, смартфон), який не підключено до будь-якої мережі, вчиняється поза кіберпростором і, відповідно, не є кіберзлочином. Необґрунтованість такого підходу очевидна.

30 Більшість кримінальних правопорушень можуть бути вчинені з використанням інформаційних (комп'ютерних) систем. Однак для окремих із них використання таких систем є внутрішньо іманентною ознакою кримінально протиправної поведінки. Тобто вчинити ці кримінальні правопорушення без використання інформаційної (комп'ютерної) мережі неможливо з огляду на специфіку об'єкта (предмета) кримінально протиправного посягання. Це, наприклад, несанкціоноване втручання в роботу комп'ютерної системи, рефайлінг, розповсюдження вірусів та шкідливого програмного забезпечення (мальваре), DDoS атаки.

31 Водночас інформаційна (комп'ютерна) система може використовуватись і для вчинення так званих «традиційних»

[21] *Кравцова М. О.* Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 157. URL : http://dspace.univd.edu.ua/xmlui/handle/123456789/3848

кримінальних правопорушень, які, за загальним правилом можуть бути вчинені і без використання такої системи. Наприклад, у винного виник умисел на заволодіння грошовими коштами потерпілого, розміщеними на банківському рахунку останнього. Він може вчинити це кримінальне правопорушення у традиційний спосіб, у «реальному світі», або ж скористатися можливостями, які дають інформаційні системи і вчинити цей злочин з використанням «віртуального світу». В обох випадках умисел винного спрямований на заволодіння чужим майном і для того, щоб реалізувати цей умисел, винному потрібні персональні дані потерпілого та реквізити його банківського рахунку. Одержати цю інформацію він може, наприклад, викравши гаманець з банківською карткою, тобто діяти у «реальному світі». Або ж винний може обрати інший спосіб і використати веб-сайт, через який «виманити» реквізити платіжної картки потерпілого під виглядом надання послуг, що не існують (наприклад, поповнення мобільного рахунку, переказів з картки на картку) або ж поза згодою потенційного потерпілого завантажити на його комп'ютер програму keylogger, яка реєструє кожне натиснення на клавішу клавіатури комп'ютера, записує необхідну інформацію та пересилає її злочинцям. У кримінології такий спосіб одержання персональних даних називають фішингом. В останньому випадку свій кримінально протиправний умисел винний реалізує з використанням «віртуального світу». Також до цієї групи кіберзлочинів можна віднести, наприклад, порушення авторських та суміжних прав, розповсюдження відеопродукції порнографічного характеру.

Залежно від значення інформаційної системи у механізмі 32
реалізації кримінально протиправної діяльності можна виділити такі види кіберзлочинів:

– кіберзлочини у власному розумінні, тобто ті, які неможливо вчинити без використання інформаційних

(комп'ютерних) систем. Це прояви кримінально протиправної поведінки, які спрямовані проти інформаційних (комп'ютерних) систем або проти об'єктів чи предметів, які існують, зберігаються, передаються, обробляються у них (комп'ютерні програми, інформація тощо);

– пов'язані з інформаційними (комп'ютерними) системами кримінальні правопорушення, тобто ті, прояви кримінально протиправної поведінки, які вчиняються з використанням цих систем, але, водночас, можуть вчинятися і без них. Ці прояви кримінально протиправної поведінки можуть полягати, зокрема, у тому, що саме кримінально протиправне діяння вчиняється у кіберпросторі з використанням інформаційних технологій або ж інформаційні технології чи кіберпростір використовуються злочинцем на інших етапах реалізації кримінально протиправної діяльності як, наприклад, знаряддя чи засіб вчинення діяння.

33 Перша група кіберзлочинів охоплює ті прояви кримінально протиправної поведінки, які спрямовані проти інформаційних (комп'ютерних) систем, а точніше проти порядку їх функціонування. Тобто йдеться не про фізичне знищення чи пошкодження, наприклад, комп'ютера, планшета чи смартфона, як матеріального об'єкта. Сутнісною ознакою юридичних визначень інформаційної (комп'ютерної) системи є її призначення: автоматична обробка, зберігання, передача та отримання комп'ютерних даних чи інформації. Вчиняючи кіберзлочин винний спрямовує своє діяння на заподіяння істотної шкоди тим процесам, які відбуваються усередині інформаційної системи і забезпечують виконання нею свого призначення, або ж проти того, з чим працюють інформаційні системи – комп'ютерної інформації. При цьому він використовує

самі інформаційні (комп'ютерні) системи у механізмі реалізації кримінально протиправного посягання.

Кримінологічна особливість першої виділеної групи 34
кіберзлочинів полягає в тому, що вчинення більшості з них вимагає достатньо глибоких спеціальних знань, розуміння особливостей функціонування та навичок використання інформаційних технологій. Очевидно, що реалізувати DDoS-атаку може лише та особа, яка має значно глибші та ґрунтовніші знання у сфері інформаційних технологій, ніж та, яка завантажує файл з відеопродукцією порнографічного характеру. Кіберзлочини у власному розумінні відрізняються від кіберзлочинів, що пов'язані з інформаційними технологіями, також і тим, що кримінально протиправна поведінка винної особи спрямована проти порядку функціонування інформаційної (комп'ютерної) системи або інформації, що обробляється у ній. Тобто інформаційна технологія є об'єктом або предметом кримінально протиправної поведінка особи. Характеристики цих об'єкта та предмета обумовлюють і вибір знарядь чи способів заподіяння шкоди, якими теж є інформаційна система. Об'єктом кіберзлочинів, які пов'язані з інформаційними (комп'ютерними) системами, є не сама система, а інші цінності – власність, приватне життя особи, моральність, авторські та суміжні права тощо. Для заподіяння шкоди цим об'єктам злочинець обирає специфічні знаряддя чи засоби – інформаційну систему.

Особливі можливості інформаційних систем, які 35
використовуються злочинцем у процесі вчинення кримінального правопорушення, обумовлюють специфіку кіберзлочинності. Зокрема, суспільно небезпечні наслідки кіберзлочину можуть наставати за тисячі кілометрів від місця вчинення суспільно небезпечного діяння. З огляду на доступність інформаційних технологій можливість вчинити кіберзлочин має широке коло

осіб, але часто застосування таких інформаційних технологій потребує спеціальних знань. Зрештою вчинення кримінального правопорушення з використанням корисних властивостей інформаційних технологій зумовлює необхідність застосування специфічних методів їх розслідування. Без наявності спеціальних знань доволі складно (а часом неможливо) виявити, зафіксувати і вилучити криміналістично значущу інформацію про кіберзлочин. Кіберзлочинність характеризується високим рівнем латентності кіберзлочинності та швидким зростанням кількості кіберзлочинів, що пов'язане зі все більшим розповсюдженням Інтернету в різних сферах і здешевлення Інтернет-послуг. Усі ці ознаки обумовлюють особливі способи запобігання і попередження цього виду злочинності.

За даними кіберполіції у 2018 році поліцейські виявили 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій, серед них 680 – у сфері протиправного контенту, 2 398 – у сфері платіжних систем, 1 598 – у сфері е-комерції, 1 325 – у сфері кібербезпеки. У 2018 році працівники поліції викрили більше 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Згідно зі статистичними даними, більша частина підозрюваних (67 %) – чоловіки, серед яких 39 % у віці від 25 до 40 років[22]. У звіті Голови Національної поліції України про результати роботи відомства у 2019 році ключовими «класичними» кіберзлочинами у 2019 році були розповсюдження комп'ютерних вірусів, шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, викрадення інформації, онлайн-торгівля наркотиками та зброєю, формування у дітей суїцидальної поведінки. У цьому році було викрито 4 263 кіберзлочинів, з яких 332 – у сфері протиправного контенту, 1 641 – у сфері платіжних систем, 744 –

[22] Підсумки 2018 року в цифрах. Кіберполіція. Національна поліція України. URL : https://cyberpolice.gov.ua/results/2018/

у сфері е-комерції, 1 494 – у сфері кібербезпеки[23]. Якщо взяти до уваги, що всього у 2018[24] та 2019[25] роках в Україні було обліковано 487 133 та 444 130 кримінальних правопорушень відповідно, то питома вага кіберзлочинів у загальній структурі злочинності є незначною та становить 1,23 % у 2018 році та 0,95 % у 2019 році. Однак такі відсоткові показники не ілюструють справжнього стану речей, що пов'язано з високим рівнем латентності кіберзлочинів.

Для вирішення наведеного на початку підрозділу казусу *необхідно проаналізувати чи в описаних у казусі ситуаціях є ознаки кіберзлочину. Спільною та найбільш істотною ознакою усіх проявів кримінально протиправної поведінки, які належать до кіберзлочинів, є те, що у процесі їх вчинення задіяні інформаційні (комп'ютерні) системи. Ці системи є або об'єктом кримінально протиправної поведінки, тобто тим, проти чого спрямоване конкретне діяння винного, або ці системи використовуються у процесі кримінально протиправної діяльності, як, зокрема, знаряддя, засіб, місце, спосіб вчинення суспільно небезпечного діяння. Тобто у процесі вчинення (скоєння) кіберзлочину винний використовує особливі можливості, властивості, якими наділені інформаційні (комп'ютерні) системи для реалізації свого кримінально протиправного умислу.*

Обставини справи, описані у першій фабулі, дають підстави стверджувати, що суспільно небезпечне діяння винного спрямоване на те, щоб отримати несанкціонований доступ до комп'ютерної системи – комп'ютера користувача, за допомогою вірусного програмного забезпечення. Тобто об'єктом кримінально протиправної поведінки винного є комп'ютерна

[23] Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL : https://www.npu.gov.ua/assets/userfiles/files/zvity/zvit_NPU_2019.pdf

[24] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

[25] Там само.

система потерпілого, доступ до якої винний намагався отримати, використовуючи ті можливості, які надають комп'ютерні програми (в цьому випадку вірусне комп'ютерне забезпечення). Отже, описану у першій фабулі кримінально протиправну поведінку винного можна віднести до кіберзлочинів.
Натомість за обставинами справи, описаними у другій фабулі, винний заподіяв шкоду об'єкту кримінально-правової охорони, а саме праву власності, шляхом зовнішнього фізичного втручання в роботу комп'ютерної системи (банкомату) за допомогою спеціального пристрою, який не є інформаційною технологією (двохсотгривневої купюри, нитки та клейкої стрічки). Тому цей прояв кримінально протиправної поведінки кіберзлочином не є.

1.2. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система

Визначте, чи є в діях М. склад кіберзлочину відповідно до Конвенції Ради Європи про кіберзлочинність та Кримінального кодексу України. Якщо так, то який?
Громадянин України М. з метою несанкціонованого доступу до комп'ютера своєї дружини придбав комп'ютерну програму, яка створена для запису послідовності натискань на клавіатурі комп'ютера. За допомогою цієї програми М. планував отримати пароль до електронної скриньки дружини.

37 **Класифікація міжнародних нормативно-правових актів, спрямованих на запобігання кіберзлочинності.** У Звіті за результатами дослідження кіберзлочинності, проведеного Комітетом ООН з наркотиків і злочинності, усі міжнародні та регіональні інструменти (акти), спрямовані на запобігання кіберзлочинності, поділено на п'ять груп з урахуванням тих міждержавних утворень, у рамках яких вони розроблені:

1) інструменти Ради Європи та ЄС;
2) інструменти СНД та Шанхайської організації співробітництва;
3) інструменти Африканського Союзу;
4) інструменти Ліги Арабських держав;
5) інструменти ООН.

Зокрема, в межах Ради Європи, ЄС, СНД та ООН питань 38
запобігання кіберзлочинності стосуються такі міжнародні та регіональні інструменти: Конвенція РЄ про кіберзлочинність від 23.11.2001 року та Додатковий протокол до неї від 28.01.2003 року, Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (2007 рік); Директиви ЄС 2000/31 про електронну комерцію, 2002/58 про захист персональних даних, 2016/1148 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, 2017/1371 про боротьбу з шахрайством, спрямованим проти фінансових інтересів Союзу, кримінально-правовими засобами, 2001/413 про боротьбу з шахрайством та підробкою безготівкових платіжних засобів; Угода про співробітництво держав-учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації (2001 рік), Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії (2000 рік). Вказані інструменти є зобов'язуючими для держави-підписанта, тобто підписання відповідного документи створює для держави правовий обов'язок імплементувати його положення у національне законодавство.

Історія прийняття Конвенції про кіберзлочинність. У 39
зарубіжній кримінології стверджується, що найсуттєвіший вплив на міжнародну та національну практику законотворення, в тому числі і в межах ЄС, мав концептуальний підхід до розуміння кіберзлочинів та напрямів боротьби з ними, закладений у

Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року та Додатковому протоколі до неї від 28.01.2003 року[26]. До прийняття Конвенції в межах Ради Європи було прийнято дві Рекомендації, які стосувалися боротьби зі злочинами, що вчиняються в кіберпросторі. Це, зокрема, Рекомендація Європейського комітету по боротьбі зі злочинністю # R (89) 9, яка стосувалася матеріально-правових питань боротьби з кіберзлочинами, та # R (85) 13, яка стосувалася процесуальних питань.

40 Для розроблення проєкту Конвенції про кіберзлочинність було сформовано спеціальний Комітет, який працював з 1997 року до 31 грудня 2000 року. 23 листопада 2001 року Конвенцію було відкрито до підписання, а з 1 липня 2004 року вона вступила в дію.

41 Розробники Конвенції про кіберзлочинність переслідували троїсту мету: гармонізувати національний матеріальний кримінальний закон держав-підписантів у частині ознак складів кримінальних правопорушень, що вчиняються у кіберпросторі та розв'язати інші, пов'язані з ними кримінально-правові проблеми (питання співучасті, місця вчинення кримінального правопорушення тощо); окреслити повноваження національних правоохоронних органів щодо розслідування цих злочинів, а також інших злочинів, що вчиняються за допомогою комп'ютера, та виробити рекомендації щодо використання електронних доказів; встановити швидкий та ефективний механізм міжнародної співпраці в частині запобігання кіберзлочинам.

42 Питання матеріального кримінального права регламентовані у частині 1 Розділу II Конвенції і передбачають, зокрема, мінімальні вимоги для держав-підписантів Конвенції щодо

[26] *Calderoni F.* The European legal framework on cybercrime: striving for an effective implementation. URL : https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation

удосконалення кримінально-правових засобів запобігання кіберзлочинам. Тобто Конвенція містить мінімальний перелік діянь, які держава-підписант зобов'язується криміналізувати, але держава може за власним вибором цей перелік розширювати. Також Конвенція дозволяє державі встановлювати умови, за яких винний не буде притягатися до кримінальної відповідальності за незначні кіберзлочини.

Поняття кіберзлочину у Конвенції про кіберзлочинність. 43
Конвенція про кіберзлочинність не містить визначення поняття кіберзлочину. У зарубіжній кримінології стверджується, що такий підхід загалом є виправданим, адже первинним завданням цього міжнародного інструменту є сприяння державам у запобіганні конкретним кіберзлочинам, а не вироблення теоретичної концепції кіберзлочину. Тому у Конвенції наведено перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність, та проведено їх класифікацію. Водночас аналіз змісту ознак складів правопорушень, які віднесені у Конвенції до кіберзлочинів, дає підстави стверджувати, що істотною, суттєвою ознакою цих правопорушень, яка відрізняє їх від інших, є об'єкт, проти якого спрямоване кримінально протиправне діяння (ним є комп'ютерні дані та комп'ютерні системи) або використання комп'ютерної системи у механізмі вчинення правопорушення.

За цими ознаками до кіберзлочинів у Конвенції про 44
кіберзлочинність запропоновано віднести такі групи посягань: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем (наприклад, незаконний доступ, нелегальне перехоплення); 2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами); 3) правопорушення, пов'язані зі змістом (наприклад, дитяча порнографія, расизм і ксенофобія); 4) правопорушення, пов'язані з порушенням

авторських та суміжних прав. Перша група кіберзлочинів виділяється за об'єктом, на заподіяння шкоди якому спрямована поведінки злочинця, а три інші – за тим, що у процесі їх вчинення винний застосовує комп'ютерну систему.

45 **Зміст ознак складів кіберзлочинів, передбачених у Конвенції про кіберзлочинність.** Склади кіберзлочинів, виділені у Конвенції про кіберзлочинність, характеризуються спільними способом та формою вини. Об'єднуючою ознакою кіберзлочинів, перерахованих у Конвенції, є вказівка на те, що відповідні діяння, які становлять зміст цих правопорушень, вчиняються «без права на це». Фактично йдеться про те, що ці діяння вчиняються незаконно, несанкціоновано, поза згодою власника. Водночас держава-підписант Конвенції у своєму національному законодавстві може передбачати випадки, коли діяння, які є *modus operandi* кіберзлочинів, описаних у статтях Конвенції, будуть законними або допустимими. Як результат вирішення питання про те, за яких умов передбачені Конвенцією діяння будуть розглядатися як вчинені «без права» і, відповідно, трактуватися як кіберзлочини, залишено на розсуд кожної держави.

46 Також усі правопорушення, передбачені в Конвенції, можуть бути кримінально караними лише якщо вони вчиняються умисно. Зміст та ознаки умислу залишаються на розсуд держави. В окремих випадках інші ознаки суб'єктивної сторони складу кримінального правопорушення національний законодавець повинен передбачати як обов'язкову ознаку складу кіберзлочину (наприклад, у випадку вчинення шахрайства, пов'язаного з комп'ютерами).

47 Для того, щоб більш детально окреслити обсяг правопорушень, які можуть бути віднесені до кіберзлочинів, у Конвенції роз'яснено, що таке комп'ютерна система та комп'ютерні дані. Зокрема, «комп'ютерна система» означає

будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичну обробку даних. У Пояснювальній записці до Конвенції вказано, що автоматична обробка означає, що система працює без прямого втручання людини, а інформація обробляється в комп'ютерній системі за допомогою комп'ютерної програми. Комп'ютерна програма – це набір інструкцій, які можуть бути виконані комп'ютером для досягнення необхідного результату. Комп'ютерною системою може бути як один окремий пристрій, так і група таких пристроїв. Загалом Конвенція використовує «технічно нейтральну» термінологію і не дає чіткого переліку об'єктів, які можуть бути віднесені до комп'ютерної системи. Такий підхід також обумовлений тим, що інформаційні технології стрімко розвиваються й обмеження поняття комп'ютерної системи чітким переліком може спричинити прогалини у правовому регулюванні у майбутньому. За вказаними у Конвенції ознаками до комп'ютерної системи належать, зокрема, планшети, смартфони, ноутбуки, банкомати, бортові комп'ютери у транспортних засобах, цифрові камери тощо. Натомість різного роду накопичувачі інформації (флеш-карти, карти пам'яті, USB накопичувачі тощо), якщо вони не під'єднані до комп'ютерної системи, самі по собі такою системою не є.

Відповідно до положень Конвенції пристрій, який є 48
комп'ютерною системою, не обов'язково має бути поєднаний з іншими пристроями у мережу. Однак якщо така мережа існує, то вона передбачає взаємозв'язок між двома чи більше комп'ютерними системами. Такий зв'язок комп'ютерних систем може бути дротовим, бездротовим (наприклад, радіо, сателіт) або змішаним. Сама мережа може бути обмежена або маленькою територією, або великою, або ж мережі можуть бути об'єднані між собою. Зокрема, Інтернет – це всесвітня

мережа, яка складається з низки взаємопов'язаних мереж, що користуються однаковим протоколом. Проте існують й інші види мереж, які забезпечують обмін інформацією між комп'ютерними системами і ці мережі можуть бути пов'язані з інтернетом або ж ні (наприклад, внутрішня мережа у фірмі). Однак щоб утворилась комп'ютерна система у межах цієї мережі має здійснюватися обмін комп'ютерними даними.

49 Термін «комп'ютерні дані» у межах Конвенції про кіберзлочинність означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою. У цьому визначенні такий зворот, як «придатний для обробки» означає, що дані повинні бути сформовані у такій формі, що їх можна було обробляти безпосередньо у комп'ютерній системі. А отже, набір незрозумілих жодній комп'ютерній системі символів не є комп'ютерними даними і, відповідно, не охороняються аналізованою Конвенцією.

50 Перша з виділених у Конвенції група кіберзлочинів (а саме правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем) становить «ядро» кіберзлочинності й об'єднує п'ять правопорушень: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями.

51 Незаконний доступ (ст. 2 Конвенції) полягає у навмисному доступі до цілої комп'ютерної системи або її частини без права на це. Під доступом варто розуміти вхід до всієї чи будь-якої частини комп'ютерної системи (апаратного забезпечення, компонентів, збережених даних встановленої системи, каталогів, даних про трафік та вмісту). Зокрема, це кримінальне правопорушення може полягати у тому, що злочинець несанкціоновано копіює

дані, які зберігаються у комп'ютерній системі, просто отримавши безпосередній доступ до системи, або він досягає тієї самої мети шляхом використання більш складних операцій (за допомогою свого комп'ютера проникає в комп'ютер потерпілого). Окрім того, у Пояснювальній записці до Конвенції зазначено, що просте надсилання електронного повідомлення електронною поштою або файлу з однієї комп'ютерної системи до іншої не утворює складу цього правопорушення. Склад незаконного доступу передбачає, що вхід до комп'ютерної системи відбувається тоді, коли вона підключена до загальнодоступних телекомунікаційних мереж, або до комп'ютерної системи, до якої під'єднаний той, хто втручається (тобто вхід до комп'ютера не зовнішнього користувача, а внутрішнього, в тій самій мережі, локальній мережі або внутрішній мережі в межах організації). Відповідно до положень Конвенції склад незаконного доступу є формальним. Конвенція дозволяє національному законодавцеві передбачати додаткові ознаки основного складу кримінального правопорушення-аналога незаконного доступу. Це, зокрема, спосіб вчинення (шляхом порушення заходів безпеки), або мета (з метою отримання комп'ютерних даних або з іншою недобросовісною метою), або додаткові характеристики предмета злочину (стосовно комп'ютерної системи, поєднаної з іншою комп'ютерною системою).

Нелегальне перехоплення (ст. 3 Конвенції) передбачає 52
навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані. Прикладом цього правопорушення є перехоплення переписки у соціальних мережах. За своєю суттю цей кіберзлочин є аналогом, наприклад, «традиційного»

прослуховування телефонних розмов. Перехоплення «технічними засобами» – це прослуховування, моніторинг або нагляд за вмістом повідомлень, отримання вмісту повідомлень або безпосередньо, тобто через доступ та використання комп'ютерної системи, або непрямим шляхом (наприклад, способом використання електронного підслуховування або пристроїв перехоплення інформації). Типовим прикладом вчинення цього злочину є встановлення програмного забезпечення, яке «зчитує» інформацію, що вводиться на клавіатурі комп'ютера.

53 Стаття 4 Конвенції, у якій закріплено ознаки складу втручання у дані, спрямована на те, щоб захистити комп'ютерні дані від несанкціонованих операцій з ними нарівні з речами матеріального світу. Втручання у дані полягає у навмисному пошкодженні, знищенні, погіршенні, зміні або приховуванні комп'ютерної інформації без права на це.

54 Кіберзлочин, передбачений у ст. 5 Конвенції – втручання у систему, є аналогом передбаченого в Рекомендації Європейського комітету по боротьбі зі злочинністю № (89) 9 правопорушення комп'ютерний саботаж. Втручання у систему охоплює навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це.

55 Вчинення вказаних вище кіберзлочинів часто вимагає наявності спеціальних знарядь – засобів доступу до комп'ютерних систем (наприклад, віруси, шкідливе програмне забезпечення). А тому, з метою ефективного запобігання вказаним вище кіберзлочинам, у кримінальних кодексах варто передбачити кримінальну відповідальність за певні суспільно небезпечні посягання, які передують вчиненню правопорушень, передбачених статтями 2–5. До таких суспільно небезпечних

посягань належить передбачене ст. 6 Конвенції правопорушення – зловживання пристроями.

Щодо наведеного казусу, *то відповідно до ст. 6 «Зловживання пристроями» Конвенції Ради Європи про кіберзлочинність придбання для використання комп'ютерних програм, створених з метою незаконного доступу до комп'ютерної системи, є кіберзлочином. Тому в діях М. є склад кіберзлочину, передбачений підпунктом 1.а.і ст. 6 Конвенції про кіберзлочинність.*

Україна ратифікувала Конвенцію про кіберзлочинність Законом від 07.09.2005 року, висловивши застереження до ст. 6 Конвенції. Україна залишила за собою право не застосовувати пункт 1 ст. 6 Конвенції в частині встановлення кримінальної відповідальності за, зокрема, придбання для використання предметів, зазначених у підпункті 1.а.і. Тому відповідно до КК такі дії не є самостійним, окремим кримінальним правопорушенням. Однак оскільки М. придбав вказану шкідливу комп'ютерну програму з метою вчинення іншого кримінального правопорушення, відповідальність за яке передбачена у ст. 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» КК, то з позиції вітчизняного кримінального законодавства його дії повинні бути оцінені за ч. 1 ст. 14 – ч. 1 ст. 361 КК України як готування до несанкціонованого втручання в роботу інформаційної (автоматизованої) системи.

1.3. Детермінанти та основні напрями запобігання кіберзлочинності

Проаналізуйте нижчеподані ситуації та визначте, який із наведених проявів деструктивної поведінки у кіберпросторі є кіберзлочином і чому?

КЕЙС 1. *Винний, перебуваючи за місцем свого проживання у кімнаті студентського гуртожитку, з метою незаконного збагачення, прийняв рішення здійснити несанкціоноване втручання в роботу автоматизованої системи Банку з використанням мобільного застосунку, шляхом автентифікації за допомогою Bank ID.*

Для реалізації злочинного умислу винний взяв мобільний телефон сусіда по кімнаті в гуртожитку, на якому був встановлений мобільний додаток банку, та виявивши його заблокованим, за допомогою графічного ключа, вийняв з нього SIM-картку оператора мобільного зв'язку і встановив її у відповідний слот мобільного телефону без блокування. Достовірно знаючи про те, що не має права доступу до автоматизованої системи Банку, шляхом надсилання запиту про зміну пароля до мобільного додатку, винний здійснив несанкціонований вхід до банківського рахунку сусіда по кімнаті, отримавши до нього доступ, що призвело до витоку інформації. Після цього здійснив дві трансакції, шляхом передачі грошових коштів у сумі 46 900 грн та 15 480 грн на власний картковий рахунок, таким способом підробив інформацію, шляхом її перекручування в автоматизованій системі.

КЕЙС 2. *Користувач розмістив на сайті «OLX.ua» оголошення про продаж мобільного телефону, якого він насправді не мав наміру відчужувати, на умовах передплати з наступним відправленням товару через оператора поштового зв'язку, та отримав банківським переказом грошові кошти і при цьому не відправив куплений товар під надуманим приводом і заблокував телефонний номер потерпілого.*

56 **Кількісні показники кіберзлочинності в Україні.** Цифрова трансформація держави, економіки і суспільства,

широке використання новітніх інформаційно-комунікаційних технологій (хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту, застосування розподілених реєстрів та ін.), спрямовані на збільшення рівня доходів та покращення якості життя населення. Водночас використання електронних інформаційних ресурсів, ІТ-технологій та інформаційно-телекомунікаційних систем може здійснюватися як з метою задоволення суспільно корисних потреб та інтересів, так і в злочинних цілях. На жаль, переміщення суспільного, політичного життя та економічної діяльності у кіберпростір супроводжується збільшенням кримінальної активності в ньому, а також поширенням проявів кіберзлочинності. У зв'язку з цим аналітики Європолу зазначають, що кіберзлочинність все більше розвивається у формі злочинного бізнесу, пов'язаного із наданням незаконних послуг у мережі Інтернет та/або інших глобальних мереж передачі даних. Експоненціальне зростання масиву даних, інтенсивний розвиток цифрової інфраструктури, збільшення чисельності користувачів, кількості підключень та часу перебування в кіберпросторі в умовах недосконалості системи кібербезпеки – суттєво ускладнюють криміногенну ситуацію із поширенням кіберзлочинності у світі та в Україні. Зі звіту компанії Майкрософт *Digital Defense Report* – 2021 слідує, що упродовж липня 2020 – червня 2021 років Україна посіла друге місце (19 %) серед країн, проти яких спрямовувалися хакерські атаки, поступившись за цим показником лише США (46 %)[27]. Показово і те, що з 2014 по 2017 роки в Україні рівень кіберзлочинності зріс майже у шість разів (443 кіберзлочинів проти 2 573), після чого спостерігається незначне зниження

[27] Microsoft Digital Defense Report, October 2021. P. 53. URL : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

кількості облікованих кіберзлочинів (2018 року – 2 301, 2019 року – 2 204, 2020 року – 2 498, жовтень 2021 року – 2 790)[28].

57 За даними дослідження американської корпорації *McAfee* «*The Hidden Costs of Cybercrime 2020*», з 2018 року сукупні втрати від кіберзлочинності становлять 1 % від світового ВВП, або $ 1 трильйон. Водночас за 2018–2020 роки вартість кіберзлочинності для світової економіки зросла на 50 %[29].

58 **Класифікація детермінантів кіберзлочинності.** На рівень, структуру та динаміку кіберзлочинності суттєво впливають різні явища і процеси, з якими вона взаємопов'язана та взаємообумовлена. За змістом і сферами дії детермінанти кіберзлочинності можна класифікувати на політичні, економічні, соціальні, нормативно-правові, організаційно-управлінські, технологічні, віктимологічні, а також чинники, пов'язані з неефективною діяльністю органів правопорядку.

59 **Політичні детермінанти кіберзлочинності.** Політичні детермінанти кіберзлочинності можна поділити на зовнішньополітичні або геополітичні та внутрішньополітичні. Зовнішньополітичні (геополітичні) детермінанти охоплюють:

– перетворення кіберпростору на середовище геополітичного суперництва за технологічне домінування у цифровому світі, монополізацію ринку інтелектуальної власності та наукоємної продукції, здійснення прихованого впливу на політичні і суспільні процеси, завуальоване втручання у зовнішню політику суверенних держав;

---

[28] Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування (2014–2021 рр.: офіційний веб-сайт Офісу генерального прокурора. URL : https://www.gp.gov.ua/ua/stat_n_st?dir_id=114368&libid=100820&c=edit&_c=fo

[29] The Hidden Costs of Cybercrime 2020. P. 3. URL : https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

- мілітаризація кіберпростору, використання його для проведення розвідувальної, терористичної, диверсійної та іншої підривної діяльності, спрямованих на ослаблення обороноздатності суверенних держав, блокування, виведення з ладу засобів зв'язку та автоматизованих систем управління новітніми видами озброєння і військами, зниження організаційно-технічної спроможності сил і засобів сектору безпеки й оборони потенційних противників;
- недостатній рівень кібернетичної стійкості мереж, інформаційних систем та об'єктів критичної інфраструктури держав-членів ЄС перед кіберзагрозами та кіберзлочинами;
- недотримання організаціями державного і приватного сектору різних держав міжнародних норм і стандартів кібербезпеки;
- декларативність політики та недостатність координації превентивних заходів держав-членів ЄС та НАТО щодо стримування та ефективної протидії застосуванню Російською Федерацією у кіберпросторі технологій гібридної війни проти України та інших суверенних держав, що поєднують військові і невійськові кіберзасоби із дестабілізації військово-політичної ситуації, створення стану невизначеності, провокування міжнародних конфліктів і ускладнень у відносинах із ключовими іноземними партнерами;
- розгортання в кіберпросторі шкідливого програмного забезпечення та проведення широкомасштабних кампаній з викрадення у політичних, економічних або військових цілях чутливої інформації, а також конфіденційна співпраця замовників кримінальних послуг з хакерськими угрупованнями і розробниками, операторами зловмисного програмного забезпечення;

– широкі можливості для проведення у кіберпросторі глобальних дезінформаційних компаній, що загрожують світовому правопорядку, демократичному розвитку та міжнародній стабільності шляхом пропагування праворадикальної ідеології, підтримки політики авторитарних урядів, поляризації спільноти користувачів Глобальної мережі на ґрунті мовних, релігійних, етнічних, ідеологічних та інших протиріч, підживлення протестних настроїв;
– фінансування та використання в геополітичних інтересах спеціальними службами і розвідувальними органами держав, що претендують на домінування у кіберпросторі, незаконних послуг міжнародних хакерських організацій, транснаціональних злочинних угруповань, організованих груп кіберзлочинців і професійних хакерів;
– нестабільність кіберпростору, постійне збільшення кількості та зміна характеру глобальних викликів і загроз для сталого функціонування національної інформаційної інфраструктури, поява нових вразливостей у мережах, інформаційно-телекомунікаційних системах і на об'єктах критично важливої інфраструктури.

60 Внутрішньополітичні детермінанти поширення кіберзлочинності включають:

– недоліки концепції державної політики у сфері забезпечення кібербезпеки та протидії кіберзлочинності, що зумовлені таким:
  а) панування державоцентристської ідеології у відносинах між державою, приватним сектором і громадянами у сфері забезпечення кібербезпеки, спрямованість діяльності суб'єктів владних повноважень на реалізацію владно-розпорядчих і контролюючих функцій та державного примусу, замість створення

умов для безпечного задоволення потреб та інтересів користувачів, і надання послуг із посилення кіберзахисту вразливих перед кіберзлочинами об'єктів;

б) декларативність принципу забезпечення захисту прав користувачів в інформаційно-телекомунікаційній системі та споживачів інформаційних електронних послуг, насамперед, права людини на приватність, заборону на розголошення персональних даних, а також не сформованість реальних механізмів захисту корпоративної інформації з обмеженим доступом, прав та законних інтересів суб'єктів господарювання;

в) консервація реактивного підходу в діяльності суб'єктів забезпечення кібербезпеки, спрямованого на стримування зловмисних дій у кіберпросторі та забезпечення інформаційної стійкості об'єктів захисту, замість всеохоплюючого упровадження проактивного підходу, що ґрунтується на ідентифікації, оцінці та управлінні наявними і потенційними кібернетичними ризиками, у тому числі кримінальними;

– непідкріплення політичної волі вищого керівництва держави щодо сталого розвитку інформаційного суспільства та створення безпечного комунікативного середовища достатнім фінансовим, матеріально-технічним та іншим ресурсним забезпеченням технологічної модернізації інформаційної інфраструктури та надійного функціонування механізму мінімізації кіберзагроз і боротьби з кіберзлочинністю;
– недостатній рівень гармонізації міжнародних стандартів кібербезпеки із законодавством України, неналежна уніфікація підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і держав-членів НАТО;

– незавершеність реформування системи захисту інформації з обмеженим доступом;
– недоліки в організації та проведення просвітницької роботи серед населення з питань безпечної поведінки у кіберпросторі та повідомлення про кіберзлочини до компетентних органів;
– нерозвинений механізм комунікацій у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю, спрямованої на поширення достовірної інформації про останні тенденції поширення кіберзлочинності, стан кібербезпеки у державному, приватному секторах; на покращення довіри до уповноважених суб'єктів та формування неприйнятного ставлення користувачів до будь-яких проявів зловмисних дій у кіберпросторі та кримінальних правопорушень;
– неефективна система підготовки кваліфікованих фахівців з кібербезпеки, а також відсутні навчальні програми з підготовки спеціалістів із виявлення, розслідування, припинення та запобігання кіберзлочинам;
– нерозвинена міжнародна співпраця з ключовими іноземними партнерами у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю.

61 **Економічні детермінанти кіберзлочинності.** Детермінанти кіберзлочинності, які належать до цього виду, полягають у такому:

– низькозатратність, малоризикованість та високодохідність кіберзлочинної діяльності (згідно зі звітом компанії з кібербезпеки «Bromium», а також за даними дослідженням компанії «*Atlas VPN*», щорічний дохід від кіберзлочинності становить $1,5 трлн на рік[30], тоді

[30] *Anton P.* Cybercrime annual revenue is 3 times bigger than Walmart's. URL : https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts

як загальний обсяг ринку кібербезпеки в 2019 році оцінюється лише $ 136 млрд[31]);

- функціонування аутсорсингової моделі організованого злочинного бізнесу в кіберпросторі (*Crime-as-a-Service*), надання платних послуг користувачам щодо організації на замовлення DDos-атак, продажу або оренди програмних кодів зловмисного програмного забезпечення та ін.;
- високий комерційний попит серед користувачів на зловмисне програмне забезпечення, кримінальні послуги операторів таких продуктів і хакерів, злочинна діяльність яких спрямовується на максимізацію доходів користувачів та замовників, мінімізацію їхніх витрат, дискредитацію та усунення конкурентів на цифровому ринку;
- велика пропозиція в темній мережі, закритих групах зловмисного програмного забезпечення, іншої незаконної продукції та кримінальних послуг з їх використання у протиправних цілях;
- розвинений у темній мережі кіберпростору незаконний обіг цифрових технологій, продуктів та послуг, що використовуються як початківцями, так і професійними хакерами у протиправних цілях;
- інноваційна відсталість економіки та її низька конкурентоспроможність, експортна орієнтованість інформаційно-комунікаційних технологій;
- інтенсивні темпи цифровізації фінансового сектору економіки і перехід на електронні платіжні системи, розвиток електронної комерції під час світової пандемії COVID-19, а також електронних послуг і пов'язана з цим

[31] Дохід від кіберзлочинів в одинадцять разів перевищує витрати на безпеку. URL : https://cybercalm.org/novyny/dohid-vid-kiberzlochyniv-v-odynadtsyat-raziv-perevyshhuye-vytraty-na-bezpeku/

концентрація у вказаних сферах левової частки грошових ресурсів, що сприяє поширенню онлайн крадіжок і кібершахрайства;

- широкі можливості здійснення конфіденційних платежів, приховування коштів та легалізації доходів, одержаних від кіберзлочинів шляхом зловживання використанням криптовалюти (біткоїнів, Monero), що конвертуються за допомогою сервісів обміну та іншими засобами[32];
- недостатній обсяг державного фінансування цифрового сектору, у тому числі заходів з кібербезпеки (менше піввідсотка ВВП);
- заощадження витрат державними і приватними структурами на купівлі та експлуатації комп'ютерної техніки й обладнання застарілих версій, використання неліцензованого програмного забезпечення, що не відповідають сучасним вимогам кібербезпеки, мають низький рівень кіберзахисту;
- збільшення обсягів трудової зайнятості в ІТ-секторі, зростання чисельності програмістів та інших фахівців у цій сфері, які можуть використовувати професійні навички і компетентності у злочинних цілях;
- функціонування в національному сегменті мережі Інтернет незаконного обігу контрафактного програмного забезпечення та неліцензованих антивірусних продуктів;
- відсутність конкурентного ринку телекомунікаційних послуг, широкі можливості для зловживання монопольним становищем операторами і провайдерами телекомунікацій шляхом встановлення завищених цін на телекомунікаційні послуги, недотримання порядку

[32] Internet Organised Crime Threat Assessment (IOCTA). URL : https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

маршрутизації трафіку на телекомунікаційних мережах, невживання заходів захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом;
- низький внутрішній попит на високотехнологічні програмні продукти, технічні рішення і проривні технології на ринку телекомунікацій, зумовлений їхньою високою вартістю.

Соціальні детермінанти кіберзлочинності. До соціальних 62
детермінант кіберзлочинності належать такі:
- зумовлені цифровізацією держави і суспільства зміни соціальної поведінки, що виражаються у переході на віртуальну модель комунікацій замість фізичної взаємодії;
- розмивання меж між реальним і віртуальним життям, що створює ілюзію безпеки;
- зловживання користувачами у кіберпросторі цифровими правами та свободами у протиправних цілях;
- використання технологій соціальної інженерії для зміни способу мислення і характеру поведінки людей та їхніх об'єднань у кіберпросторі;
- функціонування у кіберпросторі великої кількості закритих соціальних груп криміногенної спрямованості, що використовують технічні засоби таємного спілкування, навчають методам вчинення кіберзлочинів;
- деформації моральної і правової свідомості користувачів під цілеспрямованим інформаційно-психологічним деструктивним впливом та внаслідок споживання протиправного контенту;
- психологічна залежність значної частини суспільства від використання мобільних пристроїв, застосунків, соціальних мереж та інших засобів електронних комунікацій;

– зростання аудиторії користувачів та збільшення часу перебування у кіберпросторі (в 2021 році кількість глобальних користувачів смартфонів становила 5,22 млрд осіб; кількість користувачів Інтернету – 4,66 млрд; кількість користувачів соціальних мереж – 4,2 млрд[33]. В Україні у 2021 році зафіксовано 26 млн користувачів мережі Інтернет, при цьому користувачами соціальних мереж є 60 % населення[34]);
– низький рівень цифрової грамотності користувачів Інтернету, Е-сервісів, інформаційних ресурсів, несформованість цифрових навичок і цифрових компетенностей та культури безпечної поведінки у кіберпросторі.

63 **Нормативно-правові детермінанти кіберзлочинності.** Нормативно-правові детермінанти кіберзлочинності охоплюють:

– несформованість цілісної нормативно-правової бази у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю, неоднозначність термінології, неузгодженість правових приписів законів і підзаконних нормативно-правових актів, низький рівень гармонізації національного законодавства із законодавством ЄС та стандартами НАТО у цій сфері;
– нормативна неврегульованість питань щодо електронних комунікацій, використання штучного інтелекту, Інтернету речей та інших інформаційно-комунікаційних технологій, а також застарілість законодавства у сфері захисту інформації;

[33] Кількість користувачів Інтернету у світі сягнула 4,66 млрд. URL : https://root-nation.com/ua/news-ua/it-news-ua/ua-new-internet-records/#lwptoc

[34] За рік карантину кількість українців у соцмережах зросла на сім мільйонів. URL : https://www.dw.com/uk/za-rik-karantynu-kilkist-ukraintsiv-u-sotsmerezhakh-zrosla-na-sim-milioniv/a-56899697

– неповна імплементація Конвенції про кіберзлочинність у КК України, в частині закріплення повного переліку кіберзлочинів та посилення санкцій за їх вчинення, а також незакріплення в КПК України повноважень, заходів і процедур зі збору доказів в електронній формі (цифрових доказів), зокрема, щодо термінового збереження комп'ютерних даних (ст. 16), термінового збереження і часткового розкриття даних про рух інформації (ст. 17), обшуку й арешту комп'ютерних даних, які зберігаються (ст. 19), збирання даних про рух інформації в реальному часі (ст. 20), перехоплення даних змісту інформації (ст. 21), надання постачальниками послуг компетентним органам інформації про користувачів (ст. 18), що суттєво ускладнює розслідування та доказування по цій категорії кримінальних проваджень;
– неврегульованість в Законі України «Про телекомунікації» порядку взаємодії між суб'єктами забезпечення кібербезпеки та операторами, провайдерами телекомунікацій, зокрема, з питань ідентифікації кінцевих користувачів телекомунікаційних послуг та надання інформації про них, збереження інформації (про користувача послуг, про рух інформації), отримання до неї доступу (в тому числі і в електронному форматі), терміну збереження та порядку знищення інформації, а також процедур тимчасового обмеження доступу абонентів до ідентифікованого інформаційного ресурсу;
– повільні темпи наближення національного законодавства у сфері захисту персональних даних до законодавства ЄС, зокрема, Директиви (ЄС) 2016/680 про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за кримінальні зло-

чини чи виконання кримінальних покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/ПВР, а також положень Регламенту (GDPR) 2016/679 про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних і про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних);

- недостатній рівень гармонізації національного законодавства про критичну інфраструктуру та її захист із нормами Директиви (ЄС) 2016/1148 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Європейського Союзу, а також Директивою 2008/114/ЄС про ідентифікацію та призначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту;
- низька ефективність захисту прав громадян та суб'єктів господарювання у кіберпросторі, зумовлена неповною імплементацією в національне законодавство Директиви 2002/58/ЄС про обробку персональних даних та захист таємниці сектора електронних комунікацій (Директива про секретність та електронні комунікації);
- недосконалість нормативно-правової бази у сфері електронних довірчих послуг, зумовлена неповною імплементацією Регламенту ЄС 910/214 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку, що запроваджує транскордонну електронну ідентифікацію, автентифікацію з метою безпечної і безперебійної взаємодії державних органів, бізнесу і громадян;
- неврегульованість на законодавчому рівні питання запровадження ризик-орієнтованого підходу та механізму його реалізації в систему забезпечення кібербезпеки, запобігання і протидії кіберзлочинам;

– недосконалий організаційно-правовий механізм державно-приватної взаємодії у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю, недостатня синергія зусиль держави, приватного сектору і громадян;
– нечітка правова регламентація форм і механізму участі операторів, провайдерів телекомунікаційних послуг та інших суб'єктів приватного сектору, а також громадянського суспільства в реалізації стратегії і виконанні заходів запобігання і протидії кіберзлочинності.

Організаційно-управлінські детермінанти кіберзлочинності полягають у такому: 64

– організаційна незавершеність архітектури національної системи забезпечення кібербезпеки, несформованість таких складових компонентів, як: національна система захисту критичної інфраструктури, організаційно-технічна модель кібербезпеки цієї системи, загальнодержавний механізм протидії кіберзлочинності та запобігання кіберзлочинам, система управління кібернетичними ризиками у сферах електронних комунікацій, захисту інформації та кіберзахисту; національна хмарна платформа сервісів кібербезпеки та ін.;
– недостатня інституційна спроможність суб'єктів протидії кіберзлочинності, обмежений їхній штатний, технологічний, технічний, оперативний та кадровий потенціал, незадовільне інформаційно-аналітичне забезпечення правоохоронної та превентивної діяльності, недієве управління, міжвідомча взаємодія та координація у цій сфері;
– відсутність у значної частини державних органів, органів місцевого самоврядування, суб'єктів господарювання, віднесених до об'єктів критичної інфраструктури, структурних підрозділів із кібербезпеки та відповідних фахівців з кіберзахисту;

– нездійснення аудиту стану кібербезпеки на різних рівнях у державному і приватному секторах;
– недостатнє для розвитку національної системи кіберзахисту і протидії кіберзагрозам державне фінансування сфери кібербезпекової діяльності;
– низький рівень підготовки і підвищення кваліфікації фахівців з інформаційної і кібернетичної безпеки, відставання системи освітніх послуг від запитів ринку праці;
– недостатній рівень технічної захищеності державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;
– недостатньо розвинена міжнародна співпраця з питань кібербезпеки із Європейським Союзом, державами-членами НАТО, міжурядовими і неурядовими організаціями та ключовими іноземними партнерами, а також слабка інтегрованість національної системи кібербезпеки в європейський кібербезпековий простір;
– нерозробленість механізму громадського контролю за законністю та ефективністю діяльності суб'єктів забезпечення кібербезпеки і боротьби з кіберзлочинністю;
– відсутність загальнодержавної програми цифрової грамотності населення.

65 **Технологічні детермінанти кіберзлочинності.** До технологічних детермінант кіберзлочинності належать:

– технологічна і технічна відсталість цифрової інфраструктури України, моральна застарілість комп'ютерної техніки, баз даних і телекомунікаційних мереж, засобів зв'язку і технічного захисту, критично низький рівень використання державним і приватним секторами новітніх інформаційно-комунікаційних технологій, обладнання, ІТ-послуг, апаратного і програмного забезпечення останнього покоління;

- висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, відсутність системи оцінки відповідності такої продукції вимогам з безпеки, що підвищує ступінь уразливості інформаційної інфраструктури від незадекларованих функцій та звужує спроможності протидії кіберзагрозам[35];
- забюрократизованість порядку сертифікації й експертизи Комплексної системи захисту інформації та висока вартість її впровадження, що призводить до невиконання постачальниками телекомунікаційних послуг нормативно встановлених обов'язків із захисту державних інформаційних ресурсів або інформації з обмеженим доступом;
- технологічна застарілість і неефективність програмно-апаратних засобів криптографічного і технічного захисту інформації з обмеженим доступом;
- використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації в державному і приватному секторах;
- відсутність у багатьох власників і користувачів державних інформаційних ресурсів служби захисту інформації та системних адміністраторів, на яких покладається забезпечення захисту інформації та контролю за ним;
- можливість проникати в локальні мережі підприємств, організацій, установ шляхом підключення за протоколом віддаленого робочого столу (RDP) та одержувати несанкціонований доступ до серверів і баз даних через вразливі місця в службах VPN-сервісів;

[35] Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни: затверджено указ Президента України від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

- порушення загальних вимог до кіберзахисту об'єктів критичної інфраструктури власниками або керівниками підприємств, установ, організацій, віднесених до таких об'єктів;
- ненадійна система кіберзахисту інформації з обмеженим доступом в юридичних осіб державної і приватної форми власності (порушення адміністраторами і користувачами порядку доступу, поводження та встановлених регламентів збору, обробки, зберігання, поширення чи передачі інформації, відсутність засобів ідентифікації та автентифікації користувачів та адміністраторів, невикористання методу шифрування інформації, нездійснення моніторингу трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та ін.);
- незахищеність каналів зв'язку, електронної пошти, телекомунікаційних мереж, серверів і баз даних, окремих точок доступу до інформаційно-телекомунікаційної системи державних органів, юридичних осіб державної і приватної форми власності від несанкціонованого доступу третіх осіб та цілеспрямованих атак на всю мережеву інфраструктуру;
- використання застарілого антивірусного програмного забезпечення, ненадійних паролей, невпровадження інноваційних технологічних рішень Endpoint Detection & Response (EDR), що дозволяють виявити шкідливу активність у кінцевих точках і запобігти вчиненню протиправного посягання;
- недотримання суб'єктами господарювання, які працюють на ринку ЄС, вимог Регламенту щодо захисту персональних даних «*General Data Protection Regulation*» (GDPR);

- відсутність Єдиного реєстру оцінки ризиків і загроз на різних рівнях і об'єктах кіберзахисту;
- відсутність безпечного DNS-сервера («*Domain Name System*»), що містить розподілену ієрархічну базу даних про доменні імена серверів (хостів) і дозволяє за іменем визначити IP-адресу комп'ютера, служби чи інформаційного ресурсу, підключеного до мережі Інтернет;
- відсутність захищеного обміну ідентифікаційними даними фізичних та юридичних осіб, які обробляються в інформаційних системах державних органів та приватного сектору, неузгодженість у виборі ідентифікаторів, відсутність підтвердження ідентифікаційних даних[36];
- використання у системах реєстрації та контролю доступу до інформаційних систем технологічно несумісних механізмів, алгоритмів та протоколів електронної ідентифікації та впізнання[37].

Віктимологічні детермінанти кіберзлочинності. Вони полягають у такому: 66

- інтенсивний розвиток електронних послуг, зумовлений переходом на віддалений режим роботи під час світової пандемії COVID-19, зокрема інтернет-банкінгу, онлайн-аукціонів, безготівкових форм розрахунку, онлайн-платформ для електронної торгівлі, електронного документообігу, електронних державних послуг та

[36] Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки: схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

[37] Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

пов'язане з цим масове використання мобільних додатків фізичними і юридичними особами, що суттєво розширює спектр ризиків і загроз та підвищує уразливість об'єктів кіберзахисту перед кіберзлочинами;

- збільшення в рази кількості пристроїв підключених до глобальної мережі Інтернет та інших локальних мереж, що розширює можливості для кіберзлочинних посягань;
- професійна віктимність окремих категорій користувачів, які надають послуги та здійснюють господарську діяльність у кіберпросторі (провайдери/оператори телекомунікаційних послуг, адміністрація і персонал фінансових установ, суб'єкти господарювання, що здійснюють електронну торгівлю);
- високі ризики віктимізації державних службовців, які не дотримуються основ кібергігієни при роботі з публічною інформацією та інформацією з обмеженим доступом;
- економія витрат на системах програмного і технічного захисту інформації (використання старих версій браузерів, відсутність антивірусних програм, брандмауерів, ігнорування оновлення програм захисту та ін.);
- створення і самопоширення неповнолітніми компрометуючих матеріалів інтимного характеру та особистих даних у кіберпросторі;
- нерозбірливі знайомства в Інтернеті, вступ до різних груп, відверте спілкування, направлення фото і відеофайлів незнайомим користувачам;
- відвідування маловідомих сайтів і веб-сторінок інтернет-магазинів, переходи на вкладки спливаючої реклами, споживання сумнівного контенту на ринку праці, здійснення передплат за недоставлений товар або ненадані послуги;

– надмірна довірливість при використанні послуг Інтернет-банкінгу, SMS-банкінгу та спілкуванні із особами, що видають себе за операторів платіжних систем;
– заняття нелегальною електронною комерцією, а також надання нелегальних платних послуг користувачам мережі Інтернет, або інших глобальних мереж передачі даних.

Чинники, пов'язані з неефективною діяльністю правоохоронних органів: 67

– невизначеність державної політики боротьби із кіберзлочинністю, нерозробленість концепції запобігання і протидії кіберзлочинності, відсутність загальнодержавних та регіональних програм і протидії кіберзлочинності, несформованість стратегічних пріоритетів та відповідного їм комплексу заходів запобігання найбільш поширеним видам кіберзлочинів;
– недостатня спроможність суб'єктів боротьби з кіберзлочинністю ефективно здійснювати запобігання і протидію кіберзлочинам (недостатньо сил, засобів, матеріально-технічних ресурсів, кадрового потенціалу, бюджетного фінансування);
– відсутність центрального органу, відповідального за боротьбу з кіберзлочинністю в Україні, який би здійснював координацію діяльності усіх суб'єктів на загальнодержавному рівні, забезпечував міжвідомчу взаємодію та міжнародну співпрацю;
– брак кібер-експертів, оперативних працівників, слідчих, прокурорів, що спеціалізуються на запобіганні, виявленні, розслідуванні, припиненні кіберзлочинів;
– недостатня забезпеченість правоохоронних органів спеціальними технічними засобами виявлення та реагування на кіберпосягання, що містять ознаки кіберзлочинів.

68 Запобігання кіберзлочинності взаємопов'язано із забезпеченням кібербезпеки та є складовою діяльності держави у цій сфері. Водночас воно переслідує цілі недопущення вчинення злочинів у кіберпросторі чи з його використанням, припинення розпочатої кіберзлочинної діяльності, попередження рецидивних кіберзлочинів, зниження зовнішніх і внутрішніх вразливостей потенційних об'єктів протиправних посягань, протидії кіберзагрозам та використанню кіберпростору у протиправних цілях.

69 Запобігання кіберзлочинності ґрунтується на дотриманні принципів верховенства права, законності, захисту прав людини і основоположних свобод; забезпечення захисту національних інтересів України у кіберпросторі; реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права, у разі вчинення агресивних дій у кіберпросторі; невідворотності покарання за вчинення кіберзлочинів; міжнародного співробітництва, вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам; недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях; державно-приватного партнерства у сфері боротьби із кіберзлочинністю[38].

70 **Напрями запобігання кіберзлочинності.** Запобігання кіберзлочинності передбачає різнопланову діяльність державних органів у співпраці з приватними компаніями, громадянським суспільством і громадянами. Така діяльність здійснюється на стратегічному, тактичному і операційному рівнях, у масштабах держави, регіону, окремих об'єктів, стосовно постачальників і користувачів продуктів і послуг, а також на міждержавному рівні. Запобігання кіберзлочинності охоплює

[38] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII.

комплекс різних за змістом, спрямуванням, цілями заходів, які доцільно згрупувати за напрямами діяльності суб'єктів національної системи забезпечення кібербезпеки і боротьби з кіберзлочинністю.

Серед напрямів запобігання кіберзлочинності доцільно 71
вирізняти такі: профілактика кіберзлочинності, забезпечення стійкості національної інформаційної інфраструктури до впливу кіберзлочинності, відвернення загроз вчинення кіберзлочинів та припинення злочинної діяльності у кіберпросторі, міжнародна співпраця у сфері боротьби з кіберзлочинністю.

Профілактика кіберзлочинності. Профілактика 72
кіберзлочинності спрямовується на удосконалення нормативно-правового регулювання правовідносин у сфері електронних комунікацій, захисту інформації, ІТ-сфері, сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю; формування культури кібергігієни; розвиток цифрової грамотності населення і дотримання правил безпечного використання інформаційно-комунікаційних технологій, платформ, систем, сервісів, продуктів і пристроїв.

Удосконалення нормативно-правового забезпечення 73
запобігання кіберзлочинності передбачає повну імплементацію норм Конвенції про кіберзлочинність у КК України та КПК України; правову регламентацію порядку взаємодії між суб'єктами забезпечення кібербезпеки та операторами, провайдерами телекомунікацій щодо ідентифікації кінцевих користувачів телекомунікаційних послуг та надання інформації про них; гармонізацію національного законодавства з нормами Директив 2016/680/ЄС 2016/1148/ЄС, 2008/114/ЄС, 95/46/ЄС, 2002/58/ЄС, 2008/114/ЄС, а також вимогами Регламентів (GDPR) 2016/679, ЄС 910/214; нормативне врегулювання питання щодо механізму реалізації ризик-орієнтованого підходу в системі забезпечення кібербезпеки і боротьби з кіберзлочинністю,

а також державно-приватної взаємодії між спеціально уповноваженими суб'єктами боротьби з кіберзлочинністю та іншими учасниками кібербезпекової діяльності.

74 **Поняття «кібергігієни».** Формування культури кібергігієни спрямовується на створення цінностей безпечного користування комп'ютерами і мобільними пристроями, вироблення нетерпимого ставлення до порушення цифрових прав і свобод людини, до будь-яких проявів зловмисних дій у кіберпросторі та кримінальних правопорушень, а також формування навичок правильної поведінки після злочинного посягання.

75 Фахівці під «кібергігієною» розуміють «заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації»[39]. Натепер, Міністерство цифрової трансформації України та Координатор проєктів ОБСЄ в Україні на Національній онлайн-платформі для розвитку цифрової грамотності «Дія. Цифрова Освіта» презентували новий освітній серіал «Основи кібергігієни», в якому демонструються правила безпечної поведінки на роботі й у повсякденному житті при користуванні браузером, мережами Wi-Fi, особистою та службовою поштовими скриньками, мобільними пристроями та ін.[40].

76 Для підвищення рівня безпеки громадян у кіберпросторі доцільно запроваджувати загальнодержавну програму цифрової грамотності, спрямовану на розвиток цифрових навичок та цифрових компетентностей, підвищення обізнаності користувачів щодо кримінальних загроз та заходів з їх уникнення

---

[39] *Скибун О. Ж.* Кібергігієна як складова формування цифрової держави. *Вісник НАДУ*. 2021. № 2. С. 39–46. (Серія «Державне управління»).

[40] Основи кібергігієни. URL : https://osvita.diia.gov.ua/courses/cyber-hygiene

або мінімізації. Крім того, доцільно проводити регулярні загальнонаціональні інформаційно-роз'яснювальні кампанії в мас-медіа щодо основних форм прояву кіберзлочинності, типових способів вчинення кіберзлочинів, заходів убезпечення від кібершахрайства, а також формувати вміння завчасно розпізнавати ознаки кібершахрайства та інших кіберзлочинів під час віртуальних комунікацій.

77 **Поняття віктимологічної профілактики кіберзлочинності.** Віктимологічна профілактика кіберзлочинності охоплює вироблення загальних правил безпечного використання Глобальної мережі Інтернет, безпечного поводження з персональними даними, безпечного одержання довірчих електронних послуг, а також цілеспрямоване проведення просвітницької роботи з особами, які належать до групи ризику.

78 Наразі, за цим напрямом здебільшого проводяться заходи, спрямовані на роз'яснення наслідків необачної та ризикованої поведінки в кіберпросторі та популяризацію правил безпечної поведінки серед різних цільових груп користувачів. Наразі, віктимологічну профілактику кіберзлочинності більш-менш системно здійснює Департамент кіберполіції Національної поліції України. На офіційному сайті кіберполіції регулярно розміщуються тематичні рекомендації з актуальних питань кібербезпеки, а саме: щодо захисту заощаджень на банківських рахунках, захисту персональних даних під час використання мобільних додатків, безпечного онлайн-шопінгу, створення та використання надійних паролів, безпечного користування соціальними мережами, убезпечення дітей в Інтернеті, недопущення участі в злочинній діяльності транснаціональних організованих кіберугруповань, що спеціалізуються на легалізації доходів, здобутих від фішінгу, вішінгу, смішингу, а також торгівлі наркотиками, зброєю та людьми[41].

[41] Рекомендації кіберполіції. URL : https://cyberpolice.gov.ua/articles/

79 Активну просвітницьку діяльність серед дітей і батьків здійснює Міністерство освіти і науки України. За участі відомства в системі навчальних закладів популяризуються креативні ігрові та цифрові продукти, реалізовується освітній проект по захисту дітей від сексуального насильства в Інтернеті «Stop sexting», провадиться Всеукраїнська кампанія проти кібербулінгу «*Docudays UA*», створюються відео-уроки, розробляються довідникові матеріали, онлайн-курси[42].

80 Поряд із цим, є низка ініціатив з боку громадських організацій, приватних компаній, експертів, фахівців з кібербезпеки, що періодично розміщують на вебресурсах інформаційно-пізнавальні матеріали щодо захисту дітей в Інтернеті від впливу шкідливого контенту, сексуального насильства, булінгу, а також поради стосовно уникнення кібершахрайства.

81 Останнім часом до просвітницької роботи долучаються інші державні інституції. Так, на вебплатформі Міністерства цифрової трансформації України «ДІЯ. Цифрова освіта» для батьків створили серіал «Безпека дітей в інтернеті»[43]; на сайті Міністерства юстиції розміщено публікацію «Як не стати жертвою шахраїв в Інтернеті та що робити, якщо Ви потрапили в пастку»[44]. Загалом цей напрям профілактичної діяльності розвивається недостатньо інтенсивно.

82 **Суб'єкти забезпечення кібербезпеки та боротьби з кіберзлочинністю.** Забезпечення стійкості національної

[42] Безпека дітей в Інтернеті. URL : https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti

[43] Серіал для батьків «Безпека дітей в Інтернеті». URL : https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey

[44] Як не стати жертвою шахраїв в Інтернеті та що робити, якщо Ви потрапили в пастку. URL : https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku

інформаційної інфраструктури до впливу кіберзлочинності, з одного боку, спрямовується на завершення створення і розвиток інфраструктури, сил, засобів та інструментів національної системи забезпечення кібербезпеки, розширення її функціональних можливостей та удосконалення управління нею. З другого боку, вказана діяльність спрямовується на підвищення готовності уповноважених суб'єктів ефективно запобігати, виявляти та протидіяти кіберзагрозам і кіберзлочинам, мінімізувати вразливості об'єктів кіберзахисту на основі ризик-орієнтованого проактивного підходу.

У першу чергу необхідно завершити створення цілісної, 83
багаторівневої, горизонтально й вертикально інтегрованої системи суб'єктів забезпечення кібербезпеки і боротьби з кіберзлочинністю. Згідно з чинним законодавством основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Національна поліція України, Служба безпеки України, розвідувальні органи, Національний банк України. Показово, що перелічені суб'єкти забезпечують кібербезпеку і ведуть боротьбу з кіберзлочинністю паралельно із виконанням основних функцій і завдань за призначенням. При цьому Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України уповноважені запобігати, виявляти та реагувати тільки на кіберінциденти і кібератаки та усувати їх наслідки. Фактично це означає, що перелічені інституції можуть бути лише загальними суб'єктами боротьби з кіберзлочинністю, здійснювати профілактику кіберзлочинів, зменшувати вразливості та забезпечувати надійний захист державних електронних інформаційних ресурсів, критичної інформаційної

інфраструктури, інформації, вимога щодо захисту якої встановлена законом, а також повідомляти правоохоронні органи про кібератаки, що містять ознаки кримінальних правопорушень у кіберпросторі, надавати методичну, технічну та іншу допомогу у їх розслідуванні. Поєднують правоохоронні і превентивні функції тільки Національна поліція України, у складі якої функціонує Департамент кіберполіції, та Служба безпеки України, у складі якої функціонує Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, а також ситуаційний центр забезпечення кібербезпеки. Саме вказані структурні підрозділи Національної поліції України і Служби безпеки України уповноважені запобігати, виявляти, припиняти та розкривати кіберзлочини. Крім того, розвідувальні, контррозвідувальні та оперативно-розшукові заходи здійснюють функціональні підрозділи Служби зовнішньої розвідки, розвідувальний орган Державної прикордонної служби України. Функції координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, покладено на Національний координаційний центр кібербезпеки, що є робочим органом при Раді національної безпеки і оборони України. Аналіз даних про кіберінциденти в масштабах держави, взаємодію з правоохоронними органами з питань своєчасного інформування про кібератаки, з іноземними і міжнародними організаціями з питань реагування на комп'ютерні надзвичайні події, підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору, здійснює Державний центр кіберзахисту Держспецзв'язку, у складі якого працює Урядова команда реагування на комп'ютерні надзвичайні події України (*CERT-UA*).

Видається, що склад суб'єктів забезпечення кібербезпеки 84
і боротьби з кіберзлочинністю необхідно розширювати шляхом створення мережі ситуаційних центрів забезпечення кібербезпеки в усіх державних органах, органах місцевого самоврядування, об'єктів критичної інформаційної інфраструктури, а також створення технічних підрозділів з кіберзахисту на підприємствах, установах, організаціях незалежно від форми власності. До боротьби з кіберзлочинністю варто залучати власників і користувачів інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, провайдерів/операторів телекомунікацій, найбільших інтернет-посередників, приватні ІТ-компанії, об'єднання юридичних осіб (Асоціація «Блокчейн України», Українська Асоціація Платіжних Систем, Інтернет асоціація України та ін.), об'єднання громадян, наукові, науково-дослідні, експертні установи.

Пропозиції щодо структури загальнодержавної 85
організаційно-технічної моделі кіберзахисту. Для підсилення стійкості національної інформаційної інфраструктури до впливу кіберзлочинності важливо створити загальнодержавну організаційно-технічну модель кіберзахисту, в межах якої буде забезпечено на організаційному, технологічному і базисному рівнях взаємодію між суб'єктами національної системи кібербезпеки на основі відповідної захищеної інформаційної інфраструктури[45]. На думку О. Потія, така модель має складатися з трьох вертикально та горизонтально інтегрованих рівнів кіберзахисту:

[45] Ключові представники суб'єктів національної системи кібербезпеки України обговорили організаційно-технічну модель кіберзахисту. URL : https://cip.gov.ua/ua/news/klyuchovi-predstavniki-sub-yektiv-nacionalnoyi-sistemi-kiberbezpeki-ukrayini-obgovorili-organizaciino-tekhnichnu-model-kiberzakhistu

– організаційно-управлінська інфраструктура, до складу якої входять суб'єкти кіберзахисту, згруповані у державний, академічний, приватний, громадський та регіональний сектори;
– технологічна інфраструктура, в рамках якої забезпечується обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору;
– базисна інфраструктура, яка складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни)[46].

86 На організаційно-управлінському рівні суб'єктам національної системи кібербезпеки необхідно розробити проєкти загальнодержавної стратегії боротьби з кіберзлочинністю, програми її реалізації, плану спільних дій із запобігання, виявленню та протидії кіберзагрозам і кіберзлочинам; удосконалювати механізм державно-приватного партнерства у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю; здійснювати достатнє фінансове, матеріально-технічне, кадрове та інше ресурсне забезпечення сталого функціонування національної системи кібербезпеки.

87 На рівні функціонування технологічної інфраструктури загальнодержавної системи кіберзахисту доцільно вжити таких заходів:

– розвивати електронну взаємодію державних електронних інформаційних ресурсів (державних реєстрів, баз даних) на основі інтероперабельності, відповідно до вимог ЄС;
– запроваджувати засоби електронної ідентифікації та

[46] Ключові представники суб'єктів національної системи кібербезпеки України обговорили організаційно-технічну модель кіберзахисту. URL : https://cip.gov.ua/ua/news/klyuchovi-predstavniki-sub-yektiv-nacionalnoyi-sistemi-kiberbezpeki-ukrayini-obgovorili-organizaciino-tekhnichnu-model-kiberzakhistu

захищеного обміну ідентифікаційними даними фізичних та юридичних осіб, які обробляються в інформаційних системах державних органів та приватного сектору у сфері електронних послуг та електронної комерції, а також створити національний сервіс доменних імен (DNS);

- забезпечити автоматизований обмін інформацією про кібератаки, кіберзлочини та кіберзагрози між усіма суб'єктами національної системи кібербезпеки на базі єдиної технологічної платформи Національного координаційного центру кібербезпеки при РНБО України[47];
- розширювати сферу застосування технології блокчейн, зокрема в системі захисту об'єктів критичної інфраструктури, а також використовувати блокчейн у страхуванні, розслідуванні фінансових злочинів з використанням криптовалют та ін.;
- використовувати в кіберзахисті об'єктів національної інформаційної інфраструктури інноваційні технологічні рішення та програмне забезпечення, що дозволяють виявити зловмисну активність у кінцевих точках і запобігти вчиненню протиправного посягання, або виявити та усунути вразливості в електронних комунікаційних мережах та інформаційних ресурсах;
- модернізувати систему апаратних, апаратно-програмних засобів технічного захисту інформації з обмеженим доступом, а також систему захищеного доступу державних органів до мережі Інтернет;

[47] Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни: затверджено указ Президента України від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

– розробити організаційні вимоги та рекомендації щодо порядку застосування криптографічного і технічного захисту інформації, серверів, баз даних, застосунків (програм), мереж державного і приватного секторів з метою забезпечення кібербезпеки і боротьби з кіберзлочинністю;
– впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед, об'єктів критичної інформаційної інфраструктури[48];
– створення Єдиного реєстру оцінки ризиків і загроз на різних рівнях і об'єктах кіберзахисту.

88 За напрямом підвищення готовності уповноважених суб'єктів ефективно запобігати, виявляти та протидіяти кіберзагрозам і кіберзлочинам, мінімізувати вразливості об'єктів кіберзахисту, необхідно розвивати інформаційно-аналітичну діяльність та запроваджувати ризик-орієнтований підхід до забезпечення кібербезпеки і боротьби з кіберзлочинністю. Для цього треба розробити методику ідентифікації та оцінювання кримінальних ризиків у сфері електронних комунікацій, захисту інформації та кібербезпеки, закупити сучасне програмне забезпечення, комп'ютерну техніку і технічне обладнання, що дозволяє здійснювати надійний кіберзахист інформаційних та телекомунікаційних систем. На окрему увагу заслуговують питання підготовки і підвищення кваліфікації працівників структурних підрозділів (фахівців) з кіберзахисту, відповідальних осіб за адміністрування телекомунікаційних мереж, загальносистемних серверів і технічний захист

[48] Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни: затверджено указ Президента України від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

інформації, а також експертів, оперативних працівників і слідчих, що спеціалізуються на запобіганні, виявленні, припиненні та розкритті кіберзлочинів. Для укомплектування штату функціональних підрозділів з кібербезпеки в державному секторі важливо збільшити розміри грошового забезпечення цих фахівців.

89 **Заходи, що здійснюються уповноваженими суб'єктами для забезпечення кібербезпеки.** Відвернення загрози вчинення кіберзлочинів та припинення злочинної діяльності у кіберпросторі спрямовується на обмеження й усунення сприятливих умов для поширення кіберзлочинності, а також раннє виявлення, оперативне реагування і припинення кіберзлочинів, що готуються; нейтралізацію зловмисної активності у кіберпросторі груп і осіб; виявлення, протидію і припинення розвідувально-підривної, терористичної та іншої злочинної діяльності у кіберпросторі, перешкоджання використовуванню мережі Інтернет у військових цілях.

90 За розглядуваним напрямом превентивна діяльність охоплює оборонні, розвідувальні, оперативно-розшукові, контррозвідувальні заходи, що здійснюються уповноваженими суб'єктами забезпечення кібербезпеки та боротьби з кіберзлочинністю.

91 Обмеження й усунення сприятливих умов для поширення кіберзлочинності передбачає наступне:

- виявлення, блокування доступу та ліквідацію вебресурсів у темній мережі Інтернет, на яких здійснюється незаконний обіг цифрових технологій, програмних продуктів та послуг, що використовуються у протиправних цілях;
- виявлення, блокування та видалення в українському сегменті мережі Інтернет адрес, вебсайтів, вебсторінок, через які або за допомогою яких вчиняються протиправні дії;

– видалення найбільшими інтернет-посередниками за зверненням правоохоронних органів протиправного контенту, сторінки чи ресурсу, що поширюють дезінформацію, сексуальну експлуатацію та насильство над дітьми, порушують авторське право, містять деструктивну пропаганду, неправдиві метадані, прояви шахрайства тощо.

92 Раннє виявлення, оперативне реагування і припинення кіберзлочинів, що готуються, а також нейтралізація зловмисної активності груп і осіб у кіберпросторі охоплює широке коло превентивних заходів. Серед них доцільно назвати такі:

– автоматизований моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів державного і приватного сектору на предмет виявлення і блокування кібератак, а також встановлення і блокування платформ, IP-адрес, з яких вони здійснюються;
– перевірка суб'єктів господарювання, що здійснюють діяльність у сфері інформаційних технологій і комп'ютерних систем, виконують комп'ютерне програмування, надають інформаційні й телекомунікаційні послуги на предмет прихованої співпраці із іноземними спеціальними службами та розвідувальними органами, та/або співучасті чи причетності до злочинної діяльності у кіберпросторі, із послідуючим притягненням до встановленої законом юридичної відповідальності фізичних і юридичних осіб;
– посилення державного контролю за ринком товарів і послуг у сфері кібербезпеки;
– вилучення і знищення заборонених або обмежених у вільному обігу шкідливих програмних та технічних засобів, призначених для несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем,

комп'ютерних мереж чи мереж електрозв'язку; спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації;

- встановлення осіб та їх місцезнаходження, які розробляють, виготовляють, збувають і використовують шкідливе програмне забезпечення, технічні засоби, призначені для вчинення кіберзлочинів, а також захоплення таких осіб, конфіскація і знищення знарядь вчинення кримінальних правопорушень;
- відстежування осіб, які проявляють зловмисну активність в інформаційно-комунікаційних системах державного і приватного сектору, на об'єктах критичної інформаційної інфраструктури, стосовно інформації з обмеженим доступом, проведення оперативно-розшукових заходів стосовно них;
- здійснення розвідувальних, контррозвідувальних, оперативно-розшукових, оборонних та інших заходів зі запобігання, виявлення і припинення кримінальних правопорушень в секторі безпеки та оборони, що вчиняються з використанням кіберпростору, а також розвідувально-підривній, шпигунській, терористичній та іншій злочинний діяльності у кіберпросторі.

93

Заходи міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Міжнародне співробітництво у сфері боротьби з кіберзлочинністю здійснюється у різних формах. Відповідно до ст. 23 Конвенції про кіберзлочинність сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування

або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень[49].

94 Серед заходів міжнародного співробітництва в Конвенції про кіберзлочинність вирізняються такі:

- екстрадиція винних у вчинені кримінального правопорушення, передбаченого статтями 2-11 Конвенції, за умови, що вони підлягають покаранню у вигляді позбавлення волі на строк не менше одного року, або більш суворому покаранню, відповідно до законодавства обох заінтересованих сторін, у тому числі екстрадиція за запитом сторони, з якою немає договору про екстрадицію, відповідно до норм Конвенції, що є юридичною підставою для екстрадиції, відносно будь-якого визначеного кримінального правопорушення (ст. 24);
- взаємна допомога у найширшому обсязі з метою розслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними та кримінального переслідування, або з метою збирання доказів в електронній формі щодо кримінального правопорушення (ст. 25);
- добровільне, без попереднього запиту надання правоохоронним органом іноземному партнеру інформації, отриманої в ході розслідування, якщо є підстави вважати, що розкриття такої інформації може допомогти у відкритті або проведенні розслідування кіберзлочинів (ст. 26);
- взаємна допомога, спрямована на термінове збереження комп'ютерних даних, які зберігаються в комп'ютерних

[49] Конвенція про кіберзлочинність від 23.11.2001. URL : http://zakon0.rada.gov.ua

системах на території іншої сторони, яка має намір зробити запит щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних (ст. 29), а також термінове розкриття збережених даних про рух інформації (ст. 30);

– взаємна допомога з питань надання повноважень на розслідування, а саме: взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються в комп'ютерних системах на території іншої сторони (ст. 31); транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними (ст. 32); взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу (ст. 33); взаємна допомога у перехопленні даних змісту інформації (ст. 34); цілодобова мережа, тобто створення та підтримання в актуальному стані мережі, в рамках якої відбувається обмін інформацією різного роду щодо запобігання кіберзлочинам (ст. 35).

Окрім цього, міжнародне співробітництво полягає в 95
налагодженні систематичного обміну інформацією про протиправну діяльність у кіберпросторі з міжнародними партнерами; в проведенні спільних заходів і дій суб'єктами національної системи забезпечення кібербезпеки та боротьби з кіберзлочинністю і відповідними інституціями Європейського Союзу, зокрема: з Європейською агенцією мережевої та інформаційної безпеки (*European Network and Information Security Agency*, *ENISA*), Групою з реагування на комп'ютерні надзвичайні ситуації для установ, органів та установ ЄС (*CERT-EU*), Європолом, Європейським центром з розслідування кіберзлочинів (*European Cybercrime Centre*, *ECC*), Європейською агенцією оборони (*European Defence Agency*), Європейською службою зовнішніх справ (*European External Action Service*).

96 Окремим напрямом міжнародного співробітництва у сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю є надання технічної допомоги державам-членам ЄС, що фінансується за рахунок підтримки урядів Австралії, Канади, Японії, Норвегії, Великобританії і США.

97 Важливе значення для співробітництва між державами у сфері боротьби з кіберзлочинністю мають двосторонні та багатосторонні міжнародні договори про взаємну правову допомогу, взаємне визнання іноземних судових рішень, адже на їх основі також відбувається співпраця між правоохоронними органами різних країн[50].

Для відповіді на запитання, поставлені у казусах, *потрібно звернути увагу на таке.*

КЕЙС 1. *Відповідно до ст. 7 «Підробка, пов'язана з комп'ютерами» Конвенції Ради Європи про кіберзлочинність, навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти, є кіберзлочином. Тому в діях винного є склад кіберзлочину, передбачений ст. 7 Конвенції про кіберзлочинність.*

Україна ратифікувала Конвенцію про кіберзлочинність Законом від 07.09.2005 року. Відтак, згідно з національним кримінальним законодавством, такі дії є окремим кримінальним правопорушенням, передбаченим ст. 361 КК України.

На підставі викладеного, винний вчинив кіберзлочин, а саме: несанкціоноване втручання в роботу інформаційної (автоматизованої) системи, що призвело до витоку та підробки інформації (ч. 3 ст. 361 КК України).

КЕЙС 2. *Відповідно до ст. 8 «Шахрайство пов'язане з комп'ютерами» Конвенції Ради Європи про кіберзлочинність навмисне вчи-*

[50] *Марущак А. І.* Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3(26). С. 105.

нення, без права на це дій, що призводять до втрати майна іншої особи шляхом: будь-якого введення, зміни, знищення чи приховування комп'ютерних даних; будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи, – вважається кіберзлочином. Україна ратифікувала Конвенцію про кіберзлочинність Законом від 07.09.2005 року, відповідно до якої встановлено кримінальну відповідальність за вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України). Для кваліфікації цього виду шахрайства необхідно встановити, щоб відповідна фінансова операція з використанням електронно-обчислювальної техніки була незаконною, тобто мало місце втручання у функціонування системи електронних платежів, несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах з метою незаконного заволодіння майном через обман або зловживання довірою.

Оскільки перерахування коштів на рахунок через банківську установу або банківським переказом здійснювалося без втручання у функціонування комп'ютерних систем, тобто є цілком законною операцією, то дії користувача з викрадення грошових коштів не містять ознак кібершахрайства (ч. 3 ст. 190 КК України), а будуть звичайним шахрайством.

Запитання для самоконтролю

1. Назвіть існуючі у кримінології підходи до визначення поняття злочинність.
2. Який з вітчизняних кримінологічних підходів до визначення кіберзлочинності є найбільш поширеним і чому?
3. Якими термінами позначають явище «кіберзлочинність»? Як співвідносяться ці терміни?
4. Які недоліки є у законодавчому визначенні поняття кіберзлочинність?
5. За якими критеріями пропонують відносити кримінальне правопорушення до кіберзлочинів?

6. Які кримінальні правопорушення не є кіберзлочинами відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»? Чи обґрунтований такий підхід законодавця? Відповідь поясніть.

7. Які підходи до визначення кіберзлочину були сформульовані за результатами роботи X Міжнародного конгресу ООН з боротьби зі злочинністю та поводження з правопорушниками? В чому недоліки кожного з них?

8. Який підхід до визначення кіберзлочину домінує в зарубіжній кримінології?

9. Назвіть підходи до того, в чому полягає кримінологічна однорідність кіберзлочинів. Який із них найбільш обґрунтований, на Вашу думку, і чому?

10. Які групи кіберзлочинів можна виділити за значенням інформаційної системи у механізмі реалізації кримінально протиправної діяльності?

11. На які групи поділені усі міжнародні та регіональні інструменти (акти), спрямовані на запобігання кіберзлочинності, з урахуванням міждержавних утворень, в рамках яких вони розроблені?

12. Концептуальний підхід якого міжнародного акту мав найсуттєвіший вплив на міжнародну та національну практику законотворення у сфері боротьби з кіберзлочинністю?

13. Яку мету переслідували розробники Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року?

14. Чи є у Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року визначення кіберзлочину? Чи виправданий такий підхід?

15. На які групи поділено кіберзлочини у Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року? Яка з них є «ядром» кіберзлочинності?

16. Назвіть спільні ознаки складів кіберзлочинів, які виділені у Конвенції Ради Європи про кіберзлочинність?

17. Дайте визначення «комп'ютерної системи» та «комп'ютерних даних» відповідно до положень Конвенції Ради Європи про кіберзлочинність.

18. Охарактеризуйте кіберзлочин «незаконний доступ».

19. В чому полягає нелегальне перехоплення відповідно до ст. 3 Конвенції Ради Європи про кіберзлочинність?

20. Розкрийте зміст ознак складу втручання у дані відповідно до ст. 3 Конвенції Ради Європи про кіберзлочинність?

21. Про які ключові виклики і загрози кібербезпеці України йдеться в Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни».

22. Охарактеризуйте внутрішньополітичні і зовнішньополітичні детермінанти кіберзлочинності.

23. Які з детермінант кіберзлочинності впливають на формування мотивації протиправної поведінки у кіберпросторі, а які створюють сприятливі умови для вчинення кіберзлочинів?

24. Розкрийте зміст економічних детермінант кіберзлочинності та обґрунтуйте їхній вплив на зростання кіберзлочинності, як послуги.

25. Продемонструйте з позицій теорії рутинної діяльності значення соціальних детермінант у збільшенні кримінальної активності користувачів Глобальної мережі Інтернет.

26. З позицій теорії кримінальних можливостей охарактеризуйте технологічні детермінанти кіберзлочинності.

27. Яка роль віктимогенних детермінант у зростанні рівня кіберзлочинів?

28. Які напрями запобігання кіберзлочинності Ви знаєте?

29. Чим відрізняється профілактика кіберзлочинів від заходів забезпечення кіберстійкості інформаційної інфраструктури до впливу кіберзлочинності?

30. Які відмінності у повноваженнях мають суб'єкти забезпечення кібербезпеки і суб'єкти протидії кіберзлочинності?

Рекомендована література

1. *Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П.* Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посібник / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

2. *Головкін Б. М.* Види злочинності. *Журнал східноєвропейського права.* 2015. № 18. С. 14–21.

3. *Денькович О. І.* Поняття кіберзлочину у зарубіжній кримінології. Проблеми державотворення і захисту прав людини в Україні : матеріали XXIII звітної науково-практичної конференції (7–8 лютого 2017 р.) :

у 2 ч. Ч. 2. Львів : Юридичний факультет Львівського національного університету імені Івана Франка, 2017. С. 130–133.

4. *Кравцова М. О., Литвинов О. М.* Запобігання кіберзлочинності в Україні : монографія. Харків, 2016. 212 с.

5. *Марущак А. І.* Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104–110.

6. *Bernik I.* Cybercrime and Cyberwarfare. John Wiley & Sons, ISTE Ltd. 2014. 176 p.

7. *Brenner W Susan.* Cybercrime and the law: challenges, issues, and outcomes. Northeastern University Press, 2012. 198 p.

8. *Calderoni F*. The European legal framework on cybercrime: striving for an effective implementation. URL : https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation

9. Internet Organised Crime Threat Assessment (IOCTA), Europol, 2021. URL : https://www.europol.europa.eu

10. *Hong Y., Neilson W.* Cybercrime and Punishment. *The Journal of legal studies*. 2020. Vol. 49 (2). P. 431–466.

11. *Meyerowitz S. A.* Cybercrime. *The Banking law journal*. 2019. Vol. 136 (6). P. 299–301.

12. *Kai-Lung Hui, Seung Hyun Kim, Qiu-Hong Wang*. Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. MIS Quarterly. Vol. 41. No. 2 (June 2017). P. 497–524.

РОЗДІЛ 2

ОСОБЛИВОСТІ МЕТОДИКИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Опрацювавши подані нижче кейси, охарактеризуйте спосіб вчинення кіберзлочину, знаряддя його вчинення та предмет посягання.

КЕЙС 1. *Група осіб за попередньою змовою масово поширювала через мережу Інтернет дезінформацію, у тому числі щодо діяльності вищого військово-політичного керівництва України. Керівником цієї групи був громадянин рф С., який проживав у столиці і позиціонував себе як військово-політичний експерт. Своєю чергою на замовлення однієї з політичних сил він організував інформаційно-підривну діяльність: так, С. створив спеціальне програмне забезпечення, за допомогою якого учасники групи керували в автоматичному режимі необмеженою кількістю анонімних акаунтів у найбільш популярних соцмережах. Для маскування протиправної діяльності вони облаштували відповідне обладнання у різних українських містах. Для поширення деструктивного контенту учасники групи під керівництвом С. адміністрували понад мільйон власних ботів, а також численні групи в соцмережах з понад стотисячною аудиторією.*

КЕЙС 2. *Громадянин К. за допомогою комп'ютерного вірусу віддалено управляв комп'ютерами інших людей. Зокрема, зазначений вірус допомагав отримувати віддалений доступ до комп'ютерів, унаслідок чого К. мав можливість завантажувати та відвантажувати файли, керувати автозавантаженням і службами, віддалено управляти реєстром, встановлювати і видаляти програми, робити знімки з віддаленого екрану, перехоплювати звук з мікрофона і відео з вбудованих або зовнішніх камер. Більше того,*

серед функцій цього шкідливого програмного забезпечення були моніторинг натиснутих клавіш, монітор буфера обміну, цілий набір утиліт для роботи з мережею, а також можливість К. віддалено вимикати і перезавантажувати уражений комп'ютер. Програма використовувала бек-коннект, тобто сама ініціювала з'єднання з керуючою машиною.

КЕЙС 3. *Хакерське угруповання під керівництвом В., яке діяло в одному з українських міст, зламало понад мільйон акаунтів та продавало їх через мережу «Darknet». Так, учасники організованої групи входили в активні акаунти інтернет-користувачів з України та держав Євросоюзу, отримуючи доступ до персональних даних фізичних осіб. Одержану конфіденційну інформацію вони в подальшому продавали через анонімну платформу «Darknet», а грошові кошти отримували на електронні платіжні системи ЮMoney, Qiwi та WebMoney.*

КЕЙС 4. *Головний оператор відділення поштового зв'язку АТ «Стара Пошта» М., маючи доступ до автоматизованої системи «Фінансове управління», неодноразово вносив до неї недостовірні відомості. Зокрема, при створенні електронних платежів М. вносив у систему відомості, які відрізнялися від паперових звітів. Різницю в сумі майже 100 000 гривень М. привласнив, частину коштів з яких використав для купівлі ювелірних виробів, а решту одержав готівкою та витратив на побутові потреби.*

КЕЙС 5. *Громадянин Т., який створив та адміністрував автоматизовану мережу з понад 100 тисяч фейкових облікових записів, здійснював DDoS- та спам-атаки, виявляв вразливості вебсайтів та зламував їх. Окрім кібератак і зламування сайтів, він займався підбором паролів до скриньок електронної пошти на віддалених платформах так званим «брутфорсом». Замовників він знаходив на закритих форумах та у чатах соціальних мереж, а розрахунки з клієнтами здійснював через заборонені в Україні електронні платіжні системи.*

До питання про обсяг поняття «кіберзлочин» з погляду криміналістики. Будь-який процес злочинної діяльності, що передбачає використання комп'ютерів (ЕОМ), систем

та комп'ютерних мереж і мереж електрозв'язку, з плином часу технологічно ускладнюється. І це пов'язано не лише із закономірним удосконаленням високих інформаційних (комп'ютерних) технологій. У криміналістичному аспекті це зумовлено підвищенням професійного рівня самого злочинця. Обравши певний профіль злочинної діяльності в кіберпросторі, злочинець, власне, отримує «дорожню карту» вдосконалення своєї діяльності. Соціальні мережі, форуми, чати та інші способи комунікацій у кіберпросторі разом із персональною здатністю до навчання таких злочинців дозволяють не лише систематично вчиняти кіберзлочин, а й ускладнювати механізм його вчинення, розробляти власну або запозичувати чиюсь технологію вчинення злочинів. Згідно з офіційними даними Національної поліції України в 2020 році було вчинено 10 480 злочинів у сфері використання високих інформаційних технологій, за три місяці 2021 року – 3 506; у провадженні в 2020 році знаходилося загалом 23 242 матеріали (справи), за три місяця 2021 року – 16 140. Згідно із довідниками Департаменту організаційно-аналітичного забезпечення Національної поліції України при обліковуванні послуговуються категорією «злочини у сфері використання високих інформаційних технологій», що охоплює конкретні види злочинних проявів, зокрема за такими статями КК України: ст. 176 (порушення авторського права і суміжних прав); ст. 185 (крадіжка); ст. 190, ч. 3, 4 (шахрайство); ст. 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення); ст. 229 (незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару); ст. 231 (незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю); ст. 301,

ч. 3, 4, 5 (ввезення, виготовлення, збут і розповсюдження порнографічних предметів); ст. 361–363-1 (Розділ XVII «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж та мереж електрозв'язку»).

99 Втім, сьогодні міжнародною спільнотою прийнятий у змістовному плані більш лаконічно сформульований термін – «кіберзлочин», що є простим для розуміння навіть не фахівцем із права. Префікс «кібер» дає однозначну відповідь на обстановку вчинення конкретного злочинного явища – це кіберпростір як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій. У вітчизняній криміналістичній науці доволі поширеною є практика використання багатьох запозичених з інших мов термінів, наприклад, тактика (грец. *maktika* – мистецтво шикування військ), криміналістика (лат. *Criminalis*).

100 Для розуміння особливостей процесу розвитку міжнародної наукової думки щодо змісту терміна «кіберзлочин» доцільно вдатися до аналізу результатів багаторічної роботи такого консультативного органу, як Конгрес ООН з попередження злочинності та поводження з правопорушниками. Починаючи з десятого форуму Конгресу (Відень, 2000 рік), жоден (одинадцятий у Бангкоці, 2005 рік; дванадцятий у Сальвадорі, 2010 рік; тринадцятий у Досі, 2015 рік) не оминає теми боротьби з кіберзлочинами. На Десятому форумі Конгресу термін «кіберзлочин» було подано у двох значеннях[51].

[51] Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation / Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, 12–19 Appril, 2015 г. A/CONF.222/12). P. 6. URL : https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf.

Кіберзлочин у вузькому сенсі (синонім до «комп'ютерний злочин», що використовували окремі доповідачі форуму) є будь-яким протиправним діянням, здійснюваним за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних. Кіберзлочини в широкому значенні (як синонім до «злочини, пов'язані з використанням комп'ютерів») – це будь-яке протиправне діяння, вчинене за допомогою або з використанням комп'ютерної системи чи мережі, включаючи й такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі.

Форум Конгресу, датований 2015 роком, є надзвичайно важливим у сенсі практичного роз'яснення проблем та шляхів їх вирішення щодо розслідування кіберзлочинів[52]. 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 відносять 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

[52] Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation / Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, 12–19 Appril, 2015 г. A/CONF.222/12). URL : https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf.

даних і продаж заборонених товарів у режимі онлайн. Міжнародна спільнота також резюмувала, що у внутрішньому (національному) законодавстві про кіберзлочинність відповідальність за такі злочини встановлюється на підставі поєднання положень, що стосуються як суто кіберзлочинів, так і загальнокримінальних злочинів. Наведемо фрагмент офіційної публікації результатів форуму: «Кримінальна відповідальність за здійснення "основних", таких як отримання незаконного доступу до комп'ютерних даних і систем, може встановлюватися шляхом ухвалення спеціального законодавчого положення, тоді як діяння, пов'язані із застосуванням комп'ютерів для отримання особистої або фінансової допомоги або спричинення особистої або фінансової шкоди, найчастіше можуть визнаватися кримінальними на підставі положень, що стосуються здійснення загальнокримінальних (не пов'язаних із застосуванням комп'ютерів) злочинів. У деяких випадках внутрішні нормативно-правові засади приймаються у виконання з урахуванням багатобічних документів, які можуть бути обов'язковими або необов'язковими для сторін»[53].

102 В Україні центральне місце в механізмі правового регулювання боротьби з кіберзлочинами займають норми Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року[54], а також загальні та спеціальні норми КК України, які передбачають численні конвенційні склади таких

[53] Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation / Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, 12–19 Appril, 2015 г. A/CONF.222/12). 10-11 p. URL : https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf

[54] Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. URL : http://zakon3.rada.gov.ua/laws/show/2824-15.

кримінальних правопорушень (про що йшлося у підрозділах 1.1 та 1.2 цього посібника). Більш вдалим з позицій предметної сторони криміналістичної науки можна вважати запозичений з англійської мови термін «кіберзлочин», яким позначаються 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 (зокрема передбачені ст. ст. 129, 161, 163, 176, 185, 190, 200, 229, 231, 232, 300, 301, 361–363-1, 376, 442 КК України).

103 **Особливості криміналістичної характеристики кіберзлочинів.** В основі функціонування такої злочинної діяльності знаходяться зв'язки між наступними елементами, що складають механізм вчинення такої категорії злочинів: предмет посягання (матеріальні цінності, грошові кошти, інформація тощо); слідові картина злочину (в матеріальному та електронному середовищах) та обстановка його вчинення; особа злочинця; способи вчинення злочинів (підготовки, безпосереднього вчинення та приховування). Визначення типових та специфічних ознак наведених елементів механізму кіберзлочинів та зв'язків між цими елементами допоможе визначити особливості криміналістичної характеристики кіберзлочинів.

104 **Характеристика предмета посягання.** При вчиненні кіберзлочину можна говорити про систему предметів посягання, яку зумовлює полімотивованість злочинної діяльності в обстановці кіберпростору. Первинними предметами посягання у кіберпросторі є інформаційний продукт та інформаційний ресурс. Вторинними предметами посягання виступають майно (грошові готівкові або безготівкові кошти, товари), комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи. Акцентуємо свою увагу на першій групі.

105 Інформаційний продукт – це інформація/відомості, що зафіксовані в електронній формі, як результат задоволення потреб користувача/ів кіберпростору. М. В. Карчевський слушно робить акцент на цінності інформації[55], яка буває різною: може бути цінною по суті, оскільки є результатом тривалої роботи великої кількості осіб, або цінною за призначенням, оскільки її наявність є необхідною умовою для вирішення певного завдання, наприклад, отримання доступу до банківських рахунків, персональні або особисті дані. Інформаційний продукт як предмет посягання повинен бути чужим для злочинця та мати законного користувача/ів, що закономірно пов'язано з характером зафіксованих у ньому відомостей (наприклад, твір як об'єкт авторського права, персональні дані, банківська таємниця тощо). Тож, цінність інформаційного продукту, пов'язана з характером зафіксованих у ньому відомостей, зумовлює обрання злочинцем останнього для здійснення на нього впливу, що скерований загальним мотивом злочинної діяльності. Доступ сторонніх осіб до таких продуктів обмежений на підставі закону, зокрема ними виступає «інформація з обмеженим доступом» та результат чужої інтелектуальної праці.

106 У Законі України «Про доступ до публічної інформації» конкретизовані загальні вимоги при обмеженні доступу до інформації та правовий статус кожного з видів інформації[56]. Втім, з практичних міркувань доцільно розглядати інформацію з обмеженим доступом у контексті змісту та суб'єкта, що нею володіє. Тому традиційно у теорії інформаційного права вона поділяється на:

---

[55] *Карчевський М. В.* Злочини у сфері використання комп'ютерної техніки : навч. посібник. Київ : Атіка, 2010. С. 60.

[56] Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL : https://zakon.rada.gov.ua/laws/show/2939-17

1) державну таємницю (секретну інформацію);
2) конфіденційну інформацію, що охоплює інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Конфіденційна інформація поділяється на: інформацію 107
про особу (персональні дані); інформацію, що є власністю держави (службова таємниця або інформація для службового користування); комерційну таємницю; професійну таємницю (серед якої розрізняю лікарську, адвокатську, нотаріальну, страхову, банківську та деякі інші види таємниці); банківську таємницю[57]. Аналіз матеріалів судово-слідчої практики дозволяє визнати, що кіберзлочинець типово посягає на персональні дані (20 % проваджень), банківську (50 %), державну (20 %) та комерційну (10 %) таємницю.

Результат чужої інтелектуальної праці в кримінально- 108
правовій сфері має форму об'єктів авторського права або суміжних прав. В результаті аналізу судово-слідчої практики розслідування кіберзлочинів можна визначити, що серед об'єктів авторського права та суміжних прав предметами незаконного відтворення, розповсюдження та тиражування (щодо об'єктів суміжних прав) у кіберпросторі найчастіше виступають: аудіовізуальні твори (традиційно фільми, що вийшли у прокатний показ) (50 %), бази даних (компіляції даних) (10 %), комп'ютерні програми (10 %) фонограми та передачі організацій мовлення (30 %).

Інформаційний ресурс як предмет посягання. Сукупність 109
інформаційних продуктів, організована за допомогою певної інформаційної технології, у загальному розумінні виступає

[57] *Кормич Б. А.* Інформаційне право : підручник. Харків, 2011. 334 с.; *Марущак А. І.* Інформаційне право: доступ до інформації : навч. посібник. Київ, 2007. 531 с.

електронним інформаційним ресурсом. В галузі телекомунікацій ресурси (*information sourses*) – це систематизовані масиви інформації створювані та накопичувані у мережі з використанням інформаційних технологій і призначені для багаторазового запитування користувачами[58]. До традиційних сьогодні форм організації ресурсу належать: файли, бази та банки даних, електронні системи, сайти[59]. Можливість використовувати інформаційний ресурс як знаряддя задля досягнення кінцевої мети злочинної діяльності зумовлює обрання злочинцем певного інформаційного продукту/ресурсу для злочинного впливу на нього. Таким ресурсом типово виступають:

- попередньо створений злочинцем файл, наприклад, шкідливий за призначенням з метою подальшого завантаження у систему та збору інформації з обмеженим доступом, або що містить зображення порнографічного характеру;
- веб-сайт, що використовується для розповсюдження порнографічних предметів, розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію тощо;
- автоматизовані (електронно-інформаційні) системи різного призначення (платіжні системи, системи що забезпечують диспетчерське керування, повітряним або залізничним рухом, митне оформлення, поштові

[58] *Кормич Б. А.* Інформаційне право : підручник. Харків, 2011. 334 с.; *Марущак А. І.* Інформаційне право: доступ до інформації : навч. посібник. Київ, 2007. С. 34

[59] Інформаційне право та правова інформатика : курс лекцій / [В. Г. Хахановський, І. В. Мартиненко, В. М. Смаглюк та ін.] ; за заг. ред. Є. М. Моісеєва. Київ : Київ. нац. ун-т внутр. справ, 2007. 253 с.; *Соснін О. В.* Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.

відправлення тощо). Відсоткові показники стосовно поширеності тих чи інших інформаційних ресурсів як предмета посягання не уявляється можливим навести. Адже аналіз матеріалів кримінальних проваджень досліджуваної категорії злочинів свідчить про типову неспроможність суб'єкта розслідування встановити всі обставини вчинення кожного зі злочинів злочинної сукупності, а тому досить часто не всі ресурси, що стали предметом посягання у механізмі злочинної діяльності у кіберпросторі, встановлюються.

Характеристика обстановки вчинення кіберзлочину та слідової картини. Безпосередньо кіберпростір виступає обстановкою вчинення кіберзлочину. Правники, політологи неодноразово вдавалися до спроб надати визначення поняття «кіберпростір», але одностайності щодо сутності кіберпростору навіть у науках кримінального циклу досягти не вдалося[60]. Джон Барлоу – автор праці «Декларація незалежності кіберпростору» – зазначав, що електронний інформаційний простір має два рівні: 1) обмін інформацією у формі програмних кодів, який здебільшого й створює кіберпростір; 2) віртуальні життя, створювані внаслідок обміну інформацією між аватарами[61] (так

[60] *Білєнький В. П.* Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльно-правове дослідження) : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2016. 20 с.; *Дубов Д. В.* Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ, 2014. 328 с.; *April M.M.* Norm Origin and Development in Cyberspace: Models Of Cybernorm Evolution. *Washington University Law Quarterly*. 2000. No. 78. P. 59–80; *Гавловський В.* Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2000. С. 50–53.

[61] *Barlow J. P.* A Declaration of the Independence of Cyberspace. URL : https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

традиційно називають користувачів мережі). Тож, кіберпростір утворюється в результаті взаємодії між людьми шляхом обміну інформацією в електронній цифровій формі. Тому для розуміння сутності кіберпростору як специфічної обстановки вчинення кримінального правопорушення необхідно враховувати його подвійну природу: технічну та соціальну.

111 Деякі криміналісти розглядають кіберпростір у контексті місця вчинення злочину як місця, де не діють географічні та юридичні категорії. Проте це не так.

112 Технологічна складова кіберпростору уможливила утворення під час вчинення злочинів у кіберпросторі, крім традиційних у криміналістичному сенсі слідів (слідів-відображень, слідів-предметів та слідів-речовин), також «інформаційних»[62], «віртуальних» або «цифрових»[63] слідів – так званих нетрадиційних слідів, що містяться в електронному середовищі[64]. Фактично ж останні у вигляді будь-яких змін інформації містяться в предметах матеріального світу – конкретних технічних або комбінованих засобах автоматизованої обробки інформації. З огляду на віддаленість доступу до предмета посягання як особливість кіберпростору, завдяки якій він набув активного використання під час вчинення злочину, аксіомою варто визнати той факт, що сліди злочину в електронному середовищі відбиваються одночасно в багатьох апаратних засобах комп'ютерної техніки,

---

[62] *Голубєв В. О.* Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. С. 146.

[63] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

[64] *Самойленко О. А.* Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. С. 89.

комп'ютерної мережі або електронної комунікаційної мережі, мережі електрозв'язку. Останні ж фізично перебувають на чітко визначеній географічній території під юрисдикцією певної держави та у власності конкретної особи.

Характеристика особи злочинця. Злочинець, що вчиняє 113
кіберзлочин, фактично завжди виступає користувачем комп'ютерів. Маркетологи з ринку праці визначають такі їх фахові рівні: користувач, упевнений користувач, досвідчений користувач, користувач професійного рівня. Критеріями такої диференціації слугують кількість програм, які опанував користувач; ступінь опанування ним кожної з програм; рівень професійної самооцінки. Однак формальне застосування такого роду підходів для типізації особи злочинця не матиме практичного сенсу з позицій формулювання типових версій про особу злочинця. Адже професійний рівень користувача не відображає всього спектру ознак злочинця, активно задіяних у процесі детермінації механізму злочину. Професіональний рівень користувача як злочинця зумовлений певною сукупністю ознак, як-от: 1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів); 2) мобільність злочинця (індивідуальна професійна, соціальна або географічна)[65]; 3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети; 4) роль у складі організованої злочинної групи.

Спираючись на узагальнення матеріалів національної 114
судово-слідчої практики й на підставі вказаних критеріїв визначення професіональності (кваліфікації) злочинця можна певною мірою типізувати та охарактеризувати особу, що вчиняє кіберзлочин:

[65] *Стрюк М. І., Семеріков С. О., Стрюк А. М.* Мобільність: системний підхід. *Інформаційні технології і засоби навчання*. 2015. № 5. Т. 49. С. 37–70.

1) злочинець-користувач початкового рівня: особа не використовує технології анонімізації доступу до ресурсів Інтернет, має високу соціальну мобільність, характеризується відсутністю конкуренції мотивів;
2) злочинець-звичайний користувач: особи при використанні технології анонімізації доступу до ресурсів мережі Інтернет припускається вагомих помилок, має усереднені показники всіх видів мобільності, а конкуренція мотивів наявна лише за умови діяльності його в складі мережевої злочинної групи;
3) злочинець-упевнений користувач: особа пов'язана з організацією-жертвою за трудовою угодою або має особисті стосунки з фізичною особою-жертвою, вдало використовує технології анонімізації доступу, характеризується достатнім рівнем соціальної та професійної мобільностей; типовим первинним джерелом інформації про такого злочинця є заява або повідомлення про вчинення кримінального правопорушення;
4) злочинець-досвідчений користувач: особа має більш високий рівень професійної мобільності порівняно із злочинцем-упевненим користувачем, у разі невикриття правоохоронними органами першого вчиненого ним злочину досвідчений користувач підвищує свій професійний рівень, часто відмовляється від участі в організованій злочинній групі та розпочинає індивідуальну злочинну діяльність;
5) злочинець користувач-професіонал: особа характеризується використанням технологій анонімізації доступу до ресурсів Інтернет, високим рівнем індивідуальної професійної, соціальної та географічної мобільностей, складністю його злочинної діяльності (що визначає психотип злочинця), в цілому найбільш високим рівнем

кваліфікації, що вимагає максимальної концентрації зусиль працівників поліції.

Характеристика способів вчинення злочину. З метою 115
класифікації способів вчинення кіберзлочинів необхідно враховувати не лише фактичний спосіб дії злочинця, а й інформаційно-комунікаційні технології (кібертехнології), що були покладені в основу досягнення кінцевої злочинної мети. Адже саме вони виконують функцію елемента, що забезпечує інтерактивну взаємодію способів підготовки, вчинення та приховування злочину. Враховуючи сучасну практику боротьби із кіберзлочинами типові в Україні способи їх вчинення можна класифікувати так:

1. Способи злочинних дій, пов'язані з функціонуванням соціально орієнтованих мереж (від англ. *social networks*), діяльність яких заснована на так званій вікі(*viki*)-технології. Остання є технологією побудови Web-системи, призначеної для колективної розробки, зберігання, структурування тексту, гіпертексту, файлів, мультимедіа. Зазвичай злочинець початкового рівня та рівня користувача з метою доведення до відома необмеженої кількості користувачів соціальної мережі, а також сповіщення всіх користувачів мережі, яких додано до розділу «Друзі» цього акаунту, розміщує (з власного комп'ютера або здійснює так званий «репост» – поширення з іншого електронного джерела) на сторінці фото-, відеофайли, інші форми публікації протизаконного характеру, що містять: порнографію (часто дитячу); пропаганду культу насильства та жорстокості, расової, національної та релігійної нетерпимості, війни, комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів тощо. Способи підготовки пов'язані зі завантаженням, пошуком,

створенням, зберіганням, редагуванням відповідних текстових, фото-, відеофайлів або інших форм публікації. Способи приховування найчастіше не застосовують.

2. Способи злочинних дій, пов'язані з функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому або громадськості. Злочинці-користувачі вдало застосовують цю технологію для розповсюдження через Інтернет комп'ютерних програм, аудіовізуальних творів, баз даних (компіляції даних), фонограм та організації мовлення з порушенням авторського або суміжних прав шляхом їх розміщення для копіювання в мережі, а також творів, що мають порнографічний характер, шляхом надання доступу до них користувачам.
3. Способи злочинних дій, пов'язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури «BBC»). Нині шахрайські дії масово вчиняються шляхом розміщення оголошення щодо продажу користувачам інтернет-сайту будь-якого матеріального предмета, причому злочинець не має наміру поставляти його покупцеві. Зловмисник запевняє потерпілого, що відправить замовлений товар кур'єрською/поштовою службою після отримання ним як передоплати грошових коштів, для чого використовуються можливості різноманітних платіжних систем та сервісів Інтернет-банкінгу.
4. Способи злочинних дій, пов'язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет. Терміном «технології електронної комерції» позначають різноманітні принципи, яким має відповідати програмне забезпечення та сервіси для електронної комерції. Саме для них підтримуються так

звані відкриті інтернет-стандарти. Власне, здійснюється стандартизація всіх форм взаємодії між організаціями, залученими в повний цикл «постачання–продаж–купівля (англ. *Supply–Selling–Buying*)». Сюди відносять технології електронного обміну інформацією (англ. *Electronic Data Interchange*, *EDI*), електронного руху капіталу (англ. *Electronic Funds Transfer*, *EDF*), електронної торгівлі (англ. *E-trade*), обігу електронних грошей (англ. *E-cash*), електронний маркетинг (англ. *E-marketing*), електронний банкінг (англ. *E-banking*), електронні страхові послуги (англ. *E-Insurance*) тощо[66]. На підставі аналізу матеріалів кримінальних проваджень можна назвати такі поширені групи способів злочинних дій з використанням технологій електронної комерції: 1) замовлення на сайті, що здійснює електронну торгівлю (діє аналогічно до електронної дошки оголошень), товарів, що мають особливий порядок обігу, та їх отримання у формі внутрішнього або міжнародного поштового відправлення; 2) розповсюдження через сайти, які спеціалізуються на трансляції відеозображень еротичного та порнографічного характеру відеопродукції, зображень порнографічного характеру, створення та організація функціонування «студій» з виготовлення та розповсюдження такої відеопродукції, забезпечення її трансляції та зображень у режимі онлайн (з використанням режиму «*Private chat*»), а також можливе одночасне створення та адміністрування відповідних сайтів; 3) надання можливості відвідувачам створеного веб-сайту переглядати або копіювати аудіовізуальні твори, комп'ютерні програми, фонограми, права на які належать іншій особі.

[66] *Шалева О. І.* Електронна комерція : навч. посібник. Київ : Центр учб. літ., 2011. С. 10.

5. Способи злочинних дій, пов'язані з функціонуванням технології електронної розсилки (*e-mail*, від англ. *electronic mail*); IP-телефонії (найчастіше через комп'ютерну програму Viber; програмне забезпечення із закритим кодом Skype). Часто злочинець надсилає потерпілому неправдиву інформацію у формі масової розсилки для введення останнього в оману з метою отримання від нього інформації, потрібної для подальшого здійснення ним трансакції (спосіб підготовки шахрайства). Показовим є приклад щодо шахраїв, яких було викрито влітку 2017 року поліцейськими Департаменту кіберполіції. Злочинці за допомогою смс-розсилки на території Київської області завдали громадянам збитків близько на 150 000 грн. Зловмисники розсилали смс-повідомлення через організовану злочинною групою мережу «фішингових сайтів», посилання на які надходили громадянам. Злочинці використовували у своїй «діяльності» дві схеми незаконного збагачення: 1) повідомляли громадян про виграш автомобіля та шахрайським шляхом виманювали у них гроші; 2) рекомендувалися працівниками банку та повідомляли про несанкціоновані дії з картою, для припинення яких пропонували повідомити cvv-код картки, після отримання якого знімали з банківського рахунку всі кошти[67].
6. Способи злочинних дій, пов'язані з функціонуванням технологій електронних платіжних систем (англ. *electronic payment systems*), призначені для здійснення платіжних операцій через мережу Інтернет. За допомогою платіжної

[67] Кіберполіція викрила шахраїв, що за допомогою СМС-розсилки ошукували громадян. URL : https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-shaxrayiv-shho-za-dopomogoyu-sms-rozsylky-oshukuvaly-gromadyan-foto-2963

системи здійснюються оплати різного призначення, тому досить часто цю технологію використовують одночасно з технологією електронної комерції. Типовий спосіб дій злочинця полягає у створенні фіктивних сайтів, через які від потерпілих за різні послуги або товари приймаються електронні платежі.

7. Способи злочинних дій, пов'язані з функціонуванням шкідливого програмного забезпечення (з англ. «*crimeware*», де «*crime* – злочинність, *software* – програмне забезпечення; часто як синонім застосовують «вірус»). Це програмне забезпечення злочинці (за типами «впевнений користувач», «досвідчений користувач» та «професіонал») за власною ініціативою або на замовлення третьої особи розробляють та/або поширюють для отримання несанкціонованого доступу до комп'ютера з метою несанкціонованого доступу до інформації та спричинення шкоди.

Знання типових способів вчинення кіберзлочинів дозволить 116
слідчому в перебігу розслідування конкретного кримінального правопорушення якісно та методично обґрунтовано поставитися до висування версій, організації та планування досудового розслідування.

Особливості початку кримінального провадження щодо 117
кіберзлочинів. З позицій слідчої практики процесуальний порядок початку кримінального провадження триває з моменту, коли суб'єкту розслідування стало відомо про джерело обставин, що можуть свідчити про кримінальне правопорушення, до моменту внесення відповідної інформації до ЄРДР. Внутрішня організація слідчим початку кримінального провадження залежатиме від чинників як правового, так і організаційного характеру. Правові чинники пов'язані з характером джерела

обставин[68], що можуть свідчити про вчинення певного виду кримінального правопорушення. При вчиненні кіберзлочинів заяви та повідомлення осіб про вчинений злочин та ініціативні рапорти співробітників оперативного підрозділу типово виступають джерелами обставин про злочин.

118 Із заявами та повідомленнями про вчинений кіберзлочин звертаються як правило власники певного інформаційного продукту/майна, особи, що стали жертвами насильницьких, дискримінаційних дій у кіберпросторі, представники установи-жертви, Інтернет-сервісу, власники веб-сайту, що зазнав злочинного впливу. В арсеналі способів дії слідчого є опитування, огляд місця події та організаційні заходи у формі звернення до відкритих джерел інформації з метою підтвердження отриманих відомостей. Внесення до ЄРДР відомостей про кримінальне правопорушення, викладених у цьому джерелі інформації, є обов'язком слідчого, відповідне процесуальне рішення й приймається упродовж визначених законом 24 годин з моменту реєстрації уповноваженими працівниками чергової частини таких заяв і повідомлень.

119 Окрему увагу привертають ініціативні рапорти співробітників оперативного підрозділу про виявлення ними кримінального правопорушення та долучені до них матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп, відповідальність за які передбачена КК України. До суб'єктів оперативно-розшукової діяльності, перед якими прямо стоїть завдання щодо виявлення кіберзлочинів та протидії, належать Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

---

[68] *Никифорчук Д. Й.* До питання використання результатів оперативно-розшукової діяльності у кримінальному судочинстві. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. Вип. 22. С. 61–66.

та Департамент кіберполіції Національної поліції України (далі ДКП).

Звернення осіб до підрозділів ДКП НП України здійснюється 120
шляхом особистого відвідування відділення кіберполіції, відправлення листа поштою або більш поширеного сьогодні подання електронного звернення через опцію «Форма подачі електронного звернення» на офіційному вебсайті ДКП. Останній спосіб звернень функціонує на вебсторінках правоохоронних органів на підставі вимог Закону України «Про внесення змін до Закону України "Про звернення громадян" щодо електронного звернення та електронної петиції». Перевірка такого звернення, як правило, обґрунтовано є результативною з позиції прийняття в подальшому слідчим рішення про початок провадження за такими матеріалами. Адже в цій ситуації не діє фактор часу: електронні повідомлення миттєво отримує співробітник спеціально створеного (для аналізу звернення та його перевірки) відділу в ДКП, а заявник зазвичай сам зацікавлений у розгляді свого звернення.

Якщо інформація стосується тяжких та особливо тяжких 121
кіберзлочинів, що готуються, то оперативно-розшукову діяльність здійснюватимуть у межах плану заходів з реалізації матеріалів оперативно-розшукової справи, який згідно з Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами НП України затверджують начальники оперативного підрозділу й органу досудового розслідування. Оскільки цією Інструкцією на керівників органу досудового розслідування та оперативних підрозділів (за посадовими інструкціями) покладено однакові обов'язки щодо забезпечення збору, накопичення, систематизації отриманої інформації та здійснення її перевірки з метою встановлення осіб, які вчинили кримінальні правопорушення, а також подій і фактів, які можуть сприяти їх розкриттю та

досудовому розслідуванню, то спільна узгоджена діяльність слідчого й оперативного працівника для початку кримінального провадження стала правилом, а не рекомендацією.

122 **Особливості початкового етапу розслідування кіберзлочинів.** Процес діяльності слідчого з розслідування кримінального правопорушення традиційно чітко визначений часовими межами здійснення досудового розслідування як стадії кримінального провадження та традиційно поділяється на два етапи: початковий та наступний. Науковці-криміналісти та практики в цілях структурування кожної окремої криміналістичної методики в межах вказаних етапів розглядають типові слідчі ситуації, тактичні завдання, версії та програми (алгоритми) дій слідчого.

123 У сучасних умовах розвитку інформаційних (комп'ютерних) технологій важливого значення набуває можливість персоналізувати особу конкретного користувача як злочинця-користувача. Ця можливість виникає за умови визначеності у матеріалах, що передані слідчому в рамках процесу початку кримінального провадження, відомостей про користувача вебсторінки соціальної мережі, дошки оголошень чи іншій технології, що використовується у механізмі вчинення злочину, дані абонентського номера користувача, його IP-адреси, MAC-адреси обладнання, що використовувалось при вчиненні або готуванні кіберзлочину. Тож, можна охарактеризувати такі типові слідчі ситуації початкового етапу розслідування кіберзлочинів.

124 1. Кримінальне провадження розпочато в результаті отримання повідомлення особи про кримінальне правопорушення, в якій містяться розгорнуті відомості (персоналізована інформація) про особу злочинця. Характерна при вчиненні кіберзлочину внутрішнім користувачем мережі, наприклад, така особа може бути виявлена в результаті

внутрішньої перевірки в установі-жертви (аудит, технічна перевірка, моніторинг кіберпростору). Процес розслідування значно спрощений, основними тактичними завданнями є: забезпечення збереження документів, у яких фіксують роботу комп'ютерної мережі; встановлення співучасників злочину (кола осіб, що мали змогу здійснити злочин разом); забезпечення відшкодування матеріальних збитків; встановлення злочинних зв'язків між співробітниками установи-жертви. До типового комплексу слідчих (розшукових) дій будуть входити: допити службовців і посадових осіб; тимчасові доступи до речей і документів (інформація в електронній системі банку; нормативні акти та документи, що регламентують операційну роботу банку, установи, бухгалтерський облік, внутрішньобанківський контроль; функціональні обов'язки працівників; журнали й інші документи, у яких фіксують роботу оператора операційного дня банку, журнали перевірки технічного стану системи банку тощо);слідчі огляди вилученого; затримання та обшуки; призначення комп'ютерно-технічної експертизи; накладення арешту на майно і вклади.

2. Кримінальне провадження розпочато в результаті 125
отримання заяви особи про кримінальне правопорушення, в якій містяться неперсоналізовані відомості про особу злочинця, наприклад, дані абонентського номера користувача, його IP-адреси, MAC-адреси обладнання. Ситуація характерна при вчиненні або готуванні кіберзлочину з насильницьких, дискримінаційних мотивів, окремих випадках шахрайських дій. Тут потрібно акцентувати на тому, що така заява особи іноді продиктована необхідністю реалізації оперативної інформації про нетяжкі та середньої тяжкості кіберзлочини, що була отримана в ході роботи ДКП.

Перед слідчим постають такі типові тактичні завдання: 126
персоналізувати особу злочинця та її затримати; встановити всіх

потерпілих; забезпечити збереження віддалених електронних носіїв інформації, у яких зафіксовано роботу злочинця в мережі; встановити співучасників злочину; забезпечити відшкодування матеріальних збитків і можливої конфіскації майна. До комплексу слідчих (розшукових) дій обов'язково входять: проведення оперативним підрозділам негласних та слідчих (розшукових) дій з метою персоналізації відомостей про користувача як злочинця та встановлення всіх потерпілих; призначення та проведення комп'ютерно-технічної та/або мистецтвознавчої експертиз, остання щодо матеріалів, що містяться на поданих на дослідження CD-R дисках (відеозаписи, отримані внаслідок здійснення контролю за вчиненням злочину, якщо він проводився за дорученням слідчого підрозділу ДКП), допити потерпілих; тимчасові доступи до речей і документів; обшук за місцем мешкання запідозрених осіб; допити свідків.

127 3. Кримінальне провадження розпочато в результаті перевірки оперативної інформації, в результаті якої особа злочинця персоналізована або про неї містяться розгорнуті неперсоналізовані відомості. Характерна при розслідуванні тяжких конвенційних кіберзлочинів злочинцем-звичайним або упевненим користувачем, типово в ході міжнародної співпраці щодо виявлення фактів поширення дитячої порнографії або інтелектуального піратства мережі Інтернет. Основними тактичними завданнями в цій ситуації є: персоналізація особи злочинця (якщо вона неперсоналізована); затримання злочинця/ців; забезпечення збереження електронних носіїв інформації; встановлення інших фактів вчинення кіберзлочинів. До комплексу заходів пізнання слідчого входять: доручення оперативному підрозділу в порядку ст. 40 КПК України на проведення оперативних заходів і слідчих (розшукових) дій, зокрема для зняття інформації з електронних комунікаційних мереж, з електронних інформаційних систем; особистий огляд

затриманих; доручення ДКП на проведення оперативно-розшукових заходів з метою персоналізації відомостей про інших користувачів; слідчий огляд вилученого майна; проведення обшуків за місцем мешкання, роботи затриманих при вчиненні злочину.

4. Кримінальне провадження розпочато в результаті 128
перевірки оперативної інформації, втім у матеріалах відсутні будь-які відомості про особу злочинця. Ситуація є типовою при розслідуванні організованої злочинної діяльності, що пов'язана із заволодінням майном шляхом незаконних операцій з використанням електронно-обчислювальної техніки. На момент внесення інформації до ЄРДР наявні відомості про потерпілих у інших кримінальних провадженнях, їх допитано, відомий механізм вчинення злочину, однак через методи конспірації майже немає інформації про членів організованої групи, їх кількість, кількість епізодів злочинної діяльності. Слідчий, об'єднуючи кілька кримінальних проваджень в одне, отримує широкий спектр основних завдань розслідування, зокрема: подолання методів конспірації злочинної діяльності групи; здійснення документування злочинної діяльності; встановлення всіх осіб, які входять у злочинну групу; з'ясування фактів вчинення інших злочинів, не пов'язаних із відомим механізмом злочинної діяльності; виявлення суб'єктного складу щодо кожного з епізодів злочинної діяльності; встановлення осіб у складі групи, які не були обізнані щодо вчинення злочину (виконували дії, які не заборонені законодавством України (наприклад, адміністративні або технічні функції, розроблення сайту, надання послуг з його розміщення тощо); виявлення зв'язків між учасниками групи; визначення ролей кожного учасника групи щодо кожного окремого епізоду злочину; встановлення механізмів легалізації незаконно отриманих доходів. Це дуже складна слідча ситуація, при якій реалізується

весь арсенал типових тактичних операцій розслідування кіберзлочинів, зокрема: «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи» (до якої входять контроль за вчиненням злочину; зняття інформації з електронних комунікаційних мереж (електронних інформаційних систем) конкретного абонента); «Встановлення технології злочинної діяльності з використанням кіберпростору» (аудіо-, відеоконтроль особи та/або місця; спостереження за особою, річчю або місцем/дослідженням публічно недоступних місць, житла або іншого володіння особи; виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації тощо). У доктрині акцентують увагу на стійкості груп, що вчиняють корисливі злочини з використанням комп'ютера. Утім безапеляційне використання цього теоретичного положення в практичній діяльності слідчого може призвести до неповноти розслідування в конкретному кримінальному провадженні. Постійними учасниками групи часто є організатор, співорганізатори та спеціаліст, викриття останнього є ключовим моментом для розуміння механізму та кількості «злочинних проектів» таких груп.

129 5. Кримінальне провадження розпочато в результаті діяльності оперативних підрозділів згідно зі спільним зі слідчим планом реалізації матеріалів оперативно-розшукової справи за відсутності будь-яких відомостей про особу злочинця. Ця ситуація є характерною при виявленні ознак готування до злочинів, пов'язаних зі сферою захисту інформації з обмеженим доступом, яку обробляють в автоматизованих системах, до злочинів або щодо серії тяжких та особливо тяжких конвенційних кіберзлочинів. Конкретизуються такі тактичні завдання: здійснення документування злочинної діяльності; встановлення та подолання засобів конспірації злочинної

діяльності; забезпечення своєчасність прийняття управлінських й організаційних рішень; забезпечити конфіденційність осіб, які співпрацюють з правоохоронними органами, під час здійснення розслідування означеної злочинної діяльності. Окреслені завдання розслідування можна реалізувати шляхом проведення комплексу дій та заходів: зняття інформації з електронних інформаційних систем; контроль за вчиненням злочину; тимчасовий доступ до речей і документів, що містять інформацію на серверах операторів зв'язку; інформацію банківських установ про конкретний рахунок, що був використаний, наприклад, для переведення коштів злочинцю під час контролю за вчиненням злочину; обшуки за місцем роботи та мешкання; затримання одного зі співучасників злочину. Одночасно з допитом підозрюваних осіб призначають комплекс судових експертиз (комп'ютерно-технічна, судово-почеркознавча, технічна експертиза документів тощо). За умови встановлення конфіденційного співробітництва принаймні з одним можливим підозрюваним може бути також реалізована тактична операція «Встановлення технології злочинної діяльності у кіберпросторі».

Наведені типові слідчі ситуації початкового етапу 130
розслідування кіберзлочинів, відповідні їм тактичні завдання та засоби розв'язання останніх спрямовані на встановлення злочинної діяльності в повному обсязі, кожного суб'єкта злочину та тяжкості його обвинувачення.

Особливості наступного етапу розслідування кіберзлочинів. 131
Слідчі ситуації наступного етапу розслідування, зумовлені ними комплекси тактичних завдань і засоби виконання останніх традиційно корегувалися із ставленням підозрюваного до розслідування злочину; наявність протидії з боку підозрюваного визначала складність ситуації наступного етапу розслідування.

132 Втім, сьогодні можна висновувати про принципово новий характер діяльності слідчого на наступному етапі розслідування, він пов'язаний із сучасною інформаційною моделлю злочину, яка має ознаки багатоепізодної злочинної діяльності, зумовлена необхідністю виявлення злочинного наміру встановленої або невстановленої особи співучасника злочину, специфікою розподілу ролей учасників злочинної групи під час вчинення злочину організованою групою. Аналіз матеріалів практики розслідування кіберзлочинів засвідчують, що ступінь складності, трудомісткості досудового розслідування злочинів пов'язаний, сьогодні передусім, із кількістю епізодів злочинної діяльності й осіб, які брали в ній участь або продовжують її вчиняти. Відповідно до загального стану розслідування на момент реєстрації в ЄРДР інформації щодо висунення першої законної та обґрунтованої підозри, а також зайнятої підозрюваним у кримінальному провадженні позиції на наступному етапі розслідування кіберзлочинів може бути виокремлено дві типові слідчі ситуації.

133 1. Сприятлива слідча ситуація розслідування, що характеризується повнотою виконання тактичних завдань розслідування, конкретизацією зайнятих кожним з підозрюваних у кримінальному провадженні позицій. Однаково поширеними є два її різновиди:

1.1. неускладнена сприятлива ситуація, що складається за умови збігу позицій підозрюваних осіб та співпраці їх зі слідством;

1.2. ускладнена сприятлива ситуація, що наявна за умови розбіжності позицій декількох підозрюваних. З тактичних позицій ця ситуація вимагатиме виконання таких тактичних завдань розслідування, як подолання протидії розслідуванню; усунення суперечностей між джерелами доказового значення; забезпечення збереження вже

отриманих джерел доказів. До комплексу засобів їх розв'язання можна віднести: комплекс одночасних допитів декількох осіб (з метою подолання суперечностей у показаннях); комплекс слідчих експериментів (з кожним виконавцем злочину); допити свідків (понятих і спеціалістів); подальші організаційні заходи, спрямовані на збирання матеріалів, що характеризують особу підозрюваного; додаткові допити підозрюваних.

2. Несприятлива слідча ситуація розслідування. Їй 134
притаманні виконання різнопланових пізнавальних завдань розслідування та невизначеність зайнятої підозрюваним(ми) у кримінальному провадженні позиції.

Для розуміння завдань наступного етапу розслідування 135
можна навести приклад щодо групи осіб, які за попередньою змовою шляхом несанкціонованого втручання в роботу мереж суб'єкта господарювання незаконно ретранслювали телевізійні канали, право на яке має цей суб'єкт, унаслідок чого група осіб здійснила порушення встановленого порядку маршрутизації інформації електрозв'язку й авторських і суміжних прав шляхом незаконного відтворення програм мовлення. Злочинна діяльність попередньо була кваліфікована за ч. 2 ст. 361 КК України, дії одного з встановлених учасників групи під час оголошення підозри були кваліфіковані за ч. 1 ст. 176 КК України, втім у результаті негласних слідчих (розшукових) дій на початковому етапі розслідування вбачаються ознаки ч. 2 вказаної статті. Тож, на наступному етапі розслідування постають тактичні завдання щодо встановлення кількості епізодів злочинної діяльності; суми завданого суб'єкту господарювання збитку; власників (правовласників) авторських і суміжних прав; інших осіб, які залучені в механізм вчинення злочину (наприклад, були висунуті версії: правопорушення може також учинити особа, яка раніше працювала зі суб'єктом

господарювання та займалася встановленням супутникового телебачення, здійснювала розповсюдження смарт-карток для перегляду телеканалів; цього не змогли встановити на початковому етапі розслідування у зв'язку із заходами конспірації безпосереднього виконавця злочину). Для розв'язання таких завдань та перевірки висунутих версій можна провести комплекс заходів: тимчасові доступи до речей і документів у банках щодо всіх осіб, які причетні до вчинення цього кримінального правопорушення, встановлення IP-адрес, з яких відбувалися перекази грошових коштів; тимчасові доступи до речей і документів постачальника електронних комунікацій; призначення експертизи об'єктів інтелектуальної власності з метою конкретизації матеріальної шкоди право власнику. Аналіз інформації від постачальників електронних комунікаційних послуг щодо конкретних абонентів і точок доступу (у межах виконання вимог ст. 93 КПК України), які були споживачами контенту або адміністраторами сайту, допоможе запланувати подальші дії, виявити інших осіб, що адміністрували сайт, який використовували для протиправної ретрансляції телеканалів.

136 Наприкінці зазначимо, що перспективним напрямом розроблення окремих криміналістичних методик є програмування процесу розслідування. Запропоновані нами щодо кіберзлочинів особливості їх криміналістичної характеристики, слідчі ситуації розслідування, а також проміжні тактичні завдання та комплекси слідчих (розшукових) дій виступатимуть базою для подальших науково-теоретичних та практичних розробок методик розслідування окремих видів кіберзлочинів, а також злочинів, вчинених у складі організованих мережевих груп.

Опрацювавши подані нижче кейси, охарактеризуйте спосіб вчинення кіберзлочину, знаряддя його вчинення та предмет посягання.

КЕЙС 1. *В описаній фабулі наявне несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатимуть комп'ютерна техніка підозрюваних, з якої здійснювалося несанкціоноване втручання (до прикладу, апаратно-програмні комплекси, які забезпечували функціонування ботоферми; сім-карти, що використовувалися для створення та подальшого ведення технічних акаунтів; «Proxy»-сервери для підміни IP-адрес та уникнення блокування відповідних інтернет-ресурсів).*

КЕЙС 2. *В описаній фабулі наявне створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатиме комп'ютерна техніка підозрюваного з адмін-панеллю доступу до заражених комп'ютерів шкідливим програмним забезпеченням, його інсталяційні файли.*

КЕЙС 3. *В описаній фабулі наявне: а) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; б) несанкціонований 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. Їх предметом є відповідне коло інформаційних (автоматизованих),*

електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, та інформація з обмеженим доступом, яка ними передавалася. Знаряддям виступатиме комп'ютерна техніка підозрюваних з підтвердженнями незаконної діяльності.

КЕЙС 4. *В описаній фабулі наявна несанкціонована зміна 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. Його предметом є інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, а знаряддям виступатиме робочий комп'ютер підозрюваного, з якого останній отримував доступ до відповідної інформації.*

КЕЙС 5. *В описаній фабулі наявні: а) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; б) 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. Їх предметом є відповідне коло: а) інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; б) електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а знаряддям виступатиме комп'ютерна техніка підозрюваного, з якої здійснювалося несанкціоноване втручання та масове розповсюдження повідомлень.*

Запитання для самоконтролю

1. Назвіть суб'єктів оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів?
2. Назвіть типові джерела оперативної інформації про кіберзлочини?
3. Окреслить чинники, що зумовлюють форми початку кримінального провадження.
4. Охарактеризуйте організаційні форми початку кримінального провадження щодо кіберзлочинів?
5. Який типовий перелік матеріалів перевірки, що є джерелом обставин про кримінальне правопорушення, вчинене із використанням кіберпростору?
6. Охарактеризуйте процес виявлення кіберзлочинів заявником (як користувачем).
7. Як здійснюється встановлення належності сайту?
8. Якими способами можливо установити факт неправомірного доступу до інформаційної системи або мережі? Які ознаки вказують на несанкціонований доступ?
9. Які види слідів формують слідову картину кіберзлочинів? Чи можна вчинити кіберзлочин, не залишаючи при цьому слідів?
10. Співвіднесіть способи вчинення кіберзлочинів з найбільш поширеними способами їх приховування.
11. У чому полягає відмінність знарядь вчинення кіберзлочинів від предмета їх посягання?
12. Чи належать місце та час вчинення кіберзлочинів до елементів криміналістичної характеристики кіберзлочинів? Чи мають вони значення для розслідування?
13. Які кримінологічні особливості особи кіберзлочинця та потерпілого (жертви) кіберзлочину?
14. Яке значення для розслідування кіберзлочинів відіграють логфайли та метадані?
15. Які можна виокремити способи запобігання кіберзлочинам?

Рекомендована література

1. *Борисова Л. В.* Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

2. Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.

3. *Марущак А. І.* Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104–110.

4. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рекомендації / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

5. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рекомендації / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

6. *Самойленко О. А.* Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

7. *Al-garadi M. A., Varathan K. D., Ravana S. D.* Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in human behavior*. 2016. Vol. 63. P. 433–443.

8. *Al-Khater W. A., Al-Maadeed S., Ahmed A.A., Sadiq A. S., Khan M. K.* Comprehensive Review of Cybercrime Detection Techniques. *IEEE access*. 2020. Vol. 8. P.137293–137311.

9. *Babak Akhgar.* Cyber crime and cyber terrorism investigator's handbook. Waltham, 2014. 282 p.

10. *Calderoni F*. The European legal framework on cybercrime: striving for an effective implementation. URL : https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation

11. *Tropina T., Callanan C*. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing AG Switzerland, 2015.

РОЗДІЛ 3

ЕЛЕКТРОННІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

3.1. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види.
3.2. Способи збирання електронних доказів.

3.1. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види

КЕЙС 1. ***Проаналізуйте наведену ситуацію та встановіть правильність дій слідчого під час проведення огляду?***
Під час огляду ЕОМ слідчим було виявлено дані, які можуть бути використані під час доказування у кримінальному провадженні як докази, зокрема файли із кресленнями щодо виготовлення вибухових речовин. Виявивши вказані дані, слідчий скопіював їх на власний флеш-носій, що відзначив у протоколі огляду.

КЕЙС 2. ***Проаналізуйте наведену ситуацію та дайте відповідь на питання:***

1. ***Які докази необхідно зібрати у кримінальному провадженні з метою всебічного, повного і неупередженого встановлення та дослідження фактів й обставин описаного кримінального правопорушення? Які із них вважатимуться електронними доказами?***
2. ***Якої послідовності дій необхідно дотримуватися для забезпечення правильного збору та збереження опуб-***

лікованих мережі Інтернет даних та недопущення втрати такої інформації у зв'язку з її видаленням?

Громадянин А., перебуваючи за місцем реєстрації та свого фактичного місця проживання, використовуючи послуги доступу до глобальної мережі «Інтернет», з використанням належного йому в одній із соціальних мереж акаунту, створив відкриту соціальну спільноту. У ній він систематично розміщував низку власних дописів та здійснював репости інших авторів, перегляд яких у сукупності було здійснено користувачами спільноти понад 10 000 разів, за результатами яких понад 1 000 користувачів позитивно оцінили розміщену інформацію (скористалися функцією «вподобати» соціальної мережі).

У таких матеріалах містилися прояви зневаги, образи посадових осіб органів державної влади за національною приналежністю, популяризація ідей національної нетерпимості, ворожості, шовінізму, расизму, а також ведення ідеологічної, інформаційної та пропагандистської війни проти представників інших націй, з використанням негативно-оцінних найменувань і характеристик, лайливих, зневажливих лексем та погроз.

Такі дії громадянина А. було кваліфіковано за ч. 1 ст. 161 КК України як таємне розпалювання національної, расової ворожнечі та ненависті, приниження національної честі та гідності, за фактом чого внесено відомості до Єдиного реєстру досудових розслідувань і розпочато досудове розслідування.

137 **Спеціальні ознаки інформації, що створена за допомогою високих інформаційних технологій.** Основним чинником трансформації сучасного суспільства є стрімка інформатизація, яка змінює усі сторони життєдіяльності, впливає на прийняття управлінських рішень і функціонування усталених суспільних інституцій, у тому числі й правових. Змінюючи усі сторони життя людства, динамічний розвиток високих інформаційних технологій торкнувся і сфери кримінального судочинства у контексті появи нових форм представлення інформації та необхідності визначення її місця у системі доказів.

Розпочинаючи аналіз необхідно акцентувати увагу на 138
тому, що інформація, яка створена за допомогою високих інформаційних технологій має унікальні особливості, які відрізняють її від усіх форм представлення інформації, які існували раніше та є звичними для слідчих, зокрема:

- існує у нематеріальному вигляді;
- зберігається на відповідному носії, оперативній пам'яті ЕОМ або каналі зв'язку;
- для її сприйняття та дослідження необхідне використання програмно-технічних засобів;
- має здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик[69];
- має особливий статус оригіналу і може існувати у такому статусі у декількох місцях[70].

До питання про термінологічну визначеність. Будь-яка 139
наука повинна виступати у вигляді чіткої системи понять, у якій усі поняття пов'язані одне з одним і є елементами одного нерозривного ланцюжка. Серед науковців, які досліджують цю проблематику, відсутній єдиний погляд щодо визначення зазначеної форми представлення інформації. Так, вчені у наукових дослідженнях вживають термін «машинна інформація», під якою пропонується розуміти дані, знання, керуючі сигнали та набір команд, що циркулюють в ЕОМ, системі ЕОМ чи мережі, чи зафіксовані на спеціальних пристроях, що

---

[69] *Цехан Д. М.* Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві. *Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства* : матеріали між- нар. наук.-практ. конф. (Одеса, 30 травня 2008 р.). Одеса. 2008. С. 206–209.

[70] *Гонгало С. Й.* Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. … канд. юрид. наук.: спец. 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність Київ, 2013. 20 с.

потенційно можуть бути предметом злочинного посягання чи містити матеріальні сліди його здійснення[71]. Крім цього, вживається термін «комп'ютерна інформація» – інформація, що представлена у спеціальному (машинному) вигляді, призначена та придатна для її автоматизованої обробки, зберігання та передачі, яка знаходиться на матеріальному носії і має власника чи іншого законного володільця, що встановлює порядок її генерації, обробки, передачі або знищення[72]. Термін «комп'ютерна інформація» використовують також інші вчені[73]. Аналізуючи наведені визначення зрозуміло, що автори мають на увазі інформацію, яка створюється, циркулює або знищується за допомогою ЕОМ. Проте, визначаючи цю інформацію, на нашу думку, не доцільно робити акцент на технічному засобі, за допомогою якого вона створюється, циркулює та знищується, тому термін «комп'ютерна інформація» видається не зовсім вдалим.

140 Не зовсім правильним у цьому прикладі використовувати і термін «електронна інформація», оскільки він належить до службових процесів, які відбуваються в електронно-обчислювальних машинах під час їх роботи[74].

141 Проведений аналіз позицій науковців та сутності інформації, що використовується в ЕОМ, глобальних інформаційних мережах та інших автоматизованих системах, вказує на те,

---

[71] *Острушко О. В.* Організаційні аспекти методики розслідування злочинів у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук : спец. 12.00.09. Волгоград, 2000. 15 с.

[72] *Мещеряков В. О.* Основи методики розслідування злочинів в сфері комп'ютерної інформації : автореф. дис. ... д-ра юрид. наук : спец. 12.00.09. Воронеж, 2001. 30 с.

[73] *Азаров Д. С.* Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08. Київ, 2002. 246 с.

[74] *Воронов І. О.* Організаційно-тактичні основи протидії злочинам у сфері високих інформаційних технологій : монографія. Одеса : ОДУВС. 2010. 216 с.

що це передусім багаторівневий об'єкт з достатньо складною структурою та трьома основними рівнями – фізичним, логічним та семантичним.

Фізичний рівень – рівень матеріальних носіїв інформації, де 142
інформація представлена у вигляді конкретних характеристик об'єкта (намагніченість домену – для магнітних дисків, кут та дальність площини відображення лазерного променя – для лазерних дисків).

Логічний рівень – рівень представлення більш складних 143
інформаційних структур (від байта до файлу) на основі компонентів фізичного рівня. Цей рівень охоплює дві групи правил об'єднання – загальні та спеціальні. Загальні правила диктуються фізичними основами пристроїв і технічними особливостями засобів обробки, що використовуються і не можуть бути швидко змінені. Прикладом об'єднання множинності елементарних інформаційних одиниць у більші інформаційні структури може бути кількість та порядок нанесення інформаційних доріжок на магнітному носії, розмір кластера тощо. Спеціальні правила встановлюють, як правило, розробники автоматизованих інформаційних систем і можуть бути досить просто зміненими.

Семантичний рівень – це рівень змістовного представлення 144
інформації, у вигляді, сприятливому для сприйняття людиною.

Проте інформація, що створюється, модифікується або 145
знищується за допомогою ЕОМ, обробляється в ЕОМ, циркулює у глобальних мережах тощо, має спільну особливість, яка і повинна бути покладена в основу її визначення. Враховуючи, що всі ЕОМ, що використовуються суспільством, є цифровими і використовують двозначну систему обчислення, то інформація представляється у вигляді послідовності чи поля цифр, а саме «0» та «1» – елементарних інформаційних одиниць. Оскільки це є обов'язковою, інтегруючою ознакою для специфічної

форми представлення інформації, що досліджується, то, на нашу думку, її доцільно визначати як «цифрову інформацію». Крім цього, варто зазначити, що сформулювати універсальне визначення «цифрової інформації» для юридичної науки досить важко, оскільки воно буде обумовлюватися специфікою відповідної галузі. Аналогічну позицію займають М. Ю. Літвінов та Ю. В. Степанов, які розглядаючи природу комп'ютерної інформації, найбільш суттєвою її ознакою вважають спосіб кодування сигналів. Поряд із цим згадані автори з етимологічного погляду розглядають термін «цифровий», який виник унаслідок обробки електронних сигналів, що складаються з нулів та одиниць[75]. Але в подальшому заперечуючи, по суті, власні судження, використовують термін «комп'ютерна інформація».

146 **Причини наявності труднощів у використанні цифрової інформації у доказуванні.** Необхідно звернути увагу на те, що відсутність єдиного усталеного терміна не є ключовою проблемою у цій сфері, хоча і має безперечно вагоме наукове значення. Як відзначає професор В. В. Лисенко, проблематичними сторонами цього напряму є також встановлення такої інформації, її фіксація та вилучення, експертні дослідження і подальше використання під час досудового слідства та розгляду кримінальної справи в суді. Причинами цього є як об'єктивні фактори (складність отримання такої інформації, потреба використання допомоги спеціалістів у сфері інформаційних технологій, відсутність у розпорядженні правоохоронних органів спеціальної техніки), так і суб'єктивні (відсутність спеціальної підготовки та власного досвіду правоохоронних органів з питань інформаційних технологій, систем

[75] *Литвинов М. Ю.* Понятие компьютерных средств и определение направлений их использования в ОРД. *Вісник ЛДУВС*. 2008. Спец. вип. 4, ч. 1. С. 114–127.

передавання інформації тощо)[76]. Означена позиція може бути підтримана частково, оскільки проблематика виявлення та фіксації цифрової інформації знайшла своє вирішення на рівні наукових досліджень та методичних рекомендацій. Ключовою перешкодою, що на сьогодні унеможливлює її використання у якості доказу, є відсутність експертних методик її ідентифікації та аутентифікація. Так, створивши відповідний цифровий об'єкт та в подальшому скопіювавши його на інший носій, на базі наявних методик дослідження неможливо визначити, який із цих об'єктів виступає початковим (оригіналом), оскільки в інформаційному аспекті фіксація такої інформації, як правило, не пов'язана з її перекодуванням, не відбувається і її відділення від початкового носія, оскільки існує можливість створення точної копії.

На початковому етапі розвитку комп'ютерної техніки 147
проблема використання у доказуванні цифрової інформації виникла у США, де існували правила використання «нетрадиційних доказів» (novel evidence). З урахуванням особливостей англосаксонської системи права, джерелом таких правил став судовий прецедент у справі Фрай проти США (*Frye vs United States*), який стосувався використання у доказуванні нових даних та методик науки і складався із двох елементів: по-перше, суду необхідно визначити, до якої галузі наукового знання належать дані та методики, які покладені в основу доказу, а по-друге, чи визнають провідні вчені-фахівці цієї галузі принцип, на основі якого сформований доказ.

---

[76] *Лисенко В. В., Лисенко О. В.* Проблеми використання у кримінальному судочинстві інформації, що містить у електронному вигляді. *Напрями удосконалення протидії правопорушенням у сфері господарської діяльності* : зб. наук. праць за матеріалами міжнар. наук.-практ. конф., (Київ, 26–27 лист. 2010 р.). Київ, 2010. С. 243–249.

148 У вітчизняній теорії кримінального процесу докази класифікуються за різними підставами. Розподіл доказів на види – це одна з класифікаційних систем, відповідно до якої вони розподіляються, керуючись специфічними та найбільш суттєвими особливостями їх форми та змісту. При цьому окремі види доказів утворюються у випадку, коли їх форма та зміст володіють специфічними характеристиками, що визначають спеціальний режим їх отримання чи використання у кримінальному процесі. Традиційно вчені пропонують поділяти докази за механізмом формування на особисті та речові. Ю. М. Грошевой та С. С. Стахівський зазначають, що за змістом формування докази доцільно поділити на дві групи та відносити до другої докази, що містяться в предметах і документах[77].

149 У зв'язку з цим, практика діяльності правоохоронних органів склалася так, що слідчий, виявивши на жорсткому диску чи в оперативній пам'яті ЕОМ цифрову інформацію, що може містити сліди злочинної діяльності чи в інший спосіб сприяти вирішенню завдань кримінального судочинства, повинен відносити її до речових доказів у випадку, передбаченому ст. 98 КПК України чи документів відповідно до ст. 99 КПК України.

150 Але це створює логічні суперечності та неузгодженості, оскільки речові докази – це, відповідно до ст. 98 КПК України, матеріальні об'єкти. Крізь призму матеріальності об'єкта законодавець у ст. 99 КПК України визначив такий вид доказів, як документи, деталізувавши, що до документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі й електронні). Вирішення означеної проблеми на теоретичному рівні можливе за допомогою методу аналогії та звернення до історичного досвіду. Так, у римському праві власності існувала конструкція щодо поділу

[77] *Грошевий Ю. М., Стахівський С. М.* Докази і доказування у кримінальному процесі: наук.-практ. посібник. Київ : КНТ, 2006. 272 с.

речей на «тілесні» та «безтілесні», яка існувала поряд з іншими класифікаціями матеріальних об'єктів.

Дехто з фахівців у галузі цивілістики – В. О. Копилов, 151
О. О. Ситніков, Ю. Фогельсон – стверджують про можливість існування інформаційної речі, яка є складною за своєю сутністю. Специфічні властивості інформаційної речі виникають з огляду на те, що інформація передається та розповсюджується тільки на відповідному матеріальному носії і виступає як єдність інформації та носія, на якому ця інформація зафіксована.

Видається саме з такими підходами пов'язано введення у 152
науковий обіг поняття «електронного речового доказу», яке вчені використовують без належного обґрунтування. Так, під «електронним речовим доказом» розуміють технічний пристрій, що завдяки своїм індивідуальним чи системним (тим, які проявляються тільки при одночасному використанні з іншими об'єктами) властивостям слугував знаряддям злочину або зберіг на собі сліди злочину, а також може слугувати засобом для виявлення злочину чи встановлення істини у кримінальній справі. Впровадження означеного терміна обґрунтовується наявністю особливостей, що відрізняють його від традиційних речових доказів, – «віртуальна природа закріплення інформації на них».

Означена позиція має вагоме наукове значення, але як 153
проміжна наукова теорія, що потребує подальшої розробки та обґрунтування. На нашу думку, ключовою ідеєю розвитку означених положень є необхідність обґрунтування можливості використання цифрової інформації у кримінальному судочинстві без взаємозв'язку з відповідними носіями.

Видається, що під час оцінки доказу, наданого у вигляді 154
протоколу слідчої дії чи оперативно-розшукового заходу, суд оцінює інформацію, що міститься в ньому, а не папір, що був використаний для написання протоколу.

155 У дослідженні цифрової інформації та її оцінці судом носій не має першочергового значення, оскільки сутність інформації залишається константною незалежно від типу матеріального носія. Схожа позиція простежується і в роботах інших учених, які зазначають, що хоча вилучається і відповідно фіксується носій, доказом у справі буде саме інформація, що міститься на ньому. На жаль, у подальшому, вступаючи у логічні суперечності зі своїми судженнями, вчені визначають комп'ютерну інформацію як речовий доказ.

156 Окрім цього, необхідно відзначити, що на сучасному етапі у значній кількості оперативно-тактичних ситуацій, які виникають під час документування окремих видів злочинної діяльності, зокрема розповсюдження порнографічної продукції в мережі Інтернет, працівники оперативних підрозділів не вилучають носії інформації, а фіксують відповідні дані на власних носіях. Під час виявлення інформації, яка становить оперативний інтерес, необхідно обрати один із перелічених способів:

- збереження сторінки штатними засобами браузера;
- використання функції копіювання даних;
- конвертувати дані в PDF-формат;
- фіксувати дані на екрані програмними засобами.

157 Усі наведені способи не передбачають вилучання носія, а власне фіксацію цифрової інформації на носій, який належить оперативному підрозділу.

158 Саме тому цифровий об'єкт, який є нематеріальним, не має відповідних якісних фізичних характеристик, має специфічну процедуру та середовище створення, здатний до копіювання та переміщення без втрати характеристик, сприймається людиною лише після обробки ЕОМ та виведення інформації на відповідний технічний пристрій (монітор), неможливо визнати матеріальним об'єктом і, як наслідок, речовим доказом

чи традиційним документом. У цьому випадку необхідно оцінювати власне інформацію, а не матеріальний об'єкт, на якому вона зафіксована.

Поняття цифрового доказу. Як зазначає М. А. Іванов, 159
оскільки на початковому етапі йшлося в основному про інформацію, що створена за допомогою апаратних та програмних засобів комп'ютерної техніки, то вона при використанні у кримінальному судочинстві у якості доказу отримала назву «комп'ютерного доказу».

Так, І. В. Єна, оперує терміном комп'ютерні електронні докази, 160
під яким розуміє фактичні дані, що оброблені комп'ютером, зберігаються в електронному вигляді на всіх типах носіїв, і знаходяться у формі, доступній для ЕОМ або людини, на основі яких орган дізнання, слідчий, суд встановлює наявність чи відсутність суспільно небезпечного діяння, винність особи, яка вчинила злочин, а також інші обставини, що мають значення для правильного вирішення справи.

Проте широкомасштабне впровадження високих 161
інформаційних технологій призвело до розроблення та використання у практичній діяльності апаратних засобів, які відповідно до своїх характеристик не могли бути класифіковані та віднесені до такої товарної групи, як комп'ютери. До них можна віднести цифрові записні книжки, засоби мобільного зв'язку, касові та ігрові апарати, в яких інформація обробляється та зберігається у цифровій формі. Означене обумовило використання більш широкого терміна «цифрові докази».

У наукових джерелах зарубіжних країн широкого 162
застосування набув термін «*digital evidence*» (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютера і підтримують або спростовують намір чи алібі. Цифрові дані виявляються дуже

корисними при розслідуванні злочинів, оскільки є текстовою, графічною, звуковою та відеоінформацію[78].

163 Експертами *Scientific Working Group on Digital Evidence* було запропоновано під терміном «цифрові докази» розуміти будь-яку інформацію доказового значення, яка зафіксована чи передана у цифровій формі[79].

164 Саме тому сьогодні можна говорити про існування «цифрових доказів», під якими розуміються фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому, обов'язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення.

165 Необхідність підвищеної уваги до цифрових доказів зумовлюється тим, що, у слідчій та судовій практиці останніх років, обґрунтовуючи своє алібі, учасники кримінального провадження все частіше посилаються на те, що під час вчинення злочину вони взаємодіяли з електронними системами (працювали з персональним комп'ютером, користувались мобільним телефоном, потрапляли у поле зору камер спостереження, авторизувались у системах контролю доступу до приміщень), які знаходяться в іншому місці[80]. У зарубіжній практиці, як відзначає М. А. Іванов, такі пояснення отримали назву «цифрового алібі» (*digital alibi*), оскільки основою для

---

[78] *Casey E.* Digital evidence and computer crime: fo- rensic scene, computer, and the Internet. – 2nd ed. Amsterdam: Elsevier Academic Press, 2004. 690 p.

[79] Scientific Working Group on Digital Evidence. URL : http // www. swgde. org /. Title from the screen.

[80] *Давидюк П. П., Кубай І. Ю.* Висунення і перевірка слідчих версій про цифрове алібі підозрюваного (обвинуваченого). *Молодий вчений.* № 5.1 (45.1). 2017. С. 29. URL : http://molodyvcheny.in.ua/files/journal/2017/5.1/7.pdf.

їх підтвердження чи спростування є цифрова інформація, яка записана на матеріальних носіях[81]. При цьому дослідники звертають увагу на особливості перевірки такого алібі з урахуванням того, що, *по-перше*, доказова інформація, яка підтверджує чи спростовує «цифрове алібі», недоступна для безпосереднього сприйняття, і для її вивчення необхідно використовувати програмно-технічні засоби; *по-друге*, така доказова інформація є вкрай нестійкою, оскільки може бути легко знищена (у тому числі й некваліфікованими діями слідчого).

166 **Процедура фіксації цифрової інформації та забезпечення її доказового значення.** У кримінальному процесі доказ повинен відповідати двом вимогам, які висуваються до його змісту та форми, – відносності і допустимості. Закономірно, що такими ознаками повинен володіти і «цифровий доказ», що може забезпечуватися коректністю фіксації та подальшою незмінністю цифрової інформації. У зв'язку з цим, ґрунтовнішої уваги заслуговує процедура фіксації цифрової інформації та забезпечення її доказового значення. Сьогодні, під час виявлення цифрової інформації у слідчих виникають значні труднощі щодо її фіксації з урахуванням вимог, що висуває кримінальне процесуальне законодавство до доказів та подальшого використання у кримінальному судочинстві.

167 Можливість оперативно змінювати зміст сайту, фізичне розташування серверів на території інших держав, використання анонімних програмних пакетів є факторами, які суттєво ускладнюють можливість фіксації цифрової інформації. Особливої гостроти ця проблема набуває у зв'язку з тим, що встановлення факту такого порушення є чи не найвагомішою

[81] *Давидюк П.П., Кубай І.Ю.* Висунення і перевірка слідчих версій про цифрове алібі підозрюваного (обвинуваченого). *Молодий вчений.* № 5.1 (45.1). 2017. С. 29. URL : http://molodyvcheny.in.ua/files/journal/2017/5.1/7.pdf.

складовою процесу доказування у відповідних провадженнях. Серед прийомів для закріплення відомостей, розміщених у мережі Інтернет, з тим, аби їх можна було використати як докази, можна отримувати від провайдера копії файлів, що формують вебсайт. Відповідні носії таких файлів можливо долучити до матеріалів кримінального провадження як докази.

168 Проте у тому випадку складно забезпечити цілісність збереження цифрової інформації, що створює підґрунтя для її спростування як доказу. Ключовим чинником у цьому випадку є коректна фіксація інформації, яка може здійснюватися автоматично за допомогою спеціального програмного забезпечення та за участю відповідного суб'єкта (експерта, спеціаліста). Сьогодні можна говорити про низький рівень підготовки слідчих до роботи із програмно-технічними комплексами та складними програмними оболонками. У зв'язку з цим, залучення спеціаліста під час роботи з «цифровими доказами» є обов'язковим, оскільки найменша некваліфікована дія може призвести до втрати важливої доказової чи орієнтуючої інформації.

169 У кожній ситуації необхідним є висунення відповідних вимог до коректності фіксації інформації. Так, будь-яке програмне забезпечення може містити помилки, які можна розділити на систематичні та спорадичні, тобто епізодичні та нерегулярні. Аналіз роботи окремих видів програмного забезпечення свідчить, що ймовірність помилки у програмному забезпеченні залежить від її виробника. Саме тому необхідним є використання програмного забезпечення, яке сертифіковане, хоча це також не виключає можливість помилки. Проте ймовірна можливість помилки програмного забезпечення не може апріорно слугувати фактором, що спростовує зафіксовану за його допомогою цифрову інформацію.

170 Виявлена помилка повинна відповідати трьом ключовим умовам:

– підтверджуватися службою технічної підтримки виробника програмного забезпечення, його уповноваженого представника або компетентної організації, яка займається вивченням та узагальненням помилок і недоліків програмного забезпечення;
– помилка повинна мати безпосереднє відношення до фіксації інформації і тому могла призвести до її модифікації, що підтверджується висновком експерта;
– модифікувала під час фіксації саме ту інформацію, що має значення для доказування, що підтверджується висновком експерта.

Дещо інші вимоги до коректності фіксації інформації 171
необхідно визначити у випадку покрокової фіксації необхідної інформації слідчим, у тому числі з використання відповідних програмних продуктів. Для закріплення у якості доказів цифрової інформації, яка отримана внаслідок проведення слідчих дій чи негласних слідчих (розшукових) дій, потрібне виконання, принаймні, трьох умов. *По-перше,* необхідно здійснити оформлення усіх необхідних документів, що підтверджують правові підстави, окреслюють коло суб'єктів та умови фіксації даних відповідно до чинного законодавства України. *По-друге*, при фіксації необхідно уникнути можливих фізичних дефектів відповідного носія та забезпечити максимально високу якість фіксації з метою можливості подальшого експертного дослідження такої інформації. *По-третє*, у разі відсутності у слідчого необхідних спеціальних технічних знань та навичок роботи з апаратними засобами та програмним забезпеченням, повинні залучатися спеціалісти, здатні кваліфіковано поводитися з ними, і згодом підтвердити технічну можливість та факт отримання таких відомостей у судовому засіданні.

Особливості застосування копії інформації у 172
доказуванні. У практичній діяльності працівників оперативних

підрозділів та слідчих можуть виникати тактичні ситуації, коли з технічних причин неможливо представити суду носій, на якому було зафіксовано цифрову інформацію, що отримана внаслідок проведення оперативно-розшукових заходів, слідчих (розшукових) чи негласних слідчих (розшукових) дій. У такому випадку можна формувати докази копіюванням інформації на цьому носії із застосуванням відповідних технічних засобів. Копія означеного носія із супровідним документом, що містить відомості не лише про те, під час проведення якого оперативно-розшукового заходу чи слідчої дії був отриманий оригінал вказаного носія, але і про дату, місце, час копіювання, характеристики технічних засобів і носіїв, що використовувалися при цьому, повинні бути надані суду.

173 У цьому випадку гостро постає проблема збереження цілісності інформації. Існує декілька моделей апаратних та програмних копіювальників носіїв цифрової інформації. До найбільш поширених програмних засобів можна віднести: «*EnCase*», «*FTK*», «*SMART*», «*dd*», «*NED*». При цьому під копіюванням мається на увазі побітова копія, «сектор в сектор», «*bitstream image*». Аналогічні методики набули значного поширення закордоном. Так, у поліції Німеччини поширеним є метод *Perkeo*, важливою особливістю якого є надійне забезпечення цілісності інформації в ході документування злочинної діяльності та можливість її використання у кримінальному судочинстві, оскільки забезпечується копіювання інформації біт за бітом та завдяки цьому її модифікація неможлива.

174 У випадку, коли копіювання файлів проводиться за схемою «сектор в сектор», досить важливо, щоб цільовий носій, на який копіюється інформація, був попередньо очищений. Тобто усі його сектори без винятку повинні бути перезаписані нулями або випадковими бітами. В іншому випадку, під час дослідження такого носія, фахівець, досліджуючи копію одного диска, знайде

там залишки попередньої копії. При цьому факт очищення усіх секторів цільового носія доцільно фіксувати у протоколі. Окрім цього, під час копіювання корисно вираховувати хеш-функції або контрольні суми секторів, що копіюються, і заносити їх до протоколу.

Способи забезпечення допустимості цифрових доказів. 175
Звертаючи увагу на способи забезпечення допустимості «цифрових доказів», як позитивний досвід можливо використати досвід США, де суд визначив, що для визнання доказу допустимим, він має відповідати двом критеріям: засновуватися на науковому знанні (*scientific knowledge*) та сприяти розумінню чи встановленню достовірності фактів суддею чи присяжними.

Дещо інші вимоги існують щодо визначення допустимості 176
анімації та ілюстративних доказів (комп'ютерних моделей подій), які активно використовуються у кримінальних процесах зарубіжних країн. У цьому випадку суд зобов'язаний встановити: правильність параметрів, введених у програму людиною; належність програми, якою оброблялись дані, тобто, чи можна стверджувати, що створена цифрова реконструкція є точною.

В окремих слідчих ситуаціях, а саме, коли об'єкти сфери 177
високих інформаційних технологій використовувались як засоби зв'язку злочинців, для розповсюдження порнографічних предметів, розміщення інформації про продажів заборонених товарів тощо, виникає необхідність надання статусу доказів інформації, яка розміщення в мережі Інтернет. На сьогодні, на фрагментарному рівні практикою вироблені окремі методи фіксації змісту web-сайту з метою подальшого використання у кримінальному судочинстві:

- роздруківка веб-сторінки через браузер;
- роздруківка та подання рапорту працівником поліції;
- огляд вебсайту слідчим у присутності понятих;

– аналогічний огляд разом зі спеціалістом;
– відповідь провайдера на запит щодо змісту сайту.

178 З метою забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. При цьому увага експерта має зосереджуватися на виявленні ознак модифікації цифрової інформації, її способів та меж.

179 Прогресивними у контексті використання «цифрових доказів» у кримінальному провадженні є положення ст. 360 КПК України, якою суду дозволено скористатися під час дослідження доказів усними консультаціями чи письмовими роз'ясненнями спеціаліста, наданими на підставі його спеціальних знань, оскільки під час дослідження судом «цифрових доказів» існує необхідність пояснення особливостей алгоритму програмування чи обробки даних, а також специфіки комп'ютерної системи.

Відповіді на запитання кейсів

КЕЙС 1. *За обставинами справи, слідчий допустив такі помилки: а) оглянув ЕОМ без участі понятих; б) скопіював інформацію на власний носій, який не підготовлений до цього; в) не вилучив матеріальний носій, де зберігалася цифрова інформація, яка могла б бути використана у доказуванні.*

КЕЙС 2. *З метою всебічного, повного і неупередженого встановлення та дослідження фактів й обставин описаного кримінального правопорушення необхідно допитати підозрюваного, за наявності інших свідків; вилучити речові докази – комп'ютерне устаткування; зафіксувати веб-сторінки з незаконною діяльністю автора у соціальних мережах, які й виступатимуть електронними доказами.*

Для забезпечення правильного збору та збереження опублікованих у мережі Інтернет даних та недопущення втрати такої інформації у зв'язку з її видаленням:

1. *Має бути здійснене повне збереження вебсторінки за допомогою будь-якого браузера (Google chrome, Firefox, Opera та інші).*
2. *Утворюється файл з назвою збереженої сторінки із розширенням «HTML» і папка, в якій містяться автоматично створені файли цієї сторінки.*
3. *За допомогою інтернет-ресурсів, які призначені для архівації файлів (наприклад, «archive.today», «Wayback Machine» та інші), здійснюється архівація потрібної сторінки.*
4. *Уся послідовність дій під час проведення слідчої дії огляду інформації, розміщеної в Інтернеті, підлягає чіткому відображенню у протоколі огляду з графічним копіюванням вебсторінок та збереженням цифрової інформації на диску.*

Важливо наголосити, що цифрова копія такого документа, що буде прирівнюватися до оригіналу, має зберігатися у тому вигляді, в якому вона створювалася. Це означає збереження оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний.

3.2. Способи збирання електронних доказів

КЕЙС 1. ***Проаналізуйте наведену нижче ситуацію та визначте, які необхідно провести процесуальні дії для розслідування цього злочину?***

На початку травня 2021 року, Петренко О. А., діючи з корисливих мотивів, будучи обізнаним про важке матеріальне становище Котіної П. О. з використанням обману і, використовуючи її уразливий стан, запропонував їй через спілкування в соцмережі Instagram виїхати у м. Ерджан Турецької Республіки Північний Кіпр для роботи танцівницею в нічному клубі у вищезазначеному місті, при цьому не вказавши, що їй доведеться надавати сексуальні послуги незнайомим особам. Отримавши від

останньої згоду, Петренко О. А. виконав відведену йому функцію, визначивши час, місце і спосіб виїзду Котіної у м. Ерджан Турецької Республіки Північний Кіпр.
Прибувши до міжнародного аеропорту м. Ерджан Турецької Республіки Північний Кіпр, Котіну зустрів чоловік на ім'я Махмуд, який доставив її до нічного клубу «Шерідан», розташований у м. Ерджан Турецької Республіки Північний Кіпр, де надалі їй довелося надавати сексуальні послуги.
06 червня 2021 року за заявою потерпілої Котіної було розпочато розслідування за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 149 КК України.
Під час допиту потерпіла повідомила, що у неї є номер телефону чоловіка на ім'я Іван (050-721-66-92), а також його електронна адреса – ivan@mail.ru.

КЕЙС 2. ***Проаналізуйте наведену нижче ситуацію та дайте відповідь на запитання:***

1. ***Які судові експертизи підлягатимуть призначенню та проведенню, предметом яких виступатимуть електронні докази, в описаній ситуації?***
2. ***Судовим експертам яких установ такі експертизи можуть бути доручені?***
3. ***Які орієнтовні питання варто поставити експертам для з'ясування фактів та обставин, що мають істотне значення для цього кримінального провадження?***

У ході проведення досудового розслідування у кримінальному провадженні, відомості про яке внесені до Єдиного реєстру досудових розслідувань за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 203-2 КК України (незаконна діяльність з організації або проведення азартних ігор) встановлено, що в одному із приміщень міста, яке належало підозрюваному на праві приватної власності, під прикриттям офіційної діяльності пунктів з розповсюдження державних лотерей, було облаштовано незаконний гральний заклад, в якому, використовуючи комп'ютерну техніку та доступ до мережі Інтернет, клієнтам надавався доступ до азартних ігор.

З метою фіксації виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знарядь кримінального правопорушення та майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб, слідчим на підставі ухвали слідчого судді було проведено обшук приміщення грального закладу під назвою «Твоя Лотерея», в ході якого, серед іншого, було виявлено та вилучено наступне: монітори, системні блоки, клавіатури, комп'ютерні миші, роутери, мобільні телефони та грошові кошти.

Прийняття нового КПК України запровадило шлях до інформатизації кримінального провадження через запровадження складних технічних НСРД спрямованих на отримання значного обсягу електронної інформації. 180

Поява електронної форми фіксації, передачі і використання інформації викликає потребу в розробці нових методів виявлення, фіксації та оцінки доказів під час розслідування кримінальних правопорушень, особливо тих, які вчиняються із використанням засобів комп'ютерної техніки. 181

У більшості випадків розслідування кіберзлочинів відбувається із використанням можливостей оперативно-розшукових заходів та негласних слідчих (розшукових) дій. Не зупиняючись на окремих аспектах оперативно-розшукової протидії кіберзлочинам, розглянемо можливості слідчих (розшукових) дій під час розкриття кіберзлочинів. 182

Практика ВС щодо використання електронного документа як доказу. Варто погодитися з думкою, що під цифровими технологіями в кримінальному процесі можна вважати законодавчо урегульовану єдину систему засобів та прийомів збирання, фіксації, обробки, зберігання та поширення інформації[82] про кримінальне правопорушення з метою 183

[82] *Берназюк О. О.* Цифрові технології у праві: тенденції та перспективи розвитку : дис. ... д-ра юрид. наук: 12.00.07. Ужгород, 2021. С. 422.

одержання доказів у кримінальному провадженні. На підставі цих доказів слідчий, дізнавач, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

184 Відповідно до результатів проведеного Верховним Судом дослідження практики судів першої, апеляційної та касаційної інстанцій щодо справ, які перебували на розгляді у 2018 та 2019 роках, встановлено поширеність подання сторонами електронних доказів у кримінальних провадженнях, що зумовлено особливостями окремих видів злочинів, спосіб вчинення яких безпосередньо передбачає використання тих приладів та пристроїв, які оперують інформацією в електронному (цифровому) вигляді.

185 Унаслідок цього фактичні дані, на підставі яких суд встановлює наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню, існують саме в електронній (цифровій) формі.

186 ВС зазначив, що відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг», у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа.

187 Матеріальний носій – лише спосіб збереження інформації, який має значення, тільки коли електронний документ виступає доказом. Головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення.

ВС підкреслив, що долучений в якості речового доказу 188
DVD-R-диск з відеозаписом обставин події був виготовлений у зв'язку із необхідністю надання інформації, яка має значення у кримінальному провадженні, та є самостійним джерелом доказу, похідним від інформації, що зберігається на комп'ютері в електронному вигляді у вигляді файлів.

Отже, записаний на оптичний диск – носій інформації, 189
електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа[83].

Вказаний підхід був уточнений об'єднаною палатою 190
Верховного Суду, яка зазначила, що ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія.

Для виконання завдань кримінального провадження, 191
з огляду на положення Закону України «Про електронні документи та електронний документообіг», допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону, у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той же електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за

[83] Постанова Верховного Суду від 10.09.2020 року у справі № 751/6069/19. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/91722819

допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами – *CRC*-сума, *hash*-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень[84].

192 На розгляді Верховної Ради України до цього часу перебуває законопроєкт, яким пропонується внести відповідні зміни до КПК України, що стосуються:

1) визначення поняття та видів електронних доказів, доповнивши перелік процесуальних джерел доказів, та розмежувавши поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі;
2) регламентації порядку спеціальної конфіскації віртуальних активів[85].

193 Водночас 1 січня 2022 року в Україні набув чинності Закон України «Про електронні комунікації»[86], який замінив собою раніше діючий Закон України «Про телекомунікації»[87]. Новим законом було визначено правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь

---

[84] Постанова Верховного Суду від 29.03.2021 р. у справі № 554/5090/16-к. URL : https://ips.ligazakon.net/document/C017482?an=178

[85] Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : Проєкт Закону України № 4004 від 01.09.2020. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69771&pf35401=533919

[86] Про електронні комунікації : Закон України № 1089-IX від 16 грудня 2020 року [із змінами і доповненнями]. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text

[87] Про телекомунікації : Закон України № 1280-IV від 18 листопада 2003 [із змінами і доповненнями на 23.02.2014]. *Офіційний вісник України*. 2003. № 51. Ст. 2644.

у відповідній діяльності або користуються електронними комунікаційними послугами. Попри те, положеннями зазначеного закону передбачено розмежування даних про рух інформації та безпосередньо інформації, що передається за допомогою електронних комунікацій.

194 У подальшому Законом України № 2137-IX від 15 березня 2022 року «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам»[88] до КПК було внесено хоч і фрагментарні, проте необхідні та загалом позитивні зміни, якими, серед іншого, було запроваджено терміни «комп'ютерні дані», «комп'ютерні системи» у кримінальному провадженні; передбачено нову гласну слідчу (розшукову) дію – зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису; а також змінено найменування та удосконалено правове регулювання процесуального порядку здійснення таких негласних слідчих (розшукових) дій, як зняття інформації з електронних комунікаційних мереж та установлення місцезнаходження радіообладнання (радіоелектронного засобу).

195 Важливо наголосити, що вагомою складовою успішного результату розслідування кіберзлочинів є оперативність та повнота здобутих джерел доказової інформації[89]. Оскільки будь-

[88] Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України № 2137-IX від 15.03.2022. *Офіційний сайт Верховної ради України*. URL : https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 13.08.2023).

[89] *Теплицький Б. Б.* Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин

який контент сайту (до прикладу, сторінка користувача соціальної мережі) підтримується за допомогою електронно-обчислювальних ресурсів, завжди існує ризик втрати криміналістично значущої інформації, зумовлений такими факторами. По-перше, сервер, за допомогою якого підтримується контент сайту, може бути знищений або з нього повністю або частково буде видалена потрібна інформація. По-друге, інформація, що міститься в контенті сайту, може бути частково або повністю змінена, наприклад, особою, яка має доступ до контенту на правах адміністратора. Отже, якщо не здійснити оперативну фіксацію і вилучення потрібних для розслідування даних з віддалених серверів, то до моменту вилучення цифрових даних вони можуть вже бути видалені або змінені. Через це при розслідуванні кіберзлочинів виникає необхідність із залучення спеціаліста, особливо у тих випадках, коли здійснення слідчих (розшукових) дій потребує негайних рішень та існує ризик знищення слідів злочину[90].

196 **Система процесуальних дій, які використовуються під час розкриття кіберзлочинів.** Можна виокремити систему процесуальних дій, які найчастіше використовуються під час розкриття кіберзлочинів, яка складається з гласних і негласних слідчих (розшукових) дій, а також такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей та документів.

197 Зокрема, до гласних слідчих (розшукових) дій, в ході яких можна отримати електронні докази, належать наступні:

- обшук житла чи іншого володіння особи;
- призначення комп'ютерно-технічної експертизи.

(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. С. 182.

[90] *Гребенькова М. С.* Актуальні проблеми електронних відображень у соціальних мережах як джерела доказів у кримінальному провадженні. *Право і суспільство*. 2021. № 6. С. 256.

До негласних слідчих (розшукових) дій, у процесі яких 198
можна отримати електронні докази, варто віднести:

- аудіо-, відеоконтроль особи;
- зняття інформації з електронних комунікаційних мереж;
- зняття інформації з електронних інформаційних систем;
- аудіо-, відеоконтроль місця.

Також електронні докази можуть отримуватися в ході 199
тимчасового доступу до речей та документів, а також добровільно надаватися учасниками кримінального провадження.

Принципи роботи з цифровою інформацією, що є 200
доказом. Міжнародною організацією з цифрових доказів (*International Organisation on Digital Evidence* (IOCE)) визначені такі принципи роботи з цифровою інформацією, що є доказом:

1) при роботі з доказовою інформацією, що міститься на цифровому носії, повинні дотримуватися процесуальні і криміналістичні вимоги;
2) при операціях з доказовою інформацією на цифрових носіях неприпустимо внесення змін до цієї інформації;
3) всі операції з виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях повинні бути зафіксовані в документальній формі, захищені від несанкціонованої зміни і придатні для дослідження;
4) особа, яка здійснює операції з доказовою інформацією на цифрових носіях, несе відповідальність за її збереження, поки має доступ до цієї інформації;
5) будь-яка організація, що здійснює виявлення, вилучення, зберігання і переміщення доказової інформації на цифрових носіях, повинна дотримуватися вказаних принципів[91].

[91] Digital Evidence: Standards and Principles. *Forensic Sciennce Communications*. 2000. Vol. 2. № 2. URL : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.

201 **Особливості слідчих (розшукових) та інших процесуальних дій, проведення яких спрямоване на збирання та перевірку електронних доказів**.

202 1. Процесуальна коректність фіксації: зміст і реквізити цифрової інформації підлягають обов'язковому опису в протоколі слідчої дії або експертному висновку. Однак найчастіше виключно документально-текстова фіксація є недостатньою, тому рекомендується вносити в текст процесуального документа або прикладати до нього скріншоти, роздруківки логів, витяги із зовнішньої аналітики та статистики по сайту тощо. У разі копіювання цифрової інформації, також має бути доданий її носій. Окрім того, до участі у слідчому огляді рекомендується залучати понятих, яким потрібно послідовно роз'яснювати сутність усіх дій слідчого та спеціаліста, які мають значення для розслідування.

203 2. Точний опис проведених операцій із виявлення програмного забезпечення (включаючи точну версію), зокрема і використаних для цього технічних засобів. Специфіка подібної вимоги полягає в тому, що на відміну від багатьох інших слідів, цифрова інформація, особливо розміщена в Інтернеті, після вивчення суб'єктом розслідування може залишитися незмінною. Відповідно, комплекс операцій з її виявлення та фіксації повинен становити собою формалізований алгоритм, який при необхідності може бути точно відтворений згодом. Фіксації підлягають не тільки виявлені пристрої, а й навколишнє оточення. Відомості про обстановку дають підстави судити про умови як використання особою, яка вчинила злочин, електронних носіїв інформації, так і умови виявлення та процесуального вилучення цих носіїв.

204 3. Коректність встановлення зв'язку виявленої інформації з подією, що розслідується або особою підозрюваного, у тому числі робота з встановлення або спростування «цифрового

алібі». Якщо для індивідуалізованих комп'ютерних пристроїв (насамперед, особистих смартфонів) зв'язок інформації, що знаходиться на пристрої із власником пристрою може вважатися апріорним, то для стаціонарних пристроїв, особливо які розташовані в місцях, де доступ до них можуть мати різні суб'єкти, потрібне додаткове обґрунтування обумовленості операцій з цифровою інформацією з діями конкретної особи. При цьому дослідники звертають увагу на особливості перевірки такого алібі з урахуванням того, що, по-перше, доказова інформація, яка підтверджує чи спростовує «цифрове алібі», недоступна для безпосереднього сприйняття, і для її вивчення необхідно використовувати програмно-технічні засоби; по-друге, така доказова інформація є вкрай нестійкою, оскільки може бути легко знищена (у тому числі й некваліфікованими діями слідчого)[92].

Розглянемо більш детально процесуальний порядок 205
проведення та особливості кожної із процесуальних дій.

Обшук житла чи іншого володіння особи. В ході обшуку 206
слідчий може вилучати значну кількість носіїв цифрової інформації, яка в подальшому може бути використана як докази у кримінальному провадженні.

Відповідно до ч. 1 ст. 234 КПК України, обшук проводиться 207
з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб.

У клопотанні про обшук, окрім іншого, повинні міститися 208
відомості про індивідуальні або родові ознаки речей, документів,

---

[92] *Цехан Д. М.* Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 257.

іншого майна або осіб, яких планується відшукати, а також їхній зв'язок із вчиненим кримінальним правопорушенням.

209 Базовим завданням цієї слідчої дії є забезпечення безпеки комп'ютерної доказової інформації, а також полегшення її виявлення.

210 Перед обшуком бажано отримати орієнтуючу інформацію щодо комп'ютерної техніки, яка знаходиться на місці обшуку. До таких відомостей можна віднести інформацію про:

- кількість, типи, марку та конфігурацію ЕОМ;
- наявність локальної мережі або підключення комп'ютера до глобальної мережі Internet;
- кваліфікацію користувачів ЕОМ в галузі програмування та обчислювальної техніки;
- факт використання пристрою автономного та безперебійного живлення, і до яких наслідків може призвести вимкнення електроенергії;
- характеристику колективу співробітників, які обслуговують обчислювальну техніку[93].

211 При дослідженні зовнішніх характеристик комп'ютерного пристрою варто звернути увагу й описати в протоколі слідчої дії всі підключені до нього периферійні пристрої вводу-виводу: монітори, клавіатури, комп'ютерні миші та інші маніпулятори, веб-камери, принтери, сканери, копіри, модеми, хаби і т. п. При зовнішньому огляді доцільно шукати можливі відключені накопичувачі інформації. У протоколі повинен також міститися опис усіх підключених кабелів та незайнятих портів. Вкрай бажано сфотографувати розташування та факт підключення кабелів. При вилученні комп'ютерного пристрою, якщо є

[93] *Теплицький Б. Б.* Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. С. 127.

необхідність вимкнення кабелю, необхідно маркувати кожен кабель і відповідний порт, наприклад, за допомогою паперових або пластикових бирок.

Більше того, у протоколі необхідно описати: 212

- найменування, марку та модель комп'ютерного пристрою, місце його виявлення або особу, в якої він був фактично вилучений та за яких обставин;
- ідентифікаційні ознаки, зокрема серійний номер, із зазначенням способу ідентифікації (напис на пристрої, електронна інформація тощо);
- про те, що (у разі вилучення незаблокованого пристрою) на момент вилучення такий пристрій є незаблокований та відобразити здійснені суб'єктом проведення відповідної слідчої (розшукової) дії заходи щодо увімкнення режиму польоту та вимкнення Wi-Fi і Bluetooth;
- перебіг та результати копіювання всього вмісту пристрою, із зазначенням всіх здійснених суб'єктом проведення відповідної слідчої (розшукової) дії заходів, включаючи інформацію, що підлягає копіюванню, програмного забезпечення, за допомогою якого відбувається таке копіювання, відомості про його ліцензування, носій інформації, на який здійснено копіювання наявної на комп'ютерному пристрої інформації, із зазначенням ідентифікаційних номерів носія інформації (серійний чи інвентарний номер тощо)[94].

Вилучені мобільні пристрої (телефони, планшетні 213
комп'ютери, GPS-навігатори, *smart*-годинники, портативні відеореєстратори тощо) упаковуються в окремі непрозорі

[94] Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 43.

пакети, що унеможливлює увімкнення пристрою в упаковці[95].

214 Отже, в протоколі обшуку повинно бути детально зазначено всі можливі ідентифікаційні ознаки об'єктів комп'ютерної техніки. Згідно з правовою позицією Верховного суду, протокол обшуку, в якому відсутні ідентифікаційні ознаки виявлених та вилучених речей (не зазначено марки, моделі, номера, а також характерних ознак), є недопустимим доказом[96].

215 Слідчий, прокурор під час проведення обшуку має проаналізувати обстановку й обрати найбільш прийнятний (процесуально допустимий) спосіб отримання інформації: вилучати електронні носії інформації або копіювати інформацію, що міститься в інформаційній системі. Для прийняття зваженого рішення варто використовувати наступний ***алгоритм*** (див. схему 1)[97].

216 Важливим елементом процесу аналізу обстановки на місці проведення обшуку, огляду є можливість проведення експрес-пошуку інформації як форми огляду документів під час обшуку, огляду, що передбачено ч. 7 ст. 236 КПК України. Важливо зауважити, що експрес-пошук не дозволяє проаналізувати значну частину видалених файлів, а також зашифровані та заблоковані дані, однак така дія надає можливість визначитися з наступними рішеннями при проведенні обшуку, огляду.

---

[95] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 46.

[96] Постанова Верховного суду від 24.09.2020 р. у справі №306/2629/17. URL : https://ips.ligazakon.net/document/c015095?an=2

[97] *Гаркуша А., Каланча І.* Як вилучати електронні носії інформації під час обшуку з користю для слідства і без шкоди для бізнесу. алгоритм прийняття рішень. URL : https://justtalk.com.ua/post/yak-viluchati-elektronni-nosii-informatsii-pid-chas-obshuku-z-koristyu-dlya-slidstva-i-bez-shkodi-dlya-biznesu-algoritm-prijnyattya-rishen

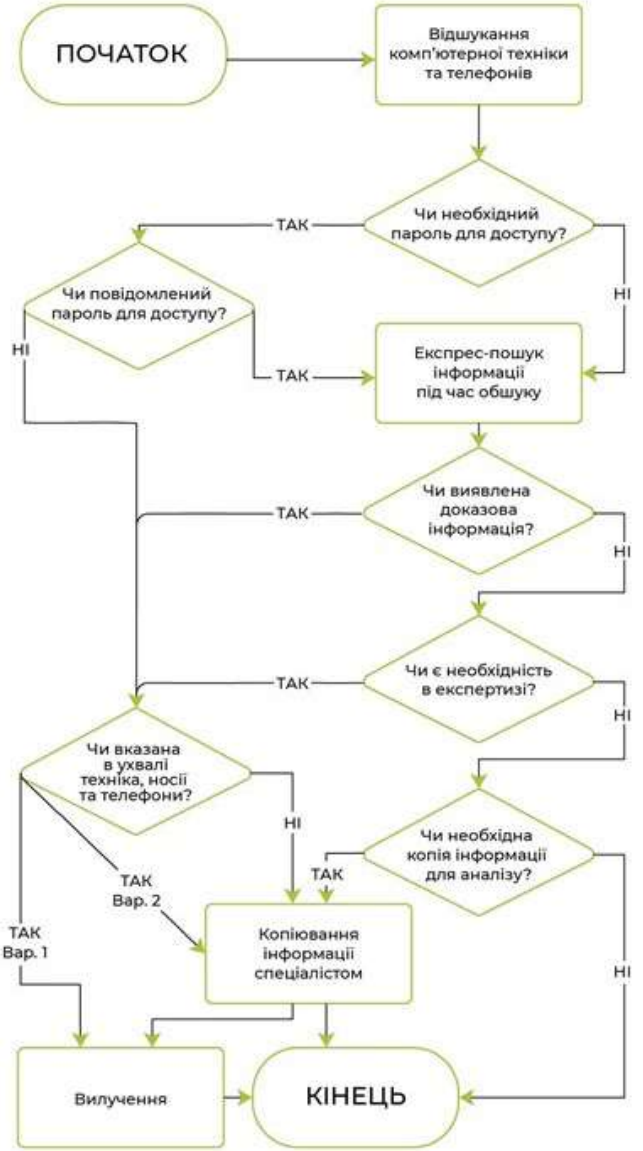
ПОЧАТОК
Відшукання комп'ютерної техніки та телефонів
Чи необхідний пароль для доступу?
ТАК
НІ
Чи повідомлений пароль для доступу?
НІ
ТАК
Експрес-пошук інформації під час обшуку
Чи виявлена доказова інформація?
ТАК
НІ
Чи є необхідність в експертизі?
ТАК
НІ
Чи вказана в ухвалі техніка, носії та телефони?
НІ
ТАК Вар. 2
ТАК Вар. 1
Чи необхідна копія інформації для аналізу?
ТАК
НІ
Копіювання інформації спеціалістом
Вилучення
КІНЕЦЬ

Схема 1

217 Не менш важливою є процедура копіювання електронної інформації, що визначена в абз. 4 ч. 2 ст. 168 КПК України. Це ефективний спосіб отримання доказової інформації, що може бути надалі дієво використаний слідчим та прокурором з огляду на статус такої інформації як оригінала документа (ч. 4 ст. 99 КПК України).

218 *Технічна неможливість копіювання електронної інформації є достатнім обґрунтуванням необхідності подальшого експертного дослідження.* Варто додати, що у випадку, коли з технічних причин неможливо скопіювати електронну інформацію з об'єктів, що не вказані в ухвалі слідчого судді, слідчий, прокурор можуть їх тимчасово вилучити в порядку, визначеному ч. 7 ст. 236 КПК України (як речі, що мають важливе значення для кримінального провадження). При цьому у протоколі мають бути зафіксовані виявлені відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження, а метою вилучення, за таких умов, є забезпечення збереження цілісності інформації на електронному носії, а не вивчення фізичних властивостей, оскільки такі властивості в достатньому обсязі вивчені до ухвалення рішення про вилучення носія (абз. 2 ч. 2 ст. 168 КПК України)[98].

219 **Призначення та проведення комп'ютерно-технічної експертизи.** Комп'ютерно-технічна судова експертиза (далі – КТЕ), становить самостійний вид судових експертиз, що належить до класу інженерно-технічних, її проводять з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення

[98] *Гаркуша А., Каланча І.* Як вилучати електронні носії інформації під час обшуку з користю для слідства і без шкоди для бізнесу. Алгоритм прийняття рішень. URL : https://justtalk.com.ua/post/yak-viluchati-elektronni-nosii-informatsii-pid-chas-obshuku-z-koristyu-dlya-slidstva-i-bez-shkodi-dlya-biznesu-algoritm-prijnyattya-rishen

й вивчення його слідової картини в розслідуваному злочині, а також одержання доступу до інформації на носіях даних з подальшим усебічним її дослідженням. Тільки КТЕ спроможна, забезпечивши отримання органами досудового розслідування унікальної розшукової інформації, створити відповідно до норм КПК України процесуальне джерело доказів – висновок експерта. За таких умов невідкладними й найважливішими завданнями слідчих та оперативних працівників є пошук, фіксація, вилучення й надання експерту в непошкодженому вигляді матеріальних об'єктів – носіїв комп'ютерної інформації, що набувають статусу об'єктів експертного дослідження, і правильне визначення завдань КТЕ[99].

220 Систему об'єктів КТЕ становлять класи (які поділяють на види й підвиди), а саме:

апаратних об'єктів:

- персональні комп'ютери (у будь-яких варіантах виконання);
- периферійні пристрої до персональних комп'ютерів;
- мережеві апаратні засоби (сервери, робочі станції, комутатори, модеми, роутери й інше серверне обладнання);
- інтегровані системи (мобільні телефони тощо);
- будь-які комплектувальні всіх зазначених вище компонентів (апаратні блоки, блоки живлення, плати розширення тощо).

221 Ці види можуть поєднуватися. Безпосередньо в контексті криміналістики найважливіший підвид запам'ятовувальних пристроїв та інших носіїв інформації (електронних даних) – усі відомі на момент призначення експертного дослідження носії інформації (електронних даних): жорсткі диски, флеш-

[99] *Теплицький Б. Б.* Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2. С. 25.

накопичувачі, диски для лазерних систем зчитування, карти пам'яті тощо. До апаратних об'єктів належать: системний блок; жорсткий диск; інші накопичувачі даних – гнучкі диски (5.25» і 3,5»), CD-ROM, магнітооптичні диски; сервер (на платформі Intel-процесорів або сумісних із ними); *RAID*-масиви; принтери (під час виконання комплексної експертизи разом із технічною експертизою документів);

222 *програмних об'єктів:*

- системне програмне забезпечення – комплекс програм, призначених для управління роботою обчислювальної системи, розподілу її ресурсів, підтримання діалогу з користувачами, надання їм допомоги в обслуговуванні комп'ютера, а також для часткової автоматизації розроблення нових програм. Системне програмне забезпечення поділяють на три основні складові: операційні системи, системи програмування, сервісні програми;
- прикладне програмне забезпечення – комплекс програм, призначених для виконання прикладних завдань фахової діяльності людини (виробничі, наукові, навчальні, розважальні тощо);

223 *інформаційних об'єктів (електронних даних):*

- текстові й графічні файли, створені з використанням комп'ютерів або мобільних пристроїв;
- аудіовізуальні (мультимедійні) дані;
- інформація у форматах баз даних та іншого прикладного програмного забезпечення[100].

224 Повноцінна організація проведення КТЕ передбачає наявність спеціалістів з різних операційних систем, прикладного

[100] *Теплицький Б. Б.* Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2. С. 26.

програмного забезпечення, бухгалтерських програм, баз даних, програмування, криптоаналізу, мультимедіа, мережевих та інтернет-технологій, апаратних компонентів комп'ютера та машинних носіїв інформації, зв'язку.

Можна виокремити такі завдання, які вирішуються під час 225
проведення КТЕ:

- визначення робочого стану комп'ютерно-технічних засобів, а також властивостей, якості, статусу та особливостей використання технічних комп'ютерних систем;
- встановлення особливостей розробки і використання програмних продуктів (при встановленні фактів використання програмного забезпечення з порушенням авторських прав його розробника);
- установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;
- виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;
- встановлення вартості програмного забезпечення;
- отримання доступу до інформації на носіях;
- підтвердження або спростування заявлених розробником характеристик, алгоритмів та властивостей програмного забезпечення;
- дослідження інформації, створеної користувачем або програмою для реалізації інформаційних процесів;
- виявлення причин блокування сайтів (віруси, мережеві атаки), а також несанкціонованого втручання в роботу сайту, сервера, комп'ютера, електронної пошти тощо;
- ідентифікаційне дослідження мережевих комунікацій та інтернет-технологій[101].

[101] *Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В.* Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посібник. Львів : Львівський державний університет внутрішніх справ, 2022. С. 36–37.

226 Окрім типових задач, у практиці цього роду експертиз трапляються й нестандартні задачі, що потребують використання спеціальних методичних підходів. До них належать, наприклад, дослідження апаратних засобів за наявності комплексу несправностей або ж дослідження несправностей апаратних засобів, що викликані зовнішнім впливом (механічним та термічним), а також впливом водяного потоку (залив). До цієї ж категорії належать і задачі диференціації електронних інформаційних пристроїв, які відносять (або не відносяться) до класу комп'ютерів. Останнім часом до цієї групи входить і встановлення комп'ютерної імітації (використання комп'ютерних систем для виготовлення грошей, зображень відбитків печаток і штампів тощо), що потребує комплексного підходу при дослідженні[102].

227 **Аудіо-, відеоконтроль особи.** Одним із різновидів втручання у приватне спілкування згідно з ч. 4 ст. 258, ст. 260 КПК є аудіо-, відеоконтроль особи, який є НСРД, що проводиться без відома такої особи на підставі ухвали слідчого судді, якщо є достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування. Зазначену НСРД законодавець розмістив першою серед негласних засобів отримання інформації, у такий спосіб визначивши її важливе значення у досудовому розслідуванні злочинів[103]. Водночас обмеженість правового регулювання та

[102] *Карпінська Н., Крикунов О.* Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1. С. 142.

[103] Окрім того, варто зазначити, що за матеріалами узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії, у провадженні апеляційних судів перебувало 10,9 тис. клопотань про аудіо-, відеоконтроль особи, з яких задоволено 9,9 тис. (Див.: Постанова Пленуму Вищого спеціалізованого суду

невизначеність співвідношення із суміжними негласними діями визначає необхідність у її науковому осмисленні та узагальненні практики проведення.

У п.п. 1.11.2. Інструкції вказано, що ця НСРД полягає у 228
негласній (без відома особи) фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування тощо. На думку Ю. Лисюка метою аудіоконтролю є спостереження за діями та розмовами особи (шляхом прослуховування та фіксації розмов) у будь-якому місці її перебування, незважаючи на те, що це місце є її власністю чи вона там тимчасово перебуває, а відеоконтролю – візуальне негласне спостереження за діями особи (шляхом відеозапису та аудіофіксації) у будь-якому місці її перебування для отримання інформації, що має значення для досудового розслідування[104]. С. Єськов уважає, що метою зазначеної НСРД є фіксація з використанням аудіо-, відеозаписуючих пристроїв поведінки особи, її розмов або інших рухів, дій, пов'язаних із її діяльністю або місцем перебування у публічно недоступних місцях[105]. Погоджуючись із зазначеними вченими, варто додати, що метою усіх НСРД є пошук та фіксація відповідних відомостей, які у перспективі матимуть доказове значення, проте більшість із таких дій мають власну

України з розгляду цивільних і кримінальних справ № 3 від 07 лютого 2014 року «Про узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії». URL : http://zakon3.rada.gov.ua/laws/show/v0003740-14

[104] *Лисюк Ю. В.* Аудіо-, відеоконтроль як різновид втручання у приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Науковий вісник Херсонського державного університету.* 2014. Вип. 6-1. Т. 4. С. 79.

[105] *Єськов С. В.* Аудіо-, відеоконтроль особи як різновид втручання у приватне спілкування : системно-структурний аналіз. URL : www.corp-lguvd.lg.ua/d130203.html

спрямованість, що обумовлює виокремлення їх у відповідний вид (класифікацію).

229 Щодо аудіо-, відеоконтролю особи, то аналіз глави 21 КПК дає змогу припустити, що ще дві НСРД мають аналогічну мету та об'єкти проведення. Йдеться про спостереження за особою, місцем або річчю та аудіо-, відеоконтроль місця. Об'єктом аудіо-, відеоконтролю особи є приватне спілкування особи у публічно недоступних місцях у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, зміст яких має значення для досудового розслідування. Такі ж об'єкти передбачені і щодо названих вище НСРД, відмінність лише щодо публічності (доступність чи недоступність) місця проведення та особливостей організаційно-тактичного та технічного забезпечення. Тому, погоджуємося з В. Уваровим у тому, що усі три НСРД мають однакові об'єкти, предмети і методи дослідження. Вони мають своїм змістом спостереження за особою й окремими місцями її перебування та різняться хіба що рівнем їх технологізації[106]. В. Тертишник зазначає, що такі НСРД, як аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця та спостереження за особою, річчю або місцем часто мають або один метод, або один предмет дослідження та перебувають у стані штучної конкуренції правових норм. На його думку, наведені вище НСРД можуть і мають бути об'єднані в єдину слідчу дію – візуальне спостереження та технічне документування, порядок провадження якої, як наголошує вчений, має бути ретельно прописаним у законі[107].

230 Аудіоконтроль особи полягає у прослуховуванні та фіксації розмов, що відбуваються на відповідних об'єктах. Аудіоконтроль

---

[106] *Уваров В. Г.* Інститут втручання у приватне життя шляхом аудіо-, відео контролю. *Право і безпека.* 2012. № 5 (47). С. 191.

[107] *Тертишник В. М.* Концептуальні проблеми реформи кримінального судочинства *Право і суспільство.* 2013. № 1. С. 139.

особи проводиться за допомогою спеціальних технічних засобів фіксації інформації. Безпосередній порядок проведення такої НСРД визначається відповідними відомчими нормативно-правовими актами. Аудіоконтроль особи може здійснюватися епізодично (наприклад, на певний проміжок часу проведення зустрічі) та неперервно (на весь проміжок часу проведення цієї дії, визначений в ухвалі слідчого судді).

Відеоконтроль особи здійснюється технічними засобами, 231
що забезпечують негласне візуальне спостереження за діями, розмовами, поведінкою підозрюваного, обвинуваченого та осіб, що контактують з ними у зв'язку з їх протиправною діяльністю. Відеоконтроль обстановки та дії осіб, їх фіксація може відбуватися в житлі або іншому володінні особи, а також у приміщеннях, транспортних засобах та інших місцях, які не належать до житла та не є іншим володінням особи. Відеоконтроль особи, як правило, здійснюється спеціальними підрозділами, що забезпечують впровадження та експлуатацію СТЗ. Посадова особа уповноваженого оперативного підрозділу правоохоронного органу, якій було доручено аудіо-, відеоконтроль особи, негайно після завершення цієї НСРД повідомляє про це слідчого та надає йому для дослідження інформацію, отриману при застосуванні технічних засобів. Слідчий, а в разі необхідності спеціаліст відповідно до вимог ст. 266 КПК вивчає зміст отриманої інформації, про що складає протокол.

Процесуальний порядок проведення аудіо-, відеоконтролю 232
особи є загальним, і передбачає постановлення ухвали слідчим суддею на підставі клопотання слідчого (погодженого з прокурором) або прокурора.

За результатами проведення аудіо-, відеоконтролю особи 233
складається протокол, в якому описуються технічні носії інформації, технічні засоби, за допомогою яких була відтворена

наявна в них інформація, результати дослідження наданої інформації. У ньому повністю відтворюється інформація із зазначенням змісту розмови осіб або інших звуків, рухів, дій, пов'язаних з її діяльністю. Протокол про проведення дослідження інформації, отриманої при застосуванні технічних засобів, не пізніше, ніж через двадцять чотири години з моменту припинення аудіо-, відеоконтролю особи передається прокурору (ч. 3 ст. 252 КПК).

234 Проведенню аудіо-, відеоконтролю особи завжди передує обстеження публічно недоступних місць, житла чи іншого володіння особи, в результаті таємного проникнення до яких встановлюються технічні засоби аудіо-, відеоконтролю особи (п. 5 ч. 1 ст. 267 КПК). Тому в разі отримання відомостей слідчим, прокурором, які мають значення для кримінального провадження про розмови конкретної особи або інші звуки, рухи, дії, пов'язані з її діяльністю та перебуванням всередині публічно недоступних місць, житла чи іншого володіння особи, вони звертаються з клопотанням до слідчого судді про дозвіл на проведення обстеження публічно недоступних місць, житла чи іншого володіння особи для встановлення технічних засобів аудіо-, відеоконтролю особи та про дозвіл на проведення аудіо-, відеоконтролю особи всередині цих місць. Як зазначають деякі дослідники, аудіо-, відеоконтроль особи часто проводиться одночасно зі спеціальним слідчим експериментом щодо службової особи під час її зустрічі з особою, що буде надавати неправомірну вигоду, у публічно недоступному місці[108].

235 **Зняття інформації з електронних комунікаційних мереж.** Зняття інформації з електронних комунікаційних мереж полягає в негласному проведенні із застосуванням відповідних

[108] *Шумейко Д. О.* Негласний елемент у системі тактичної операції по документуванню прийняття пропозиції (обіцянки) та одержання неправомірної вигоди. *Наше право*. 2015. № 3. С. 106.

технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду).

Відповідно до ст. 1 ЗУ «Про електронні комунікації», 236
електронна комунікаційна мережа – це комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг. Така мережа – це основна частина інфраструктури будь-якого оператора телекомунікації, чи то оператора традиційної телефонії, стільникового оператора, провайдера безпровідного або провідного доступу до Інтернету[109].

При цьому постачальники електронних комунікаційних 237
мереж та/або послуг зобов'язані вживати відповідних технічних та організаційних заходів для забезпечення безпеки електронних комунікаційних мереж та послуг з метою гарантування цілісності власних електронних комунікаційних мереж, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до електронних комунікаційних мереж (ч. 2 ст. 119 Закону України «Про електронні комунікації»).

Інформація, яка зосереджена в пам'яті комплексно- 238
програмного устаткування постачальників електронних комунікаційних послуг, накопичується і використовується для модернізації, оптимізації, контролю техніко-економічних показників та задоволення інформаційних послуг споживачів, тобто використовується ними для забезпечення технологічних процесів у мережі. Так, згідно з пунктом 2 ч. 8 ст. 105 Закону «Про електронні комунікації», постачальники електронних

[109] Кримінальний процесуальний кодекс України. Науково-практичний коментар / за ред. Гончаренка В. Г., Нора В. Т., Шумила М. Є. Київ : Юстиніан, 2012. С. 580.

комунікаційних послуг повинні зберігати записи про надані електронні комунікаційні послуги протягом строку позовної давності, визначеного законом.

239 З огляду на положення ст. 119 Закону України «Про електронні комунікації», постачальники електронних комунікаційних послуг повинні забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, отриманих при укладенні договору про надання електронних комунікаційних послуг та наданні електронних комунікаційних послуг. Своєю чергою інформація про електронні комунікаційні послуги, отримані кінцевим користувачем, може надаватися за наявності його попередньої згоди, вираженої у письмовій чи будь-якій іншій формі, що дає змогу зробити висновок про факт надання такої згоди або у порядку та відповідно до вимог Конституції України та законів України.

240 Водночас, ст. 121 згаданого вище нормативно-правового акту передбачено певні умови надання доступу до інформації у передбачених законом випадках:

241 *По-перше,* доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, відбувається виключно на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом.

242 *По-друге,* зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством.

243 *По-третє,* постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість

підключення технічних засобів, зазначених вище, в точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг.

Так, за допомогою додаткових програмно-апаратних 244
комплексів, встановлених на платформі оператора, можлива постановка на відстеження зразка голосу конкретної особи із встановленням IMEI-номера терміналу, номера абонента у разі, якщо така особа починає сеанс голосового зв'язку. Відповідно, можливо проводити запис розмов цієї особи незалежно від того, яким терміналом або абонентським номером вона користується[110].

Через комплексно-програмні пристрої постачальників 245
електронних комунікаційних послуг проходить потік інформації, частина якої залишається в пам'яті для технологічних цілей (статична), а інша частина проходить як наскрізна – динамічна інформація, що в інтересах слідства може бути перехоплена лише на підставі ухвали слідчого судді апеляційного суду. До статичної інформації тимчасовий доступ можливий на підставі ухвали слідчого судді місцевого суду після розгляду клопотання прокурора або слідчого[111].

Як випливає з п.п. 1.11.5.1. Інструкції, зняття інформації з 246
електронних комунікаційних мереж поділяється на два види:

– контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на

[110] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 19.

[111] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства*. 2013. № 4. С. 98.

електронних комунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється;

– зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на електронних комунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

247 Тож, об'єктом першого виду зняття інформації з електронних комунікаційних мереж будуть: телефонні лінії загального користування; відомчі мережі, що мають вихід на телефоні лінії загального користування; виділені мережі зв'язку невиробничого призначення; мережі пересувного радіотелефонного зв'язку; системи пересувного супутникового зв'язку.

248 Різновидом електронної комунікаційної мережі в цьому випадку виступає мережа мобільного зв'язку, яка становить собою рознесені в просторі приймачі, що працюють в одному і тому ж частотному діапазоні, і комутуюче обладнання, що дозволяє визначати поточне місце розташування рухомих абонентів і забезпечувати безперервність зв'язку при переміщенні абонента із зони дії одного приймача в зону дії іншого. Мобільні мережі різних операторів з'єднані одна з одною, а також зі стаціонарною телефонною мережею. Це дозволяє абонентам одного оператора робити дзвінки абонентам іншого оператора, з мобільних телефонів на стаціонарні і зі стаціонарних на мобільні. Крім того, оператори мобільного зв'язку активно укладають між собою договори роумінгу,

завдяки яким абонент, перебуваючи поза зоною покриття своєї мережі, може здійснювати і приймати дзвінки через мережу іншого оператора.

Тож, основними складовими мережі виступають базові 249
станції (мобільні вишки) і мобільні телефони (кінцеве обладнання). Базова станція – це комплекс радіопередавачів (ретранслятори, прийомо-передавачі), який здійснює зв'язок з кінцевим абонентським обладнанням – мобільним телефоном. Зона покриття від антен базової станції утворює соту, або групу сот. Базова станція забезпечує централізоване обслуговування групи кінцевих абонентських пристроїв. Мобільні телефони є кінцевим обладнанням, безпосередньо з якого і ведуться переговори[112].

Зняття інформації з електронних комунікаційних мереж 250
цього виду завжди повинно передбачати контроль розмов обидвох абонентів, шляхом використання безпосереднього підключення до телефонного каналу або сканування радіоканалу. Прослуховування телефонної розмови тільки одного з абонентів, в тому числі і з використанням технічних засобів, без підключення до мережі зв'язку не вважається зняттям інформації з електронних комунікаційних мереж, а повинно розглядатись, як інша НСРД пов'язана із втручанням у приватне спілкування (наприклад, аудіо-, відеоконтроль особи).

Об'єктом другого виду зняття інформації з електронних 251
комунікаційних мереж будуть: телексні, факсимільні, селекторні, радіорелейні, пейджингові канали обміну інформації між абонентами, комп'ютерні мережі різного рівня.

Фіксація повідомлень, переданих у комп'ютерних мережах, 252
має певні особливості. Загальним правилом є те, що інтернет-

---

[112] *Багрій М. В., Луцик В. В.* Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід: монографія. Харків : Право, 2017. С. 142.

провайдер, укладаючи договір з користувачем про підключення до глобальної мережі Інтернет, з'ясовує і фіксує в договорі анкетні дані і точну адресу користувача. Це дає можливість «прив'язати» MAC-адресу та IP-адресу комп'ютера до конкретної особи. Однак при реєстрації в чатах, на форумах, у блогах, соціальних мережах користувач може не вказувати свої анкетні дані, а використовувати нікнейм, який становить собою умовне ім'я, яке не містить ніяких реальних відомостей про певну фізичну особу.

253 Всі повідомлення користувача надходять на центральний пристрій – сервер, потім за допомогою інших пристроїв (комутатора, маршрутизатора) направляються абонентам. При цьому відомості про відправника фіксуються і зберігаються на сервері провайдера.

254 Таким способом, повідомлення в комп'ютерних мережах можна відстежити за:

а) MAC-адресою, тобто ідентифікаційною адресою комп'ютерного обладнання;
б) IP-адресою, присвоєною комп'ютеру у відповідній комп'ютерній мережі;
в) адресою електронної поштової скриньки;
г) ідентифікаційному номеру UIN, наявного у користувачів ICQ;
д) даними, що містяться в обліковому записі відвідувачів чатів, форумів, блогів, соціальних мереж.

255 В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування.

До таких ідентифікаційних ознак можна віднести: 256

- електронний код (ідентифікатор) кінцевого обладнання – код, який присвоюється виробником технічних засобів телекомунікацій для унікальної ідентифікації кінцевого обладнання (міжнародні серійні коди IMEI, ESN, MEID тощо)[113];
- ідентифікаційна телекомунікаційна картка (далі – ідентифікаційна картка) – засіб, який використовується для позначення (ідентифікації) кінцевого обладнання абонента в електронній комунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо);
- мережевий ідентифікатор споживача – індивідуальний набір цифр та/або символів, присвоєний кінцевому обладнанню абонента та/або споживачеві в електронній комунікаційній мережі чи Інтернеті. Під ним потрібно розуміти або номер абонента в мережах GSM, CDMA або IP-адресу електронної інформаційної системи (ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад, Інтернет));
- MAC-адреса (*Media Access Control* – управління доступом до носія) – унікальний ідентифікатор, що зіставляється з різними типами обладнання для комп'ютерних мереж (мережевими картами, Wi-Fi роутерами тощо). Усі комп'ютери, підключені до локальної мережі з виходом в Інтернет, як правило, мають дві адреси: логічну адресу мережевого рівня (IP-адресу) і фізичну адресу мережевої інтерфейсної карти (MAC-адресу).

[113] П. 3 Правил надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України № 295 від 11 квітня 2012 р.: [із змінами і доповненнями на 08.04.2013] *Офіційний вісник України*. 2012. № 29. Ст. 1074.

257 Не можна погодитися з думкою, що на сьогоднішній день у слідчого, прокурора чи оперативних підрозділів відсутні практичні можливості надати слідчому судді відомості, які унікально ідентифікують абонента спостереження, адже відсутні документальні підтвердження факту користування конкретною особою кінцевим обладнанням (мобільним телефоном)[114]. Варто зауважити, що закон вимагає від слідчого, прокурора вказати ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження або кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування. Тож, навіть у випадку відсутності договору з оператором мобільного зв'язку конкретної фізичної особи, органи досудового розслідування мають право надавати інформацію, яка ідентифікує кінцеве обладнання, а не абонента.

258 Проведення зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. Керівники та працівники операторів електронних комунікацій зобов'язані сприяти виконанню дій із зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді.

259 За результатами проведення цієї НСРД складається протокол, у якому вказують дату його складення, посаду,

[114] *Самбор М. А*. Негласні слідчі (розшукові) дії, пов'язані із зняттям інформації з транспортних телекомунікаційних мереж та встановленням місцезнаходження радіоелектронного засобу: підстави для проведення та умови гарантування прав і свобод людини та громадянина як споживача послуг рухомого (мобільного) зв'язку. *Вісник Дніпропетровського університету ім. А. Нобеля*. 2013. № 1. С. 78. (Серія «Юридичні науки»).

прізвище та ініціали особи, що здійснює кримінальне провадження, номер кримінального провадження у ЄРДР, номер відповідної ухвали, а також дату її прийняття та найменування суду, слідчим суддею якого надано дозвіл на зняття інформації з електронних комунікаційних мереж та строки його здійснення. Окрім того, у протоколі зазначають найменування підрозділу, працівники якого залучалися до здійснення зняття інформації з електронних комунікаційних мереж, дані про особу, стосовно якої здійснювалася НСРД, її результати, відомості про МНІ (матеріали аудіо- чи відеозапису, фото- і кінозйомки, магнітні накопичувачі тощо)[115].

Окрім складання цього протоколу ст. 265 КПК визначає, що 260
зміст інформації, яка передається особами через електронні комунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення зняття інформації з електронних комунікаційних мереж. При виявленні в інформації відомостей, що мають значення для конкретного досудового розслідування, в протоколі відтворюється відповідна частина такої інформації, після чого прокурор вживає заходів для збереження знятої інформації. Своєю чергою зміст інформації, одержаної внаслідок здійснення зняття інформації з електронних комунікаційних мереж, фіксується на відповідному носієві особою, яка здійснювала зняття та зобов'язана забезпечити обробку, збереження або передання інформації.

Отримана у такий спосіб звукова інформація має бути 261
розшифрована уповноваженою службовою особою із залученням, у необхідних випадках, відповідного спеціаліста. До протоколу цієї НСРД вносяться лише ті фрагменти, які мають значення для

[115] Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1/ за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. С. 668.

кримінального провадження. Як спеціалісти у цьому випадку можуть залучатися фахівці у галузі економіки, кредитування, аграрного сектору, природних ресурсів тощо, залежно від виду розслідуваного кримінального правопорушення. Якщо особи, чия звукова інформація знята з електронних комунікаційних мереж, спілкувалися іноземною мовою, для розшифровування (перекладу) інформації залучають перекладача. Носії інформації, на яких міститься звукозапис розмов, можуть бути досліджені на предмет ототожнення особи за фізичними параметрами голосу та встановлення технічних умов і технології отримання відео-, звукозапису[116].

262 Протоколи про проведення зняття інформації з електронних комунікаційних мереж з додатками не пізніше ніж через двадцять чотири години з моменту припинення вказаних НСРД передають прокурору (ч. 3 ст. 252 КПК).

263 Забороняється використання відомостей, речей та документів, отриманих у результаті проведення НСРД для цілей, не пов'язаних із кримінальним провадженням, або ознайомлення з ними учасників кримінального провадження чи будь-яких інших осіб. Якщо протоколи про проведення НСРД, зокрема зняття інформації з електронних комунікаційних мереж, містять інформацію щодо приватного (особистого чи сімейного) життя інших осіб, захисник, а також інші особи, які мають право на ознайомлення з протоколами, попереджаються про кримінальну відповідальність за розголошення отриманої інформації щодо інших осіб.

---

[116] Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: [навч.-практ. посібник] / Б. І. Бараненко, О. В. Бочковий, К. А. Гусєва та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка. 2014. С. 210.

264 Потрібно враховувати, що МНІ, на яких зафіксовано телефонні розмови осіб, є речовими доказами особливого виду – похідними від усного спілкування. Тому, враховуючи принцип безпосередності дослідження доказів і для перевірки обставин отримання звукозапису, необхідно отримати також показання хоча б однієї з осіб, яка брала участь у телефонній розмові, якщо це можливо. В іншому випадку для перевірки достовірності звукозапису та ідентифікації осіб, які спілкувалися між собою, може бути призначена фоноскопічна (фонографічна) експертиза, яка може дати відповіді на такі питання: Кому з-поміж перелічених осіб належать окремі вислови, що містяться на фонограмі?; Чи є голос, зафіксований на фонограмі, голосом конкретної особи?; Чи зазнавала змін ця фонограма?; Чи наявні ознаки монтажу фонограми?; Які є ознаки механічного та електронного монтажу фонограми?; Чи велась зафіксована на фонограмі розмова по телефону? тощо.

265 Складнощі виникають з матеріалами звукозапису, виготовлених з використанням цифрової техніки. Експерти досі не мають технічної можливості встановити наявність або відсутність ознак монтажу. Якщо експерти роблять висновок про те, що встановити наявність або відсутність ознак монтажу неможливо, зафіксовані на відповідному носії дані стають сумнівними[117].

266 У пам'яті обладнання постачальників електронних комунікаційних послуг часто залишаються дані (SMS, MMS, *e-mail* та інші повідомлення) з текстовою, а також фото-, відеоінформацією, що передається як кореспонденція між особами. Проте варто врахувати, що повідомлення, які надійшли на пошту електронної адреси, SMS, MMS та ін., у тому числі й голосова пошта, повідомлення на автовідповідач, але не відкриті

[117] *Уваров В. Г.* Зняття інформації з технічних каналів зв'язку. *Зовнішня торгівля: економіка, фінанси, право.* 2013. № 2. С. 180.

для прочитування (прослуховування, перегляду), належать до категорії кореспонденції, що охоплюється ст. 8 ЄКПЛ, і доступ до них може бути здійснено лише на підставі статей 261, 263 КПК. Але якщо буде встановлено, що отримувач ознайомлений з їхнім змістом, то вони можуть бути доступними для вилучення в порядку норм глави 15 КПК[118].

267 Окрім того, потрібно враховувати випадки, що навіть, якщо здійснюється онлайн-трансляція, яка є предметом зняття інформації з електронних комунікаційних мереж, то в ході її проведення все одно одержуються цифрові докази. Такий підхід також використовує Верховний Суд, який зазначає, що оскільки зображення через веб-камеру одного комп'ютера транслюється на монітор іншого комп'ютера в системі загальної для них мережі, за час проходження через останню має місце запізнення сигналу з тимчасовим збереженням зображення на серверах та у пам'яті електронних пристроїв для здійснення безперервного потоку інформації шляхом буферизації та створення тимчасових файлів, то фактично наявна форма його матеріальної фіксації в комп'ютерній мережі, в якій відбувається трансляція, хоча і на дуже незначний час[119].

268 **Зняття інформації з електронних інформаційних систем.** Відповідно до п. 1.11.6. Інструкції – зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

---

[118] *Тагієв С.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Часопис цивільного і кримінального судочинства*. 2013. № 4. С. 105.

[119] Постанова Верховного суду від 18.06.2020 року у справі № 711/7900/17. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/89929158

З таким визначенням можна погодитися лише частково, 269
оскільки одержання інформації, що міститься в комп'ютерній мережі за загальним правилом повинно охоплюватись такою НСРД, як зняття інформації з електронних комунікаційних мереж. Отримання такої інформації в межах зняття інформації з електронних інформаційних систем можливе лише в тому випадку, коли жоден із елементів локальної мережі не під'єднаний до глобальної мережі.

Електронно-обчислювальна машина (ЕОМ, комп'ютер) являє 270
собою сукупність технічних засобів та системного програмного забезпечення, створює можливість автоматизованого оброблення інформації та отримання результату в необхідній формі. Крім того, відповідно до державних стандартів, комп'ютер – це функціональний пристрій, що складається з одного або кількох взаємопов'язаних центральних процесорів і периферійних пристроїв й може виконувати обчислення без участі людини. Комп'ютер, призначений для обслуговування одного користувача, що характеризується невеликими габаритами, підвищеною надійністю, простотою зміни конфігурації та розвинутими засобами діалогу, є персональним комп'ютером.

Автоматизованою є система, що здійснює автоматизовану 271
обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

Комп'ютерна (інформаційна) мережа – це сукупність 272
територіально розосереджених систем оброблення даних, засобів та/або систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів.

Мережа електрозв'язку являє собою комплекс технічних 273
засобів електронних комунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання

знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, провідних, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

274 Відповідно до ст. 1 ЗУ «Про захист інформації в інформаційно-комунікаційних системах», інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів[120].

275 Зняття інформації з електронних інформаційних систем або їх частин може відбуватися як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного проникнення. Негласне зняття інформації із засобів електронно-обчислювальної техніки полягає у застосуванні засобів спеціальної техніки із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диска (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого, що можуть містити інформацію, яка має значення у кримінальному провадженні. Програмне проникнення до електронних інформаційних систем (їх частин) відбувається шляхом застосування спеціальних програмних продуктів, які забезпечують копіювання інформації, що обробляється на ПЕОМ підозрюваного, обвинуваченого, на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю негласну слідчу (розшукову) дію[121].

---

[120] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 : [із змінами і доповненнями на 01.07.2022]. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

[121] Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1/ за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. С. 670–671.

У клопотанні на отримання дозволу на зняття інформації з електронних інформаційних систем слідчий або прокурор повинні зазначити такі відомості: найменування кримінального провадження та його реєстраційний номер; короткий виклад обставин злочину, у зв'язку з розслідуванням якого подається клопотання; правова кваліфікація злочину із зазначенням статті (частини статті) закону України про кримінальну відповідальність; відомості про особу (осіб), місце або річ, щодо яких необхідно провести НСРД; обставини, що дають підстави підозрювати особу у вчиненні злочину; обґрунтування строку проведення зняття інформації з електронних інформаційних систем; обґрунтування неможливості отримання відомостей про злочин та особу, яка його вчинила, в інший спосіб; відомості про ідентифікаційні ознаки електронної інформаційної системи; обґрунтування можливості отримання під час проведення цієї НСРД доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин злочину або встановлення осіб, які його вчинили. До клопотання слідчого, прокурора додається витяг з ЄРДР щодо кримінального провадження, у межах якого подається клопотання. 276

В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування. 277

Ідентифікаційними ознаками електронної інформаційної системи є: 278

- IP-адреса (IP – Internet Protocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету;
- доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти;

– серійний номер та характеристики автоматизованої системи та ЕОМ.

279 В літературі висловлено пропозицію про те, що зняття інформації з електронних інформаційних систем проводиться у присутності власника, володільця чи утримувача та користувача електронної інформаційної системи і двох понятих, а перед зняттям інформації з електронних інформаційних систем слідчий пред'являє постанову про проведення указаної слідчої дії власнику, володільцю, утримувачу чи користувачу електронної інформаційної системи і пропонує їм відкрити доступ до необхідної для справи інформації[122]. Навряд чи можна погодитися з такою думкою, оскільки такий механізм фактично призводить до втрати цією НСРД її основних ознак, а саме призведе того, що відомості про факти її проведення стануть відомі учасникам кримінального провадження, а отже буде втрачена ознака негласності та конспіративності проведення цієї НСРД.

280 Під час проведення НСРД щодо цифрової інформації збір і аналіз кількісного та якісного складу інформації, яка передається через електронні комунікаційні системи певного комп'ютера, у практичній діяльності можуть бути замінені офіційним вилученням цього комп'ютера та проведенням щодо нього експертизи, оскільки це допоможе отримати інформацію тотожну тій, що перехоплювалась. Однак у такому випадку буде порушено негласність, а для вилучення й тимчасового доступу

[122] *Уваров В. Г.* Зняття інформації з електронних інформаційних систем: новели КПК України та євростандарти. *Форум права*. 2012. № 4. С. 942; *Уваров В. Г.* Втручання у приватне життя шляхом зняття інформації з електронних інформаційних систем: новели нового КПК України та євро стандарти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2012. № 3. С. 443; *Уваров В. Г.* Зняття інформації з електронних інформаційних систем: новели КПК України та євростандарти. *Вісник ХНУВС*. 2012. № 4. Ч. 1. С. 174.

до комп'ютера будуть необхідні процесуальні підстави, тобто ухвала слідчого судді[123].

Всі способи зняття інформації з електронних інформаційних 281
систем можна об'єднати в дві основні групи.

Перша група – це способи безпосереднього доступу. При їх 282
реалізації інформація отримується шляхом видачі відповідних команд з комп'ютера, на якому ця інформація знаходиться.

Друга група охоплює способи опосередкованого 283
(віддаленого) доступу до комп'ютерної інформації.

До них можна віднести: 284

- підключення до лінії зв'язку користувача (наприклад, до телефонної лінії або оптоволоконної лінії) й отримання цим шляхом доступу до електронної інформаційної системи;
- проникнення в комп'ютерну систему за допомогою підбору паролів і т. п.

У протоколі НСРД підлягають відображенню такі відомості: 285
в пам'яті якого пристрою виявлено віртуальні сліди; кому належить пристрій; чи має пристрій вихід у мережу Інтернет, інші електронні комунікаційні або локальні мережі; яка оперативна система функціонує на пристрої (*MacOS, Windows, Linux* – на комп'ютері, *iOS*, *Android*, *HarmonyOS*, *Windows mobile, Symbian* – на мобільному телефоні, комунікаторі, планшеті і т.п.); в яких файлах виявлені сліди втручання, які саме; коли файл був створений, змінений, відкривався востаннє. Щоб уникнути вивчення кожного файлу комп'ютера (кількість файлів може вимірюватися сотнями тисяч) до проведення НСРД необхідно залучати спеціаліста (програміста, системного адміністратора і т. д.).

---

[123] *Юхно О. О.* Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2. С. 90.

286 Варто погодитися з думкою, що, крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу про проведення НСРД, в ньому бажано фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення:

1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника;
2) серійний номер технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення;
3) наявний стан зношеності або будь-яких дефектів зовнішнього вигляду чи у роботі використаного технічного засобу, пристрою, обчислювальної техніки, програмного забезпечення (визначається зовнішнім візуальним оглядом слідчого чи оперативного працівника);
4) умови, у яких було використано технічний засіб, пристрій, обчислювальну техніку або програмне забезпечення, а також дату й точний час;
5) всю інформацію в цифровому вигляді, яка представляє процесуальний або оперативний інтерес незалежно від того, на якому носії вона знаходиться, бажано оглянути в присутності спеціаліста й понятих, після чого скопіювати її на матеріальний носій, який повинен бути долучений до протоколу проведення НСРД незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації[124];
6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диска комп'ютера,

[124] Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід : монографія. Харків : Право, 2017. С. 159.

необхідно користуватися програмним забезпеченням для побітового копіювання інформації, а після копіювання до протоколу проведення НСРД необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено[125].

Не потребує дозволу слідчого судді здобуття відомостей з 287
електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту. Проведення цієї НСРД без дозволу слідчого судді допускається у тому випадку, коли потрібно:

- отримати інформацію, розміщену особою у соціальних мережах, тематичних форумах;
- встановити ідентифікаційні ознаки електронної інформаційної системи за допомогою спеціальних програмних утиліт. Перший їх вид – це утиліти, що надають інформацію про комп'ютери-хости та мережі. Така інформація є необхідною для адресації в мережі і тому є доступною. Другий вид – це утиліти для збору інформації про окремих користувачів, наприклад, реальне ім'я користувача, останній час та дата входження до системи; специфічний вид активності користувача, який увійшов до системи, а інколи навіть поштова адреса та телефон користувача. Однак потрібно пам'ятати, що така інформація може бути несправжньою. Крім того, забороняється використовувати специфічні утиліти, які обходять обмеження, встановлені для користувачів

[1] *Юхно О. О.* Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2. С. 93.

системи. Це, наприклад, різноманітні програми «сніфери», які можна використовувати для перехоплення імен та паролів користувачів[126];
- поспілкуватися з особою за допомогою технології IRC (*Internet Relay Chat*) або *ICQ*;
- ознайомитися з інформацією на робочому комп'ютері працівника, за умови, що користувач не використовує системи логічного захисту інформації (паролі, криптографічні або інші програми захисту інформації).

288 **Аудіо-, відеоконтроль місця.** Відповідно до ст. 270 КПК, аудіо-, відеоконтроль місця як НСРД полягає у здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць без відома їх власника, володільця або присутніх у цьому місці осіб, за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження. Законом ця НСРД віднесена до «інших видів негласних слідчих (розшукових) дій», хоча за своїм характером вона також пов'язана із втручанням у приватне спілкування, оскільки передбачає приховане фіксування відомостей про розмови і поведінку осіб у конкретному місці.

289 Метою зазначеної НСРД є прихована фіксація з використанням аудіо-, відеозаписуючих пристроїв поведінки особи, її розмов або інших рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які відбуваються у публічно доступних місцях, що мають значення для кримінального провадження. Завданням цієї дії є виявлення

[126] Оперативно-розшукова компаративістика : монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. Харків : Золота миля, 2013. С. 283–284.

відомостей, які містять ознаки підготовлюваного, вчинюваного або вчиненого тяжкого або особливо тяжкого злочину.

Об'єктом аудіо-, відеоконтролю місця є приватне 290
спілкування особи у публічно доступному місці у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які там відбуваються, зміст яких має значення для досудового розслідування.

Суб'єкти проведення аудіо-, відеоконтролю місця аналогічні 291
тим, які проводять аудіо-, відеоконтроль особи.

Аудіо-, відеоконтроль місця може проводитись у громадських 292
місцях та в місцях загального користування, доступ до яких необмежений, тобто всередині публічно доступних місць, до яких, відповідно до ч. 2, 3 ст. 267 КПК можна увійти або в яких можна перебувати на правових підставах без відома їх власника, володільця або присутніх у цьому місці осіб. Такими місцями є кінотеатри, ресторани, кафе, музеї тощо.

Процесуальний порядок проведення та фіксації цієї НСРД 293
аналогічний аудіо-, відеоконтролю особи.

Загалом, аналізуючи аудіо-, відеоконтроль місця як 294
НСРД варто відзначити, що вона є подібною до аудіо-, відеоконтролю особи та спостереженням за особою, річчю або місцем як НСРД. Відрізняються вони місцем їх проведення, організаційно-тактичними особливостями їх здійснення та рівнем технологізації. Як уже зазначалося, законотворці деяких зарубіжних держав, унормовуючи положення процесуальних кодексів, не розмежовують аудіо-, відеоконтроль місця та особи (зокрема, у Республіці Казахстан).

Визначаючи особливості аудіо-, відеоконтролю особи, які 295
відрізняють її від спостереження за особою, річчю або місцем, аудіо-, відеоконтролю місця, С. Фомін і С. Гриненко зазначають про те, що вона проводиться щодо конкретної особи як у публічно доступних, так і у публічно недоступних місцях (місцях,

до яких неможливо увійти або в яких неможливо перебувати на правових підставах без отримання на це згоди власника, користувача або уповноважених ними осіб (ч. 2 ст. 267 КПК) чи в умовах, коли учасники спілкування мають достатні підстави вважати, що спілкування є приватним (розумно розраховують на приватність)[127]. Р. Шехавцов і М. Шумило також уважають, що відмінність аудіо-, відеоконтролю особи від передбачених ст.ст. 269, 270 КПК НСРД полягає у використанні аудіо-, відеозаписуючих пристроїв, встановлених усередині публічно недоступних місць для фіксації поведінки особи[128].

296 Також у літературі зазначено, що якщо для візуального спостереження за особою основним завданням є з'ясування і фіксація відомостей щодо її пересування, місць перебування, фактів зустрічей з іншими особами як із застосуванням технічних засобів, так і без, то аудіо-, відеоконтроль особи – НСРД, яка здійснюється з метою отримання інформації і джерелом якої є особа – об'єкт контролю: дії, рухи, висловлювання та інша аудіовізуальна інформація, при цьому місце її знаходження має факультативне значення. Вона проводиться винятково з використанням технічних засобів фіксації інформації[129].

297 Зокрема, Ю. Лисюк зазначає, що нормами КПК передбачається проведення аудіо-, відеоконтролю у двох напрямках, які, на його думку, мають на меті отримання одного й того ж результату, хоча досягають його дещо відмінними

---

[127] Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін. ; за заг. ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. С. 436.

[128] Кримінальний процесуальний кодекс України : наук.-практ. коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. Київ : Юстініан, 2012. С. 574.

[129] Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін. ; за заг. ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. С. 436–437.

способами. Говорячи про відмінність аудіо-, відеоконтролю особи та місця, автор переконує, що єдиною відмінністю цих дій є те, що вони відрізняються місцем їх проведення, тобто здійснюються шляхом установлення СТЗ у публічно доступних місцях, а також інколи в місцях імовірної появи особи. Також особливістю здійснення цих дій є те, що вони відрізняються своїми організаційно-тактичними особливостями, тобто проводяться у громадських місцях і місцях загального користування, доступ до яких не обмежений, і з обов'язковим визначенням в ухвалі слідчого судді повної та точної адреси місця, де проводитиметься НСРД, час і строки її здійснення[130].

298 Отже, особливостями аудіо-, відеоконтролю місця є: 1) проводиться лише у публічно доступних місцях; 2) їх об'єктом є приватне спілкування особи (не конкретної) у вигляді розмов або інших звуків, рухів, дій, пов'язаних із її діяльністю або місцем перебування, а також інші події, які там відбуваються; 3) організаційно-тактичні особливості проведення.

299 **Тимчасовий доступ до речей та документів.** Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої перебувають такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

300 На підставі аналізу ст. 162 КПК України можна зробити висновок, що найпоширенішою групою електронних доказів є інформація, яка знаходиться в постачальників електронних комунікаційних послуг, про зв'язок, абонента, надання електронних комунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

---

[130] *Лисюк Ю. В.* Аудіо-, відеоконтроль як різновид втручання у приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Науковий вісник Херсонського державного університету*. 2014. Вип. 6–1. Т. 4. С. 79.

301 Також у режимі тимчасового доступу можна отримати доступ до електронних документів, які знаходяться у юридичних та фізичних осіб, зокрема запису камер вуличного спостереження, камер банкоматів тощо. Однак Верховний Суд уважає, що для отримання таких доказів достатньо витребувати їх на підставі запиту слідчого. Так, судді ВС наголосили, що тимчасовий доступ до речей і документів стороні кримінального провадження надається на підставі ухвали слідчого судді місцевого суду під час досудового розслідування чи суду під час судового провадження у випадку, коли в інший спосіб неможливо отримати речі і документи, які можуть мати значення у справі.

302 Як убачається з матеріалів провадження, наявний у справі DVD-R-диск з відеозаписом обставин події з камер відеоспостереження був добровільно наданий директором ТОВ «Р» на запит слідчого, а отже, необхідності звертатися з відповідним клопотанням до слідчого судді для отримання копії цього запису в останнього не було[131].

303 Інформація, що зберігається в постачальників електронних комунікаційних послуг, – це відомості, що виникають під час експлуатації систем мобільного зв'язку як безпосередньо користувачем, а також в операційно-інформаційних системах і центрах комутації операторів мобільного зв'язку. Залежно від місця концентрації, інформація, що зосереджена у засобах систем мобільного зв'язку, міститься: у призначеному для користувача устаткуванні (абонентській станції, абонентському пристрої); різних файлах: текстових, звукових, фото, відео; в операційно-інформаційних системах і центрах комутації оператора стільникового (мобільного) зв'язку (безпосередньо в операторів)[132].

---

[131] Постанова Верховного суду від 10.09.2020 року у справі № 751/6069/19. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/91722819.

[132] *Сербінов О. С.* Окремі види інформації про абонента, яка знаходиться у користуванні операторів мобільного зв'язку та може бути отримана у

Увесь масив інформації про абонента, що зберігається в 304
постачальників електронних комунікаційних послуг, можна поділити на дві групи: перша – відомості стосовно наданих електронних комунікаційних послуг; друга – відомості про споживача, одержані при укладанні договору. До першої групи варто віднести, зокрема: дані про з'єднання терміналів абонентів операторів мобільного зв'язку у певний час («трафіки»), з'єднання певних абонентських номерів або терміналів за певний період часу («звіти»), з'єднання невизначеного кола абонентських номерів (із зазначенням IMEI-терміналу), що відбулись у межах дії певної базової станції за певний період часу («моніторинги») тощо. Відомості про споживача, одержані при укладанні договору – це особисті дані про абонента (копія паспорта, посвідчення водія, службового посвідчення працівника органів державної влади або місцевого самоврядування тощо); реєстраційні дані документів, ідентифікаційний код; відомості стосовно адреси реєстрації, фактичного місця проживання, контактного телефону, адреси електронної пошти тощо[133].

До клопотання слідчий або прокурор повинен також додати: 305

а) відомості (копії довідки оператора, провайдера, протокол допиту, слідчих дій і тощо) про ознаки, які дозволять ідентифікувати абонента шляхом уніфікації мереж (№ SIM карти, IMEI, *e-mail* тощо);

б) копії інших матеріалів, які мають вагоме значення при розгляді клопотання – слідчий суддя, суд при постановленні ухвали в резолютивній частині повинен

ході проведення оперативно-розшукових заходів або слідчих дій. *Адвокат.* 2009. № 1. С. 38.

[133] Використання можливостей операторів стільникового (мобільного) зв'язку для розкриття та розслідування злочинів [Текст] : метод. рекомендації / [Чернявський С. С., Татаров О. Ю., Алексеєва-Процюк Д. О. та ін.]. Київ : Нац. акад. внутр. справ, 2012. С. 15.

зазначати повні дані про особу, щодо якої отримується інформація (прізвище, ім'я, по батькові, місце роботи та ін.);

в) повний номер IMEI, назву оператора, провайдера, номери мобільних станцій, № SIM карти, телефону зі зазначенням коду держави України +38. (Наприклад +38 № SIM-карти телефону; точної електронної адреси мовою оригіналу, із зазначенням знаків розділу; адреси ІА; паролів SIM-карти; номера ICQ; оригінальні назви сайтів; IP-адреси, тощо)[134].

306 Варто погодитися з думкою, що правильною видається практика долучення до клопотання матеріалів радіотехнічної розвідки, які дозволяють додатково ідентифікувати базові станції через які здійснювали спілкування підозрювані, а отже обмежити порушення таємниці спілкування невизначеної кількості абонентів[135].

307 При цьому потрібно враховувати, що радіотехнічна розвідка полягає в установленні постачальниками послуг рухомого зв'язку технічного обладнання, яким охоплюється певна територія або місце. У зв'язку з цим вона не є різновидом втручання в приватне спілкування, а тому проводиться без ухвали слідчого судді[136]. Радіотехнічна розвідка повинна проводитися на підставі доручення на проведення радіотехнічної розвідки

---

[134] *Тагієв С. Р.* Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 21.

[135] *Ткачик А. Б.* Таємниця спілкування та її обмеження в кримінальному провадженні : дис. … д-ра філос. за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 – Право). Львівський державний університет внутрішніх справ, Львів, 2021. С. 107.

[136] Постанова Верховного суду від 16.03.2021 р. у справі № 364/673/18. URL : https://ips.ligazakon.net/document/c017923?an=&ed=&dtm=&le=.

виданого слідчим чи прокурором на підставі п. 3 ч. 2 ст. 40 КПК відповідному оперативному підрозділу.

308 У разі задоволення клопотання ухвала слідчого судді про надання тимчасового доступу до речей і/або документів повинна містити чітку вказівку на те:

- хто повинен надати тимчасовий доступ до речей і документів (із зазначенням повної та точної назви юридичної особи її юридичної адреси;
- якщо вказаний обов'язок покладено на фізичну особу, то зазначається її прізвище, ім'я та по батькові);
- кому повинно бути надано тимчасовий доступ до речей і документів (із зазначенням прізвища, імені, по батькові, а також посади уповноваженої особи);
- які саме необхідно надати документи для ознайомлення, отримання їх копій чи здійснення виїмки;
- який строк встановлено для застосування вказаного заходу[137].

309 Ураховуючи специфіку формату зберігання інформації, що передбачена п. 7 ч. 1 ст. 162 КПК України і знаходиться в постачальників електронних комунікаційних послуг, надання доступу до відповідних документів (тобто надання можливості ознайомитися з ними та зробити з них копії), може відбуватися як безпосередньо в оператора (провайдера), так і шляхом надання доступу до відповідних документів уповноваженому на зняття інформації з електронних комунікаційних мереж підрозділу правоохоронного органу через відповідні інформаційні системи відповідно до встановленого порядку з обов'язковим наданням копії ухвали слідчого судді відповідному оператору (провайдеру)[138].

---

[137] *Сліпченко В. І.* Тимчасовий доступ до речей і документів: процесуальний порядок отримання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2013. № 2. С. 512.

[138] *Алєксєєва-Процюк Д. О., Брисковська О. М.* Особливості проведення тимчасового доступу до речей та документів для отримання інформації від операторів мобільного зв'язку. *Митна справа*. 2013. № 1. С. 58–65.

310 Одержання (вилучення) інформації безпосередньо в постачальників електронних комунікаційних послуг вимагає забезпечення участі у проведенні цього заходу спеціалістів, передусім фахівців у галузі комп'ютерних технологій, засобів зв'язку або обслуговування мережі. Вилучення електронних комунікаційних повідомлень здійснюється у присутності представника оператора мобільного зв'язку, понятих (бажано з числа працівників фірми-оператора). Залежно від змісту повідомлень, вони можуть бути вилучені шляхом копіювання вмісту на магнітні носії комп'ютерної інформації (у цьому разі ще на підготовчій стадії вилучення необхідно підготувати апаратно-технічні засоби для зчитування і збереження інформації, що вилучається, перелік яких варто попередньо узгодити зі спеціалістом, а також переносні накопичувальні пристрої)[139].

311 **Отримання електронних доказів від учасників кримінального провадження.** Верховний Суд правильно дійшов висновку, що добровільне надання свідком стороні обвинувачення диска з відеозаписом ДТП, що було підтверджено ним у судовому провадженні, а не отримання його на підставі тимчасового доступу до речей і документів, не є підставою для визнання такого доказу недопустимим. Диск як матеріальний носій є способом збереження інформації з електронного документа і вважається його оригіналом, а тому є належним та допустимим доказом у кримінальному провадженні.

312 При цьому суд керувався такими міркуваннями. Відповідно до приписів частин 1, 2 ст. 93 КПК, збирання доказів здійснюється сторонами кримінального провадження у порядку, передбаченому цим Кодексом. Сторона обвинувачення

[139] *Чернявський С. С., Фінагеєв В. О.* Проблеми тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 183.

здійснює збирання доказів шляхом як проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, так і витребування та *отримання* від органів державної влади, місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених КПК.

Наведеними кримінальними процесуальними нормами 313
встановлено порядок отримання стороною обвинувачення від особи за її ініціативою і доброю волею, диска з відеозаписом із відеореєстратора, наданого за її письмовою заявою на ім'я слідчого, що свідок підтвердила в судовому провадженні.

При цьому необхідно зважати на те, що згідно з ч. 4 314
ст. 132 КПК, для оцінки потреб досудового розслідування варто враховувати можливість отримати речі й документи, які можуть бути використані під час судового розгляду для встановлення обставин у кримінальному провадженні, без застосування заходу забезпечення кримінального провадження.

Отримання тимчасового доступу до речей, документів і, 315
за наявності підстав для того, розпорядження про надання можливості вилучення речей і документів, обумовлене, за приписами ст. 163 КПК, необхідністю доведення стороною кримінального провадження наявності достатніх підстав уважати, що без такого доступу та вилучення існує реальна загроза зміни або знищення речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів.

За відсутності таких обставин, тим більше за умови 316
добровільного надання документів стороною чи учасником кримінального провадження, у володінні яких вони перебувають, не виникає підстав та умов до звернення з клопотанням до слідчого судді стосовно застосування заходів забезпечення

кримінального провадження у вигляді тимчасового доступу до документів і речей[140].

317 Аналогічну позицію висловив Верховний Суд в іншій аналогічній справі. Зокрема, він вказав, що збирання та подання доказів у кримінальному провадженні є різними способами одержання доказової інформації з огляду на їх відмінну правову природу, а саме збирання доказів відбувається через інститут слідчих дій, а подання доказів здійснюється особою добровільно шляхом передачі слідчому, прокурору предметів або документів, які, на її думку, мають значення для кримінального провадження. Під час отримання предметів та документів, представлених особою для залучення їх до справи як докази, орган дізнання, слідчий або суд повинні допитати цю особу з метою з'ясування джерела та обставин їх отримання, потім здійснити огляд цих предметів або документів і процесуально зафіксувати їх отримання.

318 Як вбачається з матеріалів кримінального провадження, свідок добровільно та за власною ініціативою надав слідчому зазначений диск з відеозаписом з камер відеоспостереження. Зазначений факт свідок підтвердив під час його допиту в суді першої інстанції.

319 Тож, надання цього диска з відеозаписом безпосередньо свідком, не можна вважати порушенням вимог ст. 93 КПК, оскільки сторона обвинувачення здійснює збирання доказів шляхом, у тому числі, отримання від фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом[141].

---

[140] Постанова Верховного суду від 31.03.2021 р. у справі № 333/1539/16-к. URL : https://ips.ligazakon.net/document/c018510?an=88

[141] Постанова Верховного суду від 19.05.2021 р. у справі № 204/4521/18. URL : https://ips.ligazakon.net/document/c018840

Відповіді на запитання кейсів

КЕЙС 1. *В описаній ситуації доцільно провести комплекс НСРД, спрямованих на встановлення особи підозрюваного та отримання необхідної доказової інформації про обставини вчиненого кримінального правопорушення.*

Зокрема, потрібно провести:

- *зняття інформації з електронних комунікаційних мереж, використовуючи ідентифікуючі ознаки: номер мобільного телефону (050-721-66-92) та електронну адресу – ivan@mail.ru;*
- *за можливості зняття інформації з електронної інформаційної системи мобільного терміналу з номером (050-721-66-92).*

КЕЙС 2. *В описаній ситуації необхідно провести судову комп'ютерно-технічну експертизу, предметом якої виступатимуть: а) комп'ютерна техніка; б) мобільні телефони. Доручити проведення відповідної експертизи треба експертам НДЕКЦ або НДІСЕ.*

Орієнтовні питання комп'ютерно-технічної експертизи телефона:

Які контакти та їх номери містяться на мобільному телефоні марки "..." IMEI ..., та сім-карті стільникового зв'язку "...", яка в ньому знаходиться?

Дзвінки на які номери мобільних операторів здійснено та з яких номерів мобільних операторів отримувались дзвінки із зазначенням дати та часу з мобільного телефону, із сім-карткою стільникового зв'язку, яка в ньому знаходиться?

Які повідомлення містяться, на які номери мобільних операторів вони відправлялись та з яких отримані із зазначенням дати та часу з мобільного телефону, із сім-карткою стільникового зв'язку, яка в ньому знаходиться?

Чи містяться в наданому на дослідження мобільному телефоні "..." IMEI ... з карткою мобільного оператора за номером ..., який належить ... програма "..."?

Під якими обліковим записом, псевдонімом, номером телефону у вказаній програмі зареєстрований власник мобільного телефону?

Які переписки містяться у програмі "..."?
Яка інформація про дзвінки та СМС-повідомлення міститься у пам'яті телефону?
Чи міститься у пам'яті телефону зображення?

Орієнтовні питання комп'ютерно-технічної експертизи комп'ютерної техніки:
Чи є пристрої (системні блоки "..." в кількості ... шт.), надані для проведення експертизи, у працездатному стані?
До якого типу належать надані для проведення експертизи пристрої?
Чи є пристрої, надані для проведення експертизи, виготовленими заводським способом, і хто їх виробник?
Яке програмне забезпечення міститься та використовувалось на наданих для дослідження пристроях, та яке функціональне призначення цього програмного забезпечення?
Які інтернет-ресурси відвідували з наданих на дослідження пристроїв?
Чи містяться на наданих для дослідження пристроях програмні налаштування для підключення до зовнішніх серверів, якщо так, то до яких саме?
Чи можливе використання пристроїв, наданих для проведення експертизи, в якості пристроїв для проведення азартних ігор для отримання виграшу?

Запитання для самоконтролю

1. Якими унікальними особливостями характеризується інформація, створена за допомогою високих інформаційних технологій?
2. На яких рівнях функціонує інформація в ЕОМ?
3. Які особливості перевірки цифрового алібі?
4. Яким умовам повинна відповідати виявлена помилка програмного забезпечення?
5. Які основні методи фіксації інформації з веб-сайту?
6. Розмежуйте поняття електронного доказу та його носія.
7. Чи є поняття електронного документа та електронного доказу тотожними?

8. У чому суть належності електронного доказу як його юридичної властивості?

9. У чому суть допустимості електронного доказу як його юридичної властивості?

10. У чому суть достовірності електронного доказу як його юридичної властивості?

11. Чи впливає відсутність кваліфікованого електронного підпису електронного документа на достовірність певних даних в електронній формі та їх доказове значення?

12. У чому суть «принципу недискримінації при дослідженні електронних доказів»?

13. Поясність зміст презумпції цілісності (достовірності) електронних доказів.

14. Чи застосовним до електронних доказів є принцип самоідентифікації автора?

15. Які можна виокремити способи перевірки та оцінки електронних доказів?

16. Які підстави проведення аудіо-, відеоконтролю особи?

17. Які завдання проведення аудіо-, відеоконтролю особи?

18. Що потрібно розуміти під електронною комунікаційною мережею?

19. На кого покладається обов'язок зняття інформації з електронних комунікаційних мереж?

20. Які ідентифікаційні ознаки електронних комунікаційних мереж повинні бути зазначені в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування?

21. Що потрібно розуміти під електронною інформаційною системою?

22. На які види можна поділити електронні інформаційні системи за архітектурою?

23. У яких випадках не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем?

24. Що потрібно розуміти під подоланням системи логічного захисту електронної інформаційної системи?

25. Які ідентифікаційні ознаки електронної інформаційної системи повинні бути зазначені в ухвалі слідчого судді про дозвіл на втручання у приватне спілкування?

26. Які засоби захисту інформації, отриманої в результаті НСРД, передбачає законодавець?

27. Розмежуйте зняття інформації з електронних інформаційних систем та тимчасовий доступ до відомостей, що у них містяться.

28. Чи допускається проведення описаних у розділі НСРД у кримінальних провадженнях щодо кримінальних проступків?

29. Чи допускається проведення описаних у розділі НСРД до внесення відомостей до ЄРДР?

30. Якими ще слідчими (розшуковими) чи іншими процесуальними діями можна одержати електронні докази?

Рекомендована література

1. *Багрій М. В., Луцик В. В.* Негласні слідчі (розшукові) дії у кримінальному провадженні : монографія. Тернопіль, 2014. 308 с.

2. *Багрій М. В., Луцик В. В.* Процесуальні аспекти негласного отримання інформації : вітчизняний та зарубіжний досвід : монографія. Харків : Право, 2017. 376 с.

3. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навчально-практичний посібник / Б. І. Бараненко, О. В. Бочковий, К. А. Гусєва та ін. ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

4. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

5. *Марущак А. І.* Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104–110.

6. Негласні слідчі (розшукові дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні : навч.-практ. посібник [Текст] / Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Харків : Оберіг, 2015. 424 с.

7. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рекомендації / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

8. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рекомендації / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

9. *Тагієв С. Р.* Негласні слідчі (розшукові) дії у кримінальному судочинстві України : монографія [Текст]. Київ : ВД «Дакор», 2015. 440 с.

10. *Тарасюк А. В.* Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. 192 с.

11. *Cascavilla G., Tamburri D. A., Van Den Heuvel W.-J.* Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & security. 2021. Vol. 105. P.102258.

12. *Edwards G.* Cybercrimes Investigators Handbook. Hoboken, New Jersey : John Wiley & Sons, Incorporated. 2020. 297 p.

13. *Tropina T., Callanan C*. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing AG Switzerland, 2015.

ДОДАТКИ

Додаток 1

ПЕРЕЛІК КАТЕГОРІЙ КІБЕРІНЦИДЕНТІВ[142]

1. Перелік категорій кіберінцидентів (далі – Перелік) розроблений з використанням та відповідає рекомендації Європейської агенції з кібербезпеки (ENISA Reference Incident Classification Taxonomy[143], січень 2018 року), а також спільному документу ENISA та Європейського центру боротьби з кіберзлочинністю Європолу (Common Taxonomy for Law Enforcement and The National Network of CSIRTs[144]).

2. Перелік призначений для впровадження єдиної таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

3. Перелік може застосовуватись суб'єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, наведених у цьому документі.

---

[142] Цей Перелік розроблений Державною службою спеціального зв'язку та захисту інформації України. URL : https://cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv.

[143] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[144] https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf

4. Перелік має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб'єктів забезпечення кібербезпеки.

5. Суб'єкти забезпечення кібербезпеки при обміні та поширенні інформації про кіберінциденти, підготовці звітів і публічних повідомлень про кіберінциденти застосовують Перелік.

6. Цей перелік є обов'язковим для основних суб'єктів забезпечення кібербезпеки при реєстрації, обліку та обміні інформацією про кіберінциденти, передачі звітів до НКЦК, зокрема із використанням автоматизованих платформ обміну інформацією про кіберзагрози.

7. У випадку, коли на початковій стадії реагування кіберінцидент може бути віднесений до декількох категорій, вибирається категорія із більшим рівнем загрози.

Код	**Категорія інциденту**	**Назва інциденту**	**Назва інциденту в MISP**
1	*2*	*3*	*4*
01.	Шкідливий (образливий) вміст (Abusive content)	Спам	Spam
		Образливий контент	Harmful Speech[145]
		Шкідливий контент	Child/Sexual/ Violence/...[146]

[145] Небажаний контент, у тому числі расистський чи ксенофобний матеріал, погрози особі чи групі осіб.

[146] Шкідливий контент, в тому числі дитяча порнографія, насильство, пропаганда.

1	*2*	*3*	*4*
02.	Шкідливий програмний код (Malicious Code)	Вірус	Virus
		Хробак	Worm
		Троян	Trojan
		Шпигунське програмне забезпечення	Spyware
		Діалер	Dialer
		Руткіт	Rootkit
		Шкідливе програмне забезпечення	Malware
		Управління ботами	Botnet drone
		Програма-здирник	Ransomware
		Конфігурація шкідливого програмного забезпечення	Malware configuration
		Командно-контрольний центр	C&C
03.	Збір інформації зловмисником (Information Gathering)	Сканування	Scanning
		Перехоплення і аналіз мережевого трафіку	Sniffing
		Соціальна інженерія	Social Engineering
04.	Спроби втручання (Intrusion Attempts)	Експлуатація відомих вразливостей	Exploiting of known Vulnerabilities[147]
		Спроби авторизації	Login attempts[148]
		Експлуатація раніше невідомих вразливостей	New attack signature (exploit)[149]

[147] Спроба компрометації чи пошкодження функціонування системи або сервісу шляхом експлуатації вразливостей, які мають стандартизований ідентифікатор (наприклад, CVE).

[148] Численні спроби авторизації: підбір паролів, злам паролів і т. п.

[149] Використання раніше невідомих вразливостей і експлойтів.

1	*2*	*3*	*4*
05.	Втручання (Intrusion)	Компрометація привілейованого облікового запису	Privileged Account Compromise
		Компрометація непривілейованого облікового запису	Unprivileged account compromise
		Компрометація застосунку	Application compromise
		Бот	Bot
		Дефейс	Defacement
		Компрометація системи	Compromised
		Бекдор	Backdoor
06.	Порушення доступності (Availability)	Атака на відмову в обслуговуванні	DoS
		Розподілена атака на відмову в обслуговуванні	DDoS
		Саботаж, диверсія	Sabotage
		Збій без участі зловмисника	Outage, no malice
07.	Порушення властивостей інформації (Information Content Security)	Несанкціонований доступ до інформації	Unauthorised access to information
		Несанкціоноване внесення змін до інформації	Unauthorised modification of information
		Сервер з публічними правами на запис	Dropzone[150]

[150] Зловмисники використовують сервери з правами на запис для тимчасового збереження викраденої із скомпрометованих систем інформації, в тому числі даних кейлогерів, скомпрометованих облікових даних і т. ін.

1	*2*	*3*	*4*
08.	Шахрайство (Fraud)	Несанкціоноване використання ресурсів	Unauthorized use of resources
		Порушення авторських прав	Copyright
		Маскарадинг	Masquerade[151]
		Фішинг	Phishing
09.	Відома вразливість (Vulnerable)	Вразливості, відкриті для експлуатації	Open for abuse
10.	Інше (Other)	Чорний список	Blacklist
		Недостатньо даних	Unknown
		Інше	Other[152]

[151] Використання копії ідентифікаторів суб'єкта або системи, в тому числі крадіжка особистості.

[152] Інциденти, які не відносяться до будь-якої з вищезазначених категорій.

Додаток 2

Керівні принципи Комітету міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях

(Прийняті Комітетом Міністрів 30 січня 2019
на 1335-му засіданні заступників Міністрів)

Комітет Міністрів,

Беручи до уваги, що метою Ради Європи є досягнення більшої єдності між державами-членами, зокрема шляхом сприяння прийняттю спільних правил у правових питаннях;

Враховуючи необхідність надання практичних рекомендацій щодо обробки електронних доказів у цивільних та адміністративних справах судам та іншим компетентним органам, які виконують судові функції; фахівцям, у тому числі практикуючим юристам, і сторонам у судовому процесі;

Беручи до уваги, що метою цих керівних принципів є забезпечення спільної основи, а не гармонізація національного законодавства держав-членів;

Враховуючи необхідність поважати різноманітність у правових системах держав-членів;

Визнаючи прогрес, досягнутий державами-членами стосовно оцифровування своїх систем правосуддя;

Відзначаючи, однак, перешкоди для ефективного управління електронними доказами в системах правосуддя, таких як відсутність єдиних стандартів і різноманітність та складність процедур збору доказів;

Підкреслюючи необхідність сприяти використанню електронних доказів у правових системах та у судовій практиці;

Визнаючи необхідність вивчення державами-членами сучасних недоліків у використанні електронних доказів та

визначення сфер, де можна було б запровадити чи покращити принципи та практику використання електронних доказів;

Відзначаючи, що метою цих керівних принципів є надання практичних рішень існуючим недолікам у законодавстві та на практиці,

Приймає ці керівні принципи, які слугуватимуть практичним інструментом для держав-членів, допомагатимуть їм адаптувати функціонування своїх судових та інших механізмів врегулювання спорів для вирішення питань, що виникають у зв'язку з електронними доказами у цивільних та адміністративних провадженнях, і запрошує їх широко розповсюджувати ці керівні принципи з метою їх імплементації відповідальними чи іншими зацікавленими особами.

Мета і сфера застосування

Керівні принципи стосуються:

- усних свідчень, отриманих засобами дистанційного зв'язку;
- використання електронних доказів;
- збору, вилучення та передачі доказів;
- доречності;
- достовірності;
- зберігання та збереження;
- архівування;
- підвищення обізнаності, розгляд, навчання та освіта.

Керівні принципи не повинні тлумачитися як такі, що передбачають певну доказову цінність для певних типів електронних доказів і повинні застосовуватися лише тією мірою, в якій вони не суперечать національному законодавству.

Ці керівні принципи спрямовані на полегшення використання та управління електронними доказами в правових системах і в судовій практиці.

Визначення

Для цілей цих керівних принципів:

Електронні докази

«Електронні докази» – будь-які докази, що містяться, або виробляються будь-яким пристроєм, функціонування якого залежить від програмного забезпечення або даних, що зберігаються або передаються через комп'ютерну систему або мережу.

Метадані

Термін «Метадані» стосується електронної інформації про інші електронні дані, які можуть виявити ідентифікацію, походження або історію доказів, а також відповідні дати і час.

Електронні довірчі послуги

«Електронні довірчі послуги» – електронна послуга, яка складається зі:

a. створення, верифікації та підтвердження електронних підписів, електронних печаток чи електронних відміток, електронних зареєстрованих служб доставки та сертифікатів, пов'язаних із цими послугами; або

b. створення, верифікації, та підтвердження сертифікатів для аутентифікації вебсайтів; або

c. збереження електронних підписів, печаток або сертифікатів, пов'язаних із цими послугами.

Суд

Термін «суд» охоплює будь-який компетентний орган, який виконує судові функції, при виконанні яких він використовує електронні докази.

Базові принципи

Питання вирішення потенційної доказової цінності електронних доказів належить судам відповідно до національного законодавства.

Електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема стосовно допустимості, достовірності, точності та цілісності.

Опрацювання електронних доказів не повинно бути невигідним для сторін або надавати несправедливу перевагу одній із них.

Керівні принципи

Усні свідчення, отримані засобами дистанційного зв'язку.

1. Усні свідчення можуть бути отримані дистанційно, використовуючи технічні пристрої, якщо характер доказів це дозволяє.

2. При вирішенні питання, чи можуть усні свідчення бути прийняті дистанційно, суди повинні розглянути, зокрема, такі фактори:

– значущість свідчення;
– статус особи, яка дає свідчення;
– безпека та цілісність відеозв'язку, через який мають передаватися свідчення;
– витрати та труднощі доставлення відповідної особи до суду.

3. При дистанційному прийнятті доказів необхідно забезпечити таке:

a. передача усних свідчень може бути побачена та почута особами, які беруть участь у провадженні, та представниками громадськості, якщо провадження проводиться публічно; і

b. особа, яка дистанційно була заслухана, може бачити та чути провадження, за необхідності для забезпечення справедливості та ефективності.

4. Процедура та технології, які застосовуються для отримання свідчень дистанційно, не повинні ставити під загрозу прийнятність таких доказів та здатність суду встановити особистість заінтересованих осіб.

5. Незалежно від того, чи передаються свідчення шляхом стаціонарного чи мобільного зв'язку, варто забезпечити належну якість відеоконференції та зашифрувати відеосигнал для захисту від перехоплення.

Використання електронних доказів

6. Суди не повинні відмовлятися від електронних доказів і не повинні заперечувати їх юридичну силу лише тому, що вони збираються та/або подаються в електронному вигляді.

7. В цілому, суди не повинні заперечувати юридичну силу електронних доказів винятково через те, що вони не мають розширеного, кваліфікованого або аналогічно забезпеченого електронного підпису.

8. Суди повинні розуміти доказову цінність метаданих та потенційні наслідки їх невикористання.

9. Сторонам має бути дозволено подавати електронні докази у вихідному електронному форматі без необхідності надавати роздруківки.

Збір, вилучення та передача доказів

10. Електронні докази повинні бути зібрані у належний та безпечний спосіб і подані до судів з використанням надійних послуг, таких як електронні довірчі послуги.

11. Беручи до уваги більш високий ризик потенційного знищення або втрати електронних доказів порівняно з неелектронними доказами, держави-члени повинні встановити процедури для безпечного вилучення та збору електронних доказів.

12. Суди повинні бути обізнані про окремі питання, які виникають при розгляді питання про арешт та збір електронних доказів за кордоном, у тому числі у транскордонних справах.

13. Суди повинні співпрацювати при транскордонному отриманні доказів. Суд, який отримав запит, повинен повідомити запитуючий суд про всі умови, включаючи обмеження, згідно з якими доказ може бути прийнятий запитуваним судом.

14. Збирання, структурування й управління електронними доказами має відбуватися таким способом, щоб полегшити їх передачу іншим судам, зокрема, апеляційному суду.

15. Передачу електронних доказів електронними засобами варто заохочувати і полегшувати з метою підвищення ефективності судового розгляду.

16. Системи і пристрої, що використовуються для передачі електронних доказів мають бути здатні зберігати їх цілісність.

Доречність

17. Суди повинні брати участь в активному управлінні електронними доказами з метою, зокрема, уникнення надмірного або спекулятивного надання, чи вимоги надання електронних доказів.

18. Суди можуть вимагати проведення експертами аналізу електронних доказів, особливо коли виникають складні доказові питання або коли йдеться про маніпулювання електронними доказами. Суди мають вирішувати, чи мають такі особи достатній досвід у цьому питанні.

Надійність

19. Стосовно надійності, суди повинні враховувати всі відповідні фактори відносно джерела та достовірності електронних доказів.

20. Суди мають бути обізнані щодо цінності електронних довірчих послуг у встановленні надійності електронних доказів.

21. Якщо це не суперечить нормам національної правової системи, і за винятком рішення суду, електронні дані повинні бути прийняті як докази, якщо справжність таких даних не оскаржується однією зі сторін.

22. Якщо це не суперечить нормам Національної правової системи, і підпадає під дію рішень суду, повинна бути передбачена надійність електронних даних, за умови, що особа підписувача може бути підтверджена, а цілісність даних забезпечена, якщо і поки не буде обґрунтованих сумнівів у протилежному.

23. Якщо чинне законодавство передбачає спеціальний захист для вразливих категорій осіб, закон повинен мати пріоритет над цими керівними принципами.

24. Якщо це не суперечить нормам Національної правової системи, електронні докази, які державний орган передає незалежно від сторін, є переконливим щодо їх змісту, у випадку недоведення протилежного.

Зберігання та збереження

25. Зрозумілість, доступність, цілісність, автентичність, надійність і, у разі необхідності, конфіденційність і приватність, мають бути складовими електронних доказів під час їх збереження.

26. Електронні докази повинні зберігатися зі стандартизованими метаданими, аби контекст їх створення був зрозумілим.

27. Зрозумілість і доступність збережених електронних доказів повинні гарантуватися з плином часу, враховуючи еволюції інформаційних технологій.

Архівування

28. Суди повинні архівувати електронні докази відповідно до національного законодавства. Електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватності.

29. Архівування електронних доказів мають здійснювати кваліфіковані фахівці.

30. Дані мають переписуватися на нові носії для зберігання, коли це необхідно для збереження доступності електронних доказів.

Підвищення обізнаності, огляд, навчання та освіта

31. Держави-члени повинні сприяти обізнаності про переваги та цінність електронних доказів у цивільних та адміністративних провадженнях.

32. Держави-члени повинні постійно відслідковувати технічні стандарти, пов'язані з електронними доказами.

33. Всі фахівці, що працюють з електронними доказами, повинні мати доступ до необхідного міждисциплінарного навчання щодо обробки таких доказів.

34. Судді та практикуючі юристи повинні бути обізнані про розвиток інформаційних технологій, які можуть вплинути на доступність та цінність електронних доказів.

35. Юридична освіта має включати здачу модулів щодо електронних доказів.

Додаток 3

Рекомендації щодо ідентифікації, збирання, здобуття та збереження електронних (цифрових) доказів, викладені в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»

Відповідно до наказу Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 6 грудня 2017 року № 400 «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів» з 1 січня 2019 року в Україні набрав чинності державний стандарт ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів».

Цей стандарт був прийнятий з метою гармонізації національної нормативної бази з міжнародним законодавством і розроблений методом перекладу тексту з відповідного міжнародного стандарту ISO/IEC 27037:2012 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence», що був прийнятий спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) ще у 2012 році.

Рекомендації, що викладені в стандарті, стосуються специфічної діяльності з оброблення потенційних цифрових доказів, а саме процесів: ідентифікації, збирання, здобуття та збереження цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка

буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях.

Але запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Тому в стандарті зазначається, що для підтримання цілісності цифрових доказів користувачам цього документу потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних національних законодавчих вимог.

Стандарт також може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями різних держав.

Представлений надалі текст стандарту не є його офіційним виданням.

1. СФЕРА ЗАСТОСУВАННЯ

Цей стандарт надає настанови для специфічної діяльності з оброблення цифрових доказів, а саме: ідентифікації, збирання, здобуття та збереження цифрових доказів, що можуть мати доказове значення. Цей стандарт надає настанови для фахівців стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів, та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями.

Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин:

- Носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функціями;
- Мобільні телефони, Персональні цифрові помічники (PDAs), Персональні електронні прилади (PEDs), карти пам'яті;

- Мобільні навігаційні системи;
- Цифрові фото- та відеокамери (зокрема CCTV);
- Стандартний комп'ютер з мережевими з'єднаннями;
- Мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах, а також
- Прилади з функціями, подібними до наведених вище.

Примітка 1. Наведений вище перелік приладів надано для інформації і він не є вичерпним.

Примітка 2. Наведені вище пристрої може бути запроваджено в різні способи. Наприклад, автоматизована система може містити мобільну навігаційну систему, збереження даних та сенсорну систему.

2. НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче документи потрібні для застосування цього стандарту. У разі датованих посилань застосовують тільки наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

ISO/TR 15801 Document management – Information stored electronically – Recommendations for trustworthiness and reliability (Керування документами. Інформація, що зберігається в електронному вигляді. Рекомендації стосовно справжності та надійності);

ISO/IEC 17020 Conformity assessment – Requirements for the operation of various types of bodies performing inspection (Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування);

ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary (Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд та словник).

3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни та визначення позначених ними понять згідно з ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 та ISO/TR 15801, а також наведені нижче.

3.1. Здобуття *(acquisition).*

Процес створення копії даних у межах визначеного набору.

Примітка. Результатом здобуття є копія потенційних цифрових доказів.

3.2. Виділений простір *(allocated space).*

Ділянка цифрового середовища, охоплюючи первинну пам'ять, використовувану для збереження даних, охоплюючи метадані.

3.3. Збирання *(collection).*

Процес складання фізичних об'єктів, які містять потенційні цифрові докази.

3.4. Цифровий пристрій *(digital device).*

Електронне устаткування, використовуване для оброблення чи збереження даних.

3.5. Цифровий доказ *(digital evidence).*

Інформація або дані, збережені або передані в бінарному вигляді, на які можна покладатися як на докази.

3.6. Копія цифрового доказу *(digital evidence copy).*

Копія цифрового доказу, запроваджено для підтримання надійності доказу за допомогою вміщення разом цифрового доказу та засобів верифікації, де спосіб верифікації може бути вбудованим або незалежним від інструментів, використовуваних під час верифікації.

3.7. Перший відповідальний за цифровий доказ; DEFR *(Digital Evidence First Responder).*

Авторизована особа, яка пройшла навчання та кваліфікована для того, щоб діяти першою під час розслідування інциденту, здійснюючи збирання та здобуття цифрових доказів, із відповідальністю для оброблення цього інциденту.

Примітка. Повноваження, навчання та кваліфікація є обов'язковими вимогами, необхідними для здобуття надійних цифрових доказів, але індивідуальні обставини можуть призвести до того, що особа не відповідає всім трьом вимогам. У такому разі потрібно розглянути локальні закони, організаційну політику та індивідуальні обставини.

3.8. Спеціаліст з цифрових доказів; DES *(Digital Evidence Specialist).*

Особа, яка може виконувати завдання DEFR та має спеціалізовані знання, навички та здатна поводитися з широким діапазоном технічних питань.

Примітка. DES може мати навички в додаткових сферах, наприклад, здобуття з мережі, здобуття з RAM, знання програмного забезпечення операційних систем або Mainframe.

3.9. Носій для збереження цифрових даних *(digital storage medium).*

Пристрій, на якому можуть бути записані цифрові дані.

[Адаптовано з ISO/IEC 10027:1990].

3.10. Пристрій для збереження доказів (evidence preservation facility).

Безпечне середовище або місце, де зберігають докази, зібрані чи здобуті.

Примітка. Пристрій для збереження доказів не повинен піддаватися впливу магнітних полів, пилу, вібраціям, вогкості чи будь-яких інших елементів навколишнього середовища (таких як екстремальні температури або вологість), які можуть пошкодити потенційні цифрові докази всередині пристрою.

3.11. Геш-значення *(hash value).*
Рядок бітів, яка є виходом геш-функції.

3.12. Ідентифікація (identi*fi*cation).
Процес, який охоплює пошук, розпізнавання та документування потенційних цифрових доказів.

3.13. Утворення образу *(imaging).*
Процес створення порозрядної копії носія для збереження цифрових даних.
Примітка. Порозрядна копія також має назву фізичної копії.
Приклад: Під час створення образу жорсткого диска DEFR буде також копіювати вилучені дані.

3.14. Периферія *(peripheral).*
Прилад, під'єднаний до цифрового приладу для розширення його функціональності.

3.15. Збереження *(preservation).*
Процес для підтримання та убезпечування цілісності та/або оригінальних умов потенційних цифрових доказів.

3.16. Надійність *(reliability).*
Властивість логічно передбачуваних поведінки та результатів.
[ISO/IEC 27000:2009].

3.17. Збіжність *(repeatability).*
Властивість керованого процесу отримувати однакові тестові результати в однаковому тестовому середовищі (однаковий комп'ютер, жорсткий диск, режим операції тощо).

3.18. Відтворюваність *(reproducibility).*
Властивість процесу отримувати однакові тестові результаті

в різному тестовому середовищі (різні комп'ютери, жорсткий диск, режим роботи тощо).

3.19. Псування *(spoliation).*

Дія зі здійсненням або допущенням внесення змін(и) до потенційних цифрових доказів, яка зменшує їхнє доказове значення.

3.20. Системний час *(system time).*

Час, генерований системним годинником за допомогою операційної системи; це не час, обчислюваний операційною системою.

3.21. Втручання *(tampering).*

Дія з навмисного виконання або допущення внесення змін(и) до цифрового доказу (тобто, умисне або цілеспрямоване псування).

3.22. Часовий штемпель *(timestamp).*

Різні параметри часу, які визначають точку в часі відносно до загальної довідкової інформації про час.

[ISO/IEC 11770-1:1996].

3.23. Невиділений простір *(unallocated space).*

Простір у цифровому середовищі, охоплюючи первинну пам'ять, який не був локалізованим за допомогою операційної системи та придатний для збереження даних, охоплюючи метадані.

3.24. Затвердження *(validation).*

Підтвердження за допомогою об'єктивних доказів, що вимоги для специфічного призначеного використання або застосування виконано.

[ISO/IEC 27004:2009].

3.25. Функція верифікації (*verification function*).

Функція, використовувана для підтвердження, що два набори даних – ідентичні.

Примітка 1. Два неідентичні набори даних не потрібно вважати ідентичними після функції верифікації.

Примітка 2. Функції верифікації зазвичай застосовують з використанням геш-функцій, таких як MD5, SHA1 тощо, але може бути використано інші методи.

3.26. Нестійкі дані *(volatile data).*

Дані, специфічно схильні до змін та які може бути легко модифіковано.

Примітка. Зміни може бути зумовлено виключенням живлення або переходом крізь магнітне поле. Нестійкі дані також охоплюють дані, які змінюються, коли стан системи змінюється. Прикладами можуть бути дані, збережені в RAM та динамічні IP-адреси.

4. ПОЗНАЧКИ ТА СКОРОЧЕННЯ

AVI (Audio Video Interleave) – Чергування аудіо та відео; CCTV (Closed Circuit Television) – Відеоспостереження; CD (Compact Disk) – Компакт-диск;

DNA (Deoxyribonucleic Acid) – Дезоксирибонуклеїнова кислота (ДНК);

DEFR (Digital Evidence First Responder) – Перший відповідальний за цифровий доказ;

DES (Digital Evidence Specialist) – Спеціаліст із цифрових доказів;

DVD (Digital Video/Versatile Disk) – Цифровий відео/універсальний диск;

ESN (Electronic Serial Number) – Електронний серійний номер;

GPS (Global Positioning System) – Глобальна система визначення місцеположення;

GSM (Global System for Mobile Communication) – Глобальна система мобільного зв'язку;

IMEI (International Mobile Equipment Identity) – Міжнародний ідентифікатор мобільного обладнання;

IP (Internet Protocol) – Інтернет-протокол;

ISIRT (Information Security Incident Response Team) – Команда реагування на інциденти інформаційної безпеки;

LAN (Local Area Network) – Локальна мережа;

MD5 (Message-Digest Algorithm 5) – Алгоритм перетворення повідомлення 5;

MP3 (MPEG Audio Layer 3) – MPEG аудіо рівень 3;

MPEG (Moving Picture Expert Group) – Група експертів з питань кіно;

NAS (Network Attached Storage) – Мережа пристроїв для збереження даних;

PDA (Personal Digital Assistant) – Персональний цифровий помічник;

PED (Personal Electronic Device) – Персональний електронний прилад;

PIN (Personal Identification Number) – Персональний ідентифікаційний номер;

PUK (PIN Unlock Key) – Ключ розблокування PIN;

RAID (Redundant Array of Independent Disks) – Надлишковий масив незалежних дисків;

RAM (Random Access Memory) – Оперативна пам'ять для тимчасового збереження даних з випадковим доступом;

RFID (Radio Frequency Identification) – Ідентифікація радіочастот;

SAN (Storage Area Network) – Мережа сховищ;

SHA (Secure Hash Algorithm) – Безпечний геш-алгоритм;

SIM (Subscriber Identity Module) – Модуль ідентифікації абонента;

USB (Universal Serial Bus) – Універсальна послідовна шина;

UPS (Uninterruptible Power Supply) – Безперебійне джерело живлення;

USIM (Universal Subscriber Identity Module) – Універсальний модуль ідентифікації абонента;

UV (Ultraviolet) – Ультрафіолет;
Wi-Fi (Wireless Fidelity) – Бездротова передача інформації.

5. ЗАГАЛЬНИЙ ОГЛЯД

5.1. Обставини для збирання цифрових доказів

Цифрові докази можуть бути потрібними для використання в низці окремих сценаріїв, кожен із яких має різний баланс між рушієм доказової якості, своєчасністю аналізування, відновлюванням послуги та вартістю збирання цифрових доказів. Тому організаціям потрібно буде запровадити процес визначення пріоритетів, який ідентифікує потреби та баланс доказової якості, своєчасності та відновлення послуг до того, як буде надано завдання ресурсам DEFR. Процес визначення пріоритетів охоплює виконання оцінювання матеріалів, доступних для визначення можливого доказового значення, та порядок, у якому потенційні цифрові докази потрібно збирати, здобувати чи зберігати. Процес визначення пріоритетів відбувається задля мінімізації ризику, що потенційні цифрові докази будуть псуватися, та доведення до максимуму доказового значення зібраних потенційних цифрових доказів.

5.2. Принципи цифрових доказів

У більшості юрисдикцій та організацій цифрові докази ґрунтуються на трьох основних принципах: важливість, надійність та достатність. Ці три принципи є важливими в усіх розслідуваннях, але не тільки такі цифрові докази прийнятні в суді. Цифровий доказ є надійним, якщо він надає можливість засвідчувати або не засвідчувати елемент розслідуваного специфічного випадку. Хоча детальні визначення «надійність» відрізняються в різних юрисдикціях, основне значення цього принципу «гарантувати, що цифровий доказ є таким, яким він має бути» широко вживають. Не завжди потрібно для DEFR збирати всі дані або робити повну копію первісного цифрового доказу. У більшості юрисдикцій концепція достатності означає,

що DEFR повинен зібрати достатню кількість потенційних цифрових доказів, щоб забезпечити можливість відповідного перевірення та дослідження елементів справи. Розуміння цієї концепції є важливим для DEFR для визначення пріоритетів зусиль правильно, якщо це стосується часу або вартості.

Примітка. DEFR повинен гарантувати, що збирання потенційних цифрових доказів відповідає локальному законодавству та нормативним документам, як це потрібно для специфічних обставин.

Усі процеси, використовувані DEFR та DES, мають бути затвердженими до їхнього використання. Якщо затвердження зроблено в екстремальних умовах, DEFR та DES мають підтвердити, що затвердження є прийнятним для їхнього специфічного використання процесів та середовища й обставин, у яких ці процеси будуть використані. DEFR та DES мають також:

a) документувати всі дії;
b) визначати та застосовувати метод для оцінювання точності та надійності копій потенційних цифрових доказів відносно первісного джерела; а також
c) зазначити, що дія збереження потенційних цифрових доказів не може завжди бути без наявності втручання.

5.3. Вимоги щодо оброблення цифрових доказів

5.3.1. Загальні положення

Принципи, наведені вище в 5.2, можна задовольнити так:

– Важливість: Є змога показати, що здобуті матеріали є надійними для розслідування, тобто, що вони містять величини, які допомагають у розслідуванні конкретного інциденту, та що є доречна причина для їхнього здобуття. За допомогою аудиту та юрисдикції DEFR повинен мати змогу описати підтримані процедури та пояснити, як було прийнято рішення для здобуття кожного елемента.
– Надійність: Усі процеси, використані під час оброблення потенційних цифрових доказів, потрібно піддавати аудиту та вони мають бути збіжними.

– Достатність: DEFR повинен ураховувати, що достатню кількість матеріалів має бути зібрано, щоб дозволити зробити належні дослідження. DEFR повинен мати змогу з використанням аудиту та законодавства надати пояснення, яку кількість матеріалу, загалом, розглянуто та які процедури використано для вирішення питання, яку кількість та який матеріал здобуто.

Примітка. Матеріали має бути зібрано за допомогою дій зі здобуття та збирання.

Є чотири ключові аспекти в обробленні цифрових доказів: можливість аудиту, відповідність юрисдикції та збіжність або відтворюваність залежно від конкретних обставин.

5.3.2. Можливість аудиту

Незалежні аудитори або інші зацікавлені сторони повинні мати змогу оцінювати діяльність DEFR та DES. Це буде можливим за допомогою документування всіх запроваджених дій. DEFR та DES повинні мати змогу доказу законності процесу прийняття рішення у виборі такого плану дій. DEFR та DES мають бути доступними для незалежного оцінювання для визначення, чи запроваджено відповідні наукові методи, методики та процедури.

5.3.3. Збіжність

Збіжності досягають, якщо ті самі результати отримують за таких умов:

– Використання такої самої процедури та методики;
– Використання таких самих інструментів та за таких самих умов; а також
– Може бути повторено в будь-який час після первісного тесту.

DEFR з належними навичками та досвідом повинен мати змогу починати всі процеси, описані в документації, та отримувати такі самі результати без настанови або інтерпретації. DEFR повинен бути обізнаним, що можуть бути обставини, коли тест не може бути повторено, наприклад, якщо первісний жорсткий диск було скопійовано та повернуто в експлуатацію, або коли об'єкт має

нестійку пам'ять. У цьому разі DEFR повинен гарантувати, що процес здобуття є надійним. Для досягнення збіжності мають бути контроль якості та документація.

5.3.4. Відтворюваність

Відтворюваності досягають, якщо ті самі результати тесту отримують за таких умов:

- Використання такої самої методики вимірювання;
- Використання інших інструментів та за інших умов;
- Може бути відтворено в будь-який час після первісного тесту.

Потреба у відтворюванні результатів змінюється залежно від юрисдикції та обставин, тому DEFR чи особа, яка здійснює відтворювання, має бути поінформованою стосовно прийнятних умов.

5.3.5. Відповідність юрисдикції

DEFR повинен мати змогу доказати відповідність юрисдикції усіх дій та методів, застосованих під час оброблення потенційних цифрових доказів. Відповідності юрисдикції може бути досягнуто демонстрацією того, що такі рішення є найкращим вибором для отримання всіх потенційних цифрових доказів. Інші DEFR або DES можуть також показати це за допомогою успішного відтворювання або затвердження дій та використовуваних методів.

В інтересах конкретної організації наймати DEFR або DES, які мають основні навички та компетенцію, як описано в додатку А цього стандарту. Це буде гарантувати, що під час оброблення потенційних цифрових доказів буде застосовано правильні процеси та процедури для забезпечення кінцевого збереження цифрових доказів, які можуть мати доказове значення. Це також гарантує, що організація матиме змогу використання потенційних цифрових доказів, наприклад, у своїх дисциплінарних процедурах або сприяти обміну потенційними цифровими доказами між юрисдикціями.

Примітка. Компетентність, описану в додатку А, обмежено функціями DEFR, що сумісна з роллю DES, як визначено в 3.8.

5.4. Процеси оброблення цифрових доказів

5.4.1. Загальні питання

Хоча повний процес оброблення цифрових доказів охоплює інші діяльності (наприклад, представлення, контроль тощо), сфера застосування в цьому стандарті охоплює тільки початковий процес оброблення, який складається з ідентифікації, збирання, здобуття та збереження потенційних цифрових доказів.

Цифрові докази можуть бути нестійкими за природою. Вони можуть змінюватися, псуватися або руйнуватися під час неправильного оброблення або перевірення. Обробники цифрових доказів мають бути компетентними стосовно ідентифікації та керування ризиками і послідовності потенційних напрямів дій, якщо мають справу із цифровими доказами. Неправильна робота цифрових пристроїв для оброблення може зробити потенційні цифрові докази, яка містять ці прилади, непридатними.

DEFR та DES повинні підтримувати задокументовані процедури для гарантування цілісності та надійності потенційних цифрових доказів. Ці процедури мають містити настанови щодо оброблення джерел потенційних цифрових доказів та ґрунтуватися на таких фундаментальних принципах:

- Мінімізування оброблення первісних цифрових пристроїв або потенційних цифрових доказів;
- Пояснення будь-яких змін та документування запроваджених дій (щоб експерт мав змогу сформувати висновок щодо надійності);
- Відповідність локальним правилам стосовно доказів; та
- DEFR та DES не повинні виконувати дій поза межами їхньої компетентності.

Потенційні цифрові докази мають зберігатися відповідно до цих фундаментальних принципів та вимог оброблення потенційних цифрових доказів. Усі дії та пояснення потрібно задокументовувати, особливо у випадках, якщо може бути внесено невідворотні зміни.

Кожен процес оброблення цифрових доказів, тобто ідентифікація, збирання, здобуття та збереження докладно описано в наступних розділах.

5.4.2. Ідентифікація

Цифрові докази наведено у фізичній та логічній формах. Фізична форма вміщує презентацію даних усередині реального приладу. Логічна форма потенційних цифрових доказів належить до віртуальної презентації даних усередині приладу.

Процес ідентифікації вміщує пошук, розпізнавання та документування потенційного цифрового доказу. Процес ідентифікації має ідентифікувати носій для збереження цифрових даних та пристрої для оброблення, які можуть містити потенційні цифрові докази, що стосуються інциденту. Цей процес також містить діяльність щодо визначення пріоритетів збирання доказів, який ґрунтується на їхній несталості. Цю несталість даних має бути ідентифікованою для гарантування процесів правильного збирання та здобуття даних для мінімізації пошкодження потенційних цифрових доказів та отримання найкращих доказів.

Додатково, процес має ідентифікувати ймовірність наявності прихованих потенційних цифрових доказів. DEFR та DES повинні бути обізнаними, що не всі типи носіїв для збереження цифрових даних може бути легко ідентифіковано та визначено їхнє місце розташування, наприклад, хмарні обчислювання, NAS та SAN – це додає віртуальні компоненти в процес ідентифікації.

DEFR повинен систематично здійснювати ретельний пошук елементів, які можуть містити потенційні цифрові докази. Різні типи цифрових пристроїв, які можуть містити потенційні цифрові докази, можуть бути легко пропущені (наприклад, через малий розмір), піддані сумніву або змішані з іншими матеріалами, що не стосуються справи.

Пункти 6.1 та 6.6 надають більше інформації стосовно послідовності аспектів охорони, пакування та позначення в процесі ідентифікації цифрових доказів. Розділ 7 визначає

настанови, які стосуються специфічних моментів ідентифікації, збирання, здобуття та збереження цифрових доказів.

5.4.3. Збирання

Якщо цифрові пристрої, які можуть містити потенційні цифрові докази, ідентифіковано, DEFR та DES повинні прийняти рішення щодо застосування збирання чи здобуття як наступних процесів. Є низка рішень, які на це впливають, докладніше розглянутих у розділі 7. Це рішення має ґрунтуватися на конкретних обставинах.

Збирання – це процес у процесі оброблення цифрових доказів, де пристрої, які можуть містити потенційні цифрові докази, переносяться з їхнього первісного місця розташування до лабораторії або іншого контрольованого середовища для подальшого здобуття потенційних цифрових доказів та аналізування. Пристрої, які містять потенційні цифрові докази, можуть перебувати в одному з двох станів: коли систему ввімкнено або коли систему вимкнено. Залежно від стану приладу потрібні різні підходи та інструменти. Локальні процедури можуть застосовувати підходи та інструменти, використовувані для процесу збирання.

Цей процес вміщує документування підходу в цілому, а також пакування цих приладів перед транспортуванням. Для DEFR та DES важливо зібрати будь-які матеріали, які можуть бути пов'язаними з потенційною цифровою інформацією (наприклад, папір із записаними паролями, шинами та коннекторами живлення для підключених системних приладів). Якщо не буде застосовано належну обережність, потенційні цифрові докази можуть бути втраченими або пошкодженими. DEFR та DES повинні визначити кращі з можливих методів, ґрунтуючись на конкретній ситуації, вартості й часі, та задокументувати це рішення використання специфічного методу.

Примітка 1. Перенесення носія для збереження цифрових даних не завжди рекомендовано та DEFR повинен бути впевненим, що вони мають компетенцію для перенесення носія для збереження

цифрових даних, та усвідомлювати, коли це доречно та дозволено робити.

Примітка 2. Деталі стосовно незібраних цифрових пристроїв має бути задокументовано відповідно до застосовуваної юрисдикції, та відповідно до вимог цієї юрисдикції.

5.4.4. Здобуття

Процес здобуття вміщує створення копії цифрових доказів (наприклад, повного жорсткого диска, його частини, вибраних файлів) та документування використовуваних методів і застосованих дій. DEFR повинен визначити належний метод здобуття, ґрунтуючись на конкретній ситуації, вартості і часі, та задокументувати це рішення використання специфічного методу або інструментів.

Методи, використовувані для здобуття потенційних цифрових доказів, мають бути докладно задокументованими та, якщо це можливо, бути відтворюваними або мати змогу перевірення компетентним DEFR. DEFR або DES повинні здобувати потенційні цифрові докази так, щоб максимально зменшити втручання, де це можливо, щоб запобігти змінам, які може бути внесено. Для застосування цього процесу DEFR повинен розглянути найбільш належний метод для використання. Якщо цей процес призведе до невідворотних змін у цифрових даних, усі виконані дії, має бути задокументовано для врахування змін у даних.

Запроваджуваний метод має забезпечити копіювання цифрових доказів з потенційних цифрових доказів або цифрового пристрою, який може містити потенційні цифрові докази. Як первісне джерело, так і копія потенційного цифрового доказу мають бути підтверджені засвідченою функцією верифікації (засвідчується точність у цей момент часу), що є прийнятною для особи, яка буде використовувати цей доказ. Первісне джерело та кожна копія цифрового доказу має давати такий самий результат функції верифікації.

Процес верифікації не може бути зроблено за деяких обставин, наприклад, під час здобуття потенційних цифрових

доказів з працюючої системи, якщо первісна копія містить помилкові сектори, або період часу здобуття є обмеженим. У таких випадках DEFR повинен використовувати найкращі можливі доступні методи та мати змогу підтвердити й захистити вибір цього методу. Якщо утворення образу не може бути підтвердженим, тоді це необхідно задокументувати та підтвердити. Якщо потрібно, запроваджуваний метод повинен мати змогу отримання локалізованого та нелокалізованого простору.

Примітка 1. Якщо не може бути застосовано процес підтвердження для всього джерела через помилки на джерелі, може бути використано ті частини джерела, які може бути надійно прочитано.

Можуть виникнути ситуації, у яких неможливо чи не дозволено створити копію цифрового доказу, наприклад, якщо джерело є занадто великим. У таких випадках DEFR може здійснити логічне здобуття, ціллю якого будуть тільки специфічні типи даних, директорії чи окремі місця. В основному це застосовується на рівні файлів і сегментів. Під час логічного здобуття потенційних цифрових доказів можуть бути скопійовані активні файли та нефайлові структури виділеного простору; знищені файли та невиділений простір на носії для збереження цифрових даних можуть бути нескопійованими залежно від застосовуваного методу. Цей метод може бути корисним в інших ситуаціях, коли розглядувані критичні системи не може бути зупинено.

Примітка 2. Деякі юрисдикції можуть потребувати спеціального оброблення даних; наприклад, їхнє запечатування в присутності власника даних. Запечатування має бути зроблено відповідно до локальних вимог (законодавство та процедури).

5.4.5. Збереження

Потенційні цифрові докази має бути збережено для гарантування їхньої придатності в розслідуванні. Важливо захистити цілісність доказів. Процес збереження містить захист від втручання та псування потенційних цифрових доказів та цифрових приладів, які можуть містити потенційні

цифрові докази. Процес збереження має бути ініційованим та підтримуватися протягом процесів оброблення цифрових доказів, починаючи з ідентифікації цифрових приладів, які можуть містити потенційні цифрові докази.

У найкращому сценарії не повинно бути псування даних чи будь-яких метаданих, пов'язаних із ними (наприклад, дата та штампи часу). DEFR повинен мати змогу показати, що доказ не було модифіковано з моменту, коли його було зібрано чи здобуто, чи було зроблено логічні обґрунтування та дії було задокументовано, якщо було внесено невідворотні зміни.

Примітка. У деяких випадках потрібна конфіденційність потенційних цифрових доказів, або є вимоги бізнесу чи законодавчі вимоги (наприклад, приватність). Потенційні цифрові докази мають зберігатися так, щоб гарантувати конфіденційність даних.

6. КЛЮЧОВІ КОМПОНЕНТИ ІДЕНТИФІКАЦІЇ, ЗБИРАННЯ, ЗДОБУТТЯ ТА ЗБЕРЕЖЕННЯ ЦИФРОВИХ ДОКАЗІВ

6.1. Хронологічне документування

У будь-яких дослідженнях DEFR повинен мати змогу звітувати про всі здобуті дані та прилади в той час, коли вони знаходяться під захистом DEFR. Запис хронологічного документування є документом, який показує хронологію переміщень та оброблення потенційних цифрових доказів. Вона має охоплювати час від процесу збирання або здобуття. Зазвичай, її супроводжує простежування історії елемента від часу, коли його було ідентифіковано, зібрано або здобуто командою дослідників до поточного статусу та місця знаходження.

Запис хронологічного документування є документом чи набором пов'язаних документів, які деталізують хронологічне документування та записи, хто відповідав за оброблення потенційних цифрових доказі, або у вигляді цифрових даних, або в іншому форматі (як паперові нотатки). Ціллю підтримання записів хронологічного документування є змога ідентифікації

доступу та переміщення потенційних цифрових доказів у будь-якій точці часу. Самі записи хронологічного документування можуть містити більше ніж один документ, наприклад, для потенційних цифрових доказів має бути сучасний документ, у якому записано здобуття цифрових даних на конкретному пристрої, переміщення цього пристрою та документація, яка містить послідовні виписки або копії потенційних цифрових доказів для аналізування та інших цілей.

Записи хронологічного документування мають містити таку інформацію, щонайменше:

Унікальний ідентифікатор доказу;

- Хто мав доступ до доказу та час і місце, де це зроблено;
- Хто перевіряв доказ під час уведення в та виведення з обладнання збереження доказу та коли це було зроблено;
- Чому доказ було перевірено (в якому випадку та з якою ціллю) та відповідний дозвіл, якщо його було надано; та
- Будь-які невідворотні зміни в потенційних цифрових доказах, а також ім'я особи, відповідальної за це та юрисдикцію для внесення цих змін.

Хронологічне документування має бути підтримувано протягом усього часу життя доказів та зберігатися протягом визначеного періоду часу після завершення часу життя доказів – цей період часу може бути встановлено відповідно до локального законодавства збирання та застосування доказів. Його має бути встановлено від моменту, коли цифрові прилади та/або потенційні цифрові докази здобуто та не повинен змінюватися.

Примітка. Деякі юрисдикції можуть мати спеціальні вимоги стосовно хронологічного документування. DEFR повинен виконувати ці вимоги.

6.2. Застороги на місці інциденту

6.2.1. Загальні положення

DEFR повинен застосовувати дії для убезпечення та захисту місця знаходження потенційних цифрових доказів, якщо вони наставали в цьому місці. Ця діяльність має підтримувати таке, залежно від локальних законів:

- Убезпечити та контролювати місце, що містить пристрої;
- Визначити, хто винен у змінах їхнього місцезнаходження;
- Гарантувати, що особи віддалені від пристроїв та елементів живлення;
- Документувати будь-кого, хто мав доступ до місце-знаходження, та будь-кого, хто має причини бути причетним до епізоду інциденту;
- Якщо пристрій увімкнено, не треба його вимикати, та якщо пристрій вимкнено, не треба його вмикати;
- Якщо це можливо, задокументувати (наприклад, схема, фото або відео) місце, усі компоненти та кабелі в їхньому первісному положенні. Якщо камери та/або відеокамери немає, нарисувати схематичний план системи та позначки портів і кабелів так, щоб систему могло бути підтверджено та відновлено пізніше;
- Якщо це дозволено, дослідити місце для пошуку елементів, таких як причеплені нотатки, щоденники, папери, ноутбуки чи описи обладнання та програмного забезпечення з критичними деталями стосовно пристроїв, таких як паролі та PIN.

Примітка 1. Деякі юрисдикції можуть накладати спеціальні вимоги стосовно визнання фото та відеодоказів. DEFR повинен виконувати ці вимоги.

Примітка 2. DEFR повинен бути обізнаним, що потенційні цифрові докази можуть не завжди знаходитися в очевидних місцях, таких як розподілені або віртуальні сховища.

DEFR повинен із самого початку зазначити всі ризики, які виникають під час виконання всіх процесів протягом розслідування. Необхідно

розглянути, як захистити персонал та потенційні цифрові докази на місці інциденту.

6.2.2. Персонал

Важливо застосувати оцінювання ризиків стосовно безпеки персоналу до початку процесу, оскільки безпека персоналу, задіяного в процесі, є життєво важливою.

Питання, які мають бути розглянутими під час оцінювання ризиків стосовно персоналу включають, але не обмежуються, таке:

- Чи будуть присутні особи(-а), яких досліджують? Якщо присутні, чи мають вони схильність до насилля?
- Протягом якого часу доби буде проведено цю операцію?
- Чи може місце інциденту бути ізольовано від свідків?
- Чи наявна зброя в цьому місці?
- Чи є будь-який фізичний ризик для осіб, що будуть присутні?
- Чи може будь-що в близькості, охоплюючи пристрої, налагоджене так, щоб спричинити фізичне лихо, якщо неналежно обробляється, наприклад, приховану пастку?
- Чи можуть матеріали, що їх має бути зібрано, мати деяку ймовірність отримати фізіологічне ушкодження або порушення?
- Чи може місце інциденту розглядатися як небезпечне?
- Чи може оточення мати вплив на потенційний ризик?

6.2.3. Потенційний цифровий доказ

DEFR повинен бути обережним під час використання специфічних інструментів для збирання або здобуття потенційних цифрових доказів. Невизначені ризики перед виконанням дій можуть призвести до втрати частини або всього в цілому потенційного цифрового доказу через технологію, запроваджену протягом збирання або здобуття.

Ризики має бути оцінено для зменшення впливу стосовно подальших пошкоджень.

Оцінювання ризиків охоплює систематичну оцінку ризиків та потенційного впливу, який вони можуть мати на дослідження цифрових доказів. Аспекти, які потрібно розглянути протягом

оцінювання ризиків стосовно потенційних цифрових доказів, охоплюють, але не обмежуються таким:

- Який тип методів збирання/здобуття застосовують?
- Яке обладнання може бути потрібно на місці?
- Який рівень нестабільності (нестійкості) даних та інформації, пов'язаних з потенційними цифровими доказами?
- Чи можливий віддалений доступ до будь-яких цифрових приладів та чи складає він загрозу цілісності доказів?
- Що трапиться, якщо дані/обладнання буде пошкоджено?
- Чи може бути дані скомпрометовано?
- Чи може цифровий пристрій бути сконфігуровано так, щоб зруйнувати (наприклад, за допомогою логічної бомби), пошкодити або заплутати дані, якщо його вимкнути чи отримати доступ неконтрольовано?

6.3. Ролі та відповідальності

Роль DEFR охоплює ідентифікацію, збирання, здобуття та збереження потенційних цифрових доказів на місці інциденту. Вона охоплює розроблення звіту щодо збирання та здобуття, але звіт стосовно аналізування не є необхідним. Роль DEFR також охоплює гарантування цілісності й автентичності потенційних цифрових доказів. Для виконання своєї ролі DEFR повинен мати достатній досвід, навички та знання стосовно оброблення цифрових доказів. Це є критичним, оскільки потенційні цифрові докази можуть бути легко пошкоджені.

DEFR може також вимагати допомоги від персоналу технічної підтримки у відповідній сфері. Роль DES охоплює здійснення технічного підтримування DEFR в ідентифікації, збиранні, здобутті та збереженні потенційних цифрових доказів на місці інциденту. DES виконує спеціалізовану експертизу для DEFR. Матриця компетентності для DEFR (див. додаток А) служить як настанова для ідентифікації відповідних рівнів їх компетенції.

Примітка. У контексті оброблення інциденту за наявності ISIRT в ISO/IEC 27035:2011 розглянуто ролі DEFR та DES як членів ISIRT.

6.4. Компетентність

DEFR та DES повинні мати належні технічні та законодавчі компетенції (тобто, надані в додатку А) та продемонструвати, що вони пройшли відповідне навчання та мають достатнє технічне та законодавче розуміння для належного оброблення потенційних цифрових доказів.

Це охоплює розуміння процесів та методів, прийнятних для оброблення потенційних джерел цифрових доказів. Відповідні навички будуть потрібні DEFR для оброблення цифрових пристроїв, які містять потенційні цифрові докази. Наявність найкращого набору інструментів не буде гарантувати якості цифрових доказів, якщо DEFR не має компетенції у виконанні цих завдань.

Деякі юрисдикції приписують, як DEFR повинен доказувати свою кваліфікацію. Відповідальністю DEFR є гарантування того, що його належно поінформовано про те, як зробити це у відповідній юрисдикції. Якщо потрібно, DEFR та/або DES повинні мати змогу показати, що вони мають компетенцію для оброблення потенційних цифрових доказів з використанням інструментів та методів, визначених для виконання цих завдань. Також потрібно, щоб DEFR мав змогу надавати доказ своєї поточної компетенції.

Деякими передумовами для DEFR є такі:

- Вони мають належно та відповідно пройти навчання стосовно роботи із цифровими пристроями стосовно дослідницької діяльності;
- Вони мають показати відповідним органам у відповідній сфері та підтримувати свої навички та компетентність в обробленні потенційних цифрових доказів; та
- Відповідальністю особи(-іб) та роботодавця є гарантування, що вони відповідно пройшли навчання та підтримують навички та компетентність.

Примітка. Компетентність DEFR може змінюватися від однієї юрисдикції до іншої.

6.5. Запровадження необхідної обережності

Треба уникати будь-яких дій, які призведуть до псування потенційних цифрових доказів, що зберігаються в цифрових пристроях через навмисні або ненавмисні дії. Наприклад, піддавання впливу магнітних полів може псувати потенційні цифрові докази, які містяться на магнітних носіях для збереження. DEFR не повинен здійснювати доступу до цифрових пристроїв, таких, що знімають дамп пам'яті із цифрових пристроїв наживо, крім випадків, якщо вони мають належну компетентність та використовують надійні та затверджені процеси.

Є деякі обставини, коли неможливо збирати чи здобувати потенційні цифрові докази. DEFR повинен розглянути такі обставини, але не обмежуватися тільки ними:

- Якщо немає законних прав чи авторизації для збирання цифрових доказів;
- Якщо є зобов'язання щодо використання інших методів (наприклад, для уникнення переривання бізнесу);
- Якщо DEFR бажає охопити особливості виконання операцій протягом зловживання системою;
- Якщо збирання або здобуття мають здійснюватися приховано, якщо це вважається легальним у рамках юрисдикції;
- Якщо це критичний пристрій, який не може простоювати;
- Якщо фізичний розмір цифрового пристрою є дуже великим, наприклад, сервер у дата- центрі або RAID-система;
- Якщо це критичний цифровий пристрій безпеки, який ставить під загрозу життя, якщо буде зупинено; та
- Якщо це цифровий пристрій, який також надає послуги невинним сторонам.

6.6. Документація

Документація є критичною під час оброблення цифрових пристроїв, які можуть містити потенційні цифрові докази. DEFR повинен виконувати таке під час документування:

- Кожну виконувану дію має бути задокументовано. Це гарантує, що жодної деталі не було упущено під час виконання процесів ідентифікації, збирання, здобуття та збереження. Це може бути також доречним під час транскордонних розслідувань, там, де потенційні цифрові докази, які збираються з іншої частини земної кулі, може бути відповідно простежено.
- DEFR повинен бути уважним до встановлення часу та дати, якщо цифрові пристрої увімкнено. Порівняти встановлення часу з надійним джерелом часу, таким, як час, синхронізованим з надійним джерелом та який можливо простежити. Ці встановлення часу має бути задокументовано та зазначено, якщо є будь-яка різниця. Деякі системи потребують великої кількості взаємодій з користувачем для отримання встановлення часу та дати. DEFR повинен бути обережним, щоб не модифікувати систему. Тільки належно навчений персонал повинен виправляти ці встановлення.
- DEFR повинен задокументувати все, що видно на екрані цифрового пристрою: активні програми та процеси, а також назви відкритих документів. Це документування має охоплювати опис того, що видимо, оскільки деякі зловмисні програми можуть маскуватися під добре відоме програмне забезпечення.
- Будь-які переміщення цифрових пристроїв має бути задокументовано відповідно до локальних вимог.
- Документувати всі унікальні ідентифікатори цифрових пристроїв та приєднаних частин, таких як серійні номери та унікальне маркування.

Приклади мінімального набору документації для обміну потенційними цифровими доказами між різними юрисдикціями наведено в додатку Б.

Примітка. Для докладнішої інформації стосовно документації треба звернутися до розділу керування документами та розділу керування записами ISO/IEC 17025:2005.

6.7. Інструктаж

6.7.1. Загальні положення

Важливо, щоб DEFR та DES були відповідно проінструктовані уповноваженим органом перед виконанням їхніх завдань, особливо стосовно деяких законів про конфіденційність та обмеження (тобто, потрібні базисні знання). Важливо мати формальну сесію інструктажу для розуміння інциденту, що треба очікувати та не очікувати протягом розслідувань, та нагадування стосовно недопущення втручання та псування доказів. Інструктаж має бути достатньо суттєвим для членів, прийнятно підготовлених у розподілі ролей та відповідальності; отже буде гарантовано вилучення всіх прийнятних потенційних цифрових доказів.

6.7.2. Особливість цифрових доказів

Сесія інструктажу, сфокусована чітко на специфічних настановах щодо цифрових доказів, потрібна для інформування DEFR щодо особливостей, притаманних розслідуванню. Протягом цієї сесії інструктажу DEFR та DES повинні бути ознайомлені з відповідною інформацією та докладними інструкціями стосовно потенційних цифрових доказів, які має бути зібрано чи здобуто. Це може охоплювати:

- Тип інциденту (якщо відомий);
- Дату й час інциденту (якщо відомі);
- План розслідування (збирання та/або здобуття, відома мережева діяльність, відомі вимоги щодо нестабільних (нестійких) даних, тощо);
- Розглянути, де і як потенційні цифрові докази будуть зберігатися/транспортуватися після збирання або здобуття;

- Специфічні інструменти, потрібні для здобуття потенційних цифрових доказів;
- Потенційні цифрові докази, які потребують специфічних типів досліджень;
- Обладнання та описи стосовно цифрових пристроїв;
- Нагадування членам команди про потребу відключити будь-які можливості Bluetooth або Wi-Fi на їхніх телефонах/комп'ютерах, щоб вони не могли випадково взаємодіяти із цифровими пристроями, за винятком телефонів/комп'ютерів, використовуваних для виявлення зв'язків.
- Важливість документування протягом розслідування; та
- Запровадження законодавчих або інших чинників, які забороняють збирання будь-яких пристроїв та потенційних цифрових доказів, що вони містять.

Ця особлива сесія інструктажу може бути частиною загальної сесії інструктажу, описаною в розділі 6.7.1.

6.7.3. Особливості персоналу

Сесія інструктажу, сфокусована на специфічних настановах щодо персоналу, потрібна для інформування DEFR щодо особливостей, притаманних сторонам, які беруть участь у розслідуванні. Протягом цієї сесії інструктажу команда дослідників має бути ознайомлена з інструкціями стосовно персоналу. Це може охоплювати:

- Призначення, ролі та відповідальність членів команди дослідників на місці інциденту;
- Чи очікується, що інші сторони (медичний персонал, біологічні судові дослідники тощо) будуть брати участь у цих розслідуваннях;
- Вимогу до членів команди дослідників не допускати технічної допомоги від будь-яких неавторизованих осіб; та
- Вимогу до членів команди дослідників суворо дотримуватися процедури, щоб мінімізувати ризик псування потенційних цифрових доказів, такого як

уникнення використання інструментів або матеріалів, які можуть спричиняти або емітувати статичну електрику або магнітне поле, що може пошкодити або зруйнувати потенційні цифрові докази.

Ця особлива сесія інструктажу може бути частиною загальної сесії інструктажу, описаною в розділі 6.7.1.

6.7.4. Інциденти реального часу

Найбільш бажано, щоб розслідування інциденту було заплановано заздалегідь, але є обставини (наприклад, якщо інцидент розвивається та створює відклики), де повне планування не можливо. У таких ситуаціях команда має бути проінструктовано стосовно початкової стратегії та тактики розслідування та має дозвіл розробити нову стратегію та тактику у відповідь на існуючі умови. Інформація стосовно цього інциденту, як він розвивається, має бути поширена серед членів команди так швидко, як це можливо, щоб гарантувати, що рішення стосовно дій, які треба здійснити, було визначено ефективно та з урахуванням потреб юрисдикції.

6.7.5. Інша інформація стосовно інструктажу

Окремо від інструктажу щодо цифрових доказів та персоналу, команді дослідників має бути надано інструктаж щодо іншої важливої інформації, яка охоплює:

- Визначення місця, де буде проведено розслідування, охоплюючи назву організації, адресу та карту місцевості (якщо можливо);
- Дозвіл на розслідування;
- Подробиці пошукових повноважень та інших повноважень, притаманних цьому розслідуванню, охоплюючи обмеження пошуку та конфіскації;
- Законодавчі аспекти й особливості залучення;
- Часовий діапазон розслідування;
- Обладнання, яке потрібно доставити на місце інциденту для досліджень;
- Інформація щодо логістики; та

– Потенційний конфлікт інтересів.

DEFR та DES повинні уникати ситуацій, коли може бути висунуто обвинувачення в прихованій упередженості. Прикладом прихованої упередженості є ситуація, коли DEFR копіює один комп'ютер, а не інший (який, як пізніше виявляється, містить виправдовувальні докази), ґрунтуючись на своїх уявленнях, що сформовано інструктажем.

6.8. Визначення пріоритетів збирання та здобуття

Під час визначення пріоритетів збирання або здобуття потенційних цифрових доказів, обов'язковим для DEFR є розуміння причин для збирання або здобуття потенційних цифрових доказів. Як загальний принцип, DEFR повинен спробувати отримати максимальну кількість даних, збережених за допомогою дій зі збирання та здобуття. Однак може бути потрібним визначити пріоритетні елементи залежно від значення нестійкості та/або значущості/потенційних цифрових доказів. Елементи з високим релевантним/потенційним значенням цифрових доказів є такі, що найімовірніше містять дані, які безпосередньо стосуються розслідуваного інциденту.

Визначення пріоритетів унаслідок пошкодження може бути запроваджено, тільки якщо цього потребують специфічні обставини розслідуваного випадку. Потенційні цифрові докази може бути розділено на дві категорії: нестійкі та сталі. Нестійкі дані може бути легко зіпсовано або втрачено назавжди, якщо не застосовують належну обережність для захисту цих даних. Наприклад, вимикання живлення цифрового пристрою може призвести до втрати нестійких даних. Сталі дані залишаються в середовище навіть якщо живлення вимкнено.

Оскільки деякі типи цифрових доказів можуть мати короткий термін життя, потенційні цифрові докази можуть бути легко зіпсовані або порушені. Там, де незрозуміло, чи містить цифровий пристрій потенційні цифрові докази, або які елементи є важливішими, може виникнути потреба перевірити

їх перед збиранням з використанням процесу визначення пріоритетів. Цифрові пристрої, які необхідно розглянути для збирання, охоплюють, але не обмежуються: IT-обладнанням та носіями для збереження цифрових даних, CCTV-системами, PED, автоматизованими системами, системами контролю та імпровізованими електронними системами. Спочатку треба здобути найбільш нестійкі потенційні цифрові докази, такі як RAV, простір свопінгу, запущені процеси тощо. DEFR повинен володіти глибокими знаннями для визначення пріоритетів відповідно до нестійкості.

Протягом ідентифікації DEFR повинен:

– Визначити пріоритети потенційних цифрових доказів, які може бути втрачено назавжди, якщо буде вимкнено живлення; та
– Прийняти швидкі дії для збирання та здобуття цих даних за допомогою затверджених методів.

Примітка 1. Деякі нестійкі дані можуть змінюватися через чинники, які охоплюють, але не обмежуються, переміщення, час та зміни в оточенні цифрових пристроїв – необхідно гарантувати, що такі дані збережено перед переміщення цього пристрою.

Примітка 2. Цифрові пристрої, які містять потенційні цифрові докази, можуть бути джерелом фізичних доказів (наприклад, відбитків пальців, DNA тощо). DEFR повинен бути обережним, щоб не зіпсувати такі докази, та координувати свої наступні дії з відповідальними особами, які збирають такі докази.

Примітка 3. Якщо допустимо наявність шифрування або шкідливого програмного забезпечення, бажано перевірити нестійкі дані.

За таких обставин час може бути обмежувальним чинником протягом дослідження. У таких випадках треба віддавати перевагу потенційним цифровим доказам, ідентифікованим як притаманним цьому специфічному інциденту.

6.9. Збереження потенційних цифрових даних

6.9.1. Загальні положення

Під час збереження здобутих потенційних цифрових доказів та зібраних цифрових приладів під час пакування важливо убезпечити ці елементи так, щоб уникати псування або порушення. Псування може бути результатом несприятливих змін магнітного поля та електричного живлення, впливу тепла, високої або низької вологості, а також удару та вібрацій. Порушення може бути результатом дій з навмисного внесення змін або допущення внесення змін у потенційні цифрові докази. Тому є дуже критичним захистити потенційні цифрові докази в найкращий можливий спосіб та найменш використовувати первісні дані. Важливо, щоб DEFR був ознайомлений з вимогами щодо пакування у використовуваній юрисдикції.

6.9.2. Збереження потенційних цифрових доказів

Усі зібрані цифрові пристрої та здобуті потенційні цифрові докази має бути захищено, наскільки це можливо, від втрати, порушення або псування. Найважливішою діяльністю в процесі збереження є підтримання цілісності та автентичності потенційних цифрових доказів та їхнього хронологічного документування.

Зібрані цифрові пристрої та здобуті потенційні цифрові докази потрібно зберігати в пристроях збереження доказів, де запроваджено заходи фізичної безпеки, такі як системи контролю доступу, системи спостереження або системи виявлення вторгнень або в іншому контрольованому середовищі для збереження потенційних цифрових доказів. Основними цілями фізичної безпеки є захист та уникнення втрат, пошкоджень та порушень, а також уможливлення здійснення аудиту.

Зібрані цифрові пристрої перед переміщенням в інше місце має бути обгорнуто чи розміщено у відповідному пакуванні, придатному для цього пристрою для уникнення спотворення цифрового пристрою(-їв). Потрібно використовувати пакування, яке захищає від ударів для уникнення фізичного пошкодження будь-яких компонентів пристрою(-їв).

– DEFR повинен розглянути чутливість цифрового пристрою до статичної електрики. Якщо це дійсно існує, пристрій має бути захищено антистатичною упаковкою.
– Основні блоки системи та ноутбуки потребують захисту в належному контейнері для уникнення пошкодження або псування потенційних цифрових доказів, які можуть залишатися там.

Примітка. Використання пакування Фарадея або іншого пакування з екрануванням від радіочастот може збільшити витік батареї мобільного телефону. Це може потребувати забезпечення додаткового живлення для пристрою, доки він знаходиться в середині пакування, якщо ресурси дозволяють.

6.9.3. Пакування цифрових пристроїв та потенційних цифрових доказів

6.9.3.1. Основні дії. пакування потенційних цифрових доказів

Основні дії потрібно виконувати, навіть якщо є зиск не виконувати їх. Це можна також розглядати як мінімальні дії, які треба виконувати. Протягом пакування DEFR повинен записувати та звертати увагу на такі основні дії:

– Не торкатися магнітних стрічок, краще працювати зі стрічками в їхніх захисних контейнерах або торкатися лише в місцях, які завідомо не містять даних (наприклад, край оптичних дисків). Це має бути зроблено, тільки якщо DEFR одягає спеціальну рукавичку.

Примітка. Спеціальні місця середовища збереження, про які відомо, що вони не містять даних, залежать від типу середовища. DEFR відповідає за знання новітніх технологій та повинен бути ознайомлений з обробленням середовищ збереження.

– Для гарантування правильної ідентифікації DEFR повинен позначати етикетками всі потенційні цифрові докази. Деякі юрисдикції мають спеціальні вимоги стосовно формату етикеток доказового матеріалу. DEFR повинен знати, та підтвердити вимоги, які потрібно застосовувати. DEFR повинен позначити етикетками всі потенційні цифрові

докази, зібрані цифрові пристрої та будь-які частини обладнання, пов'язані з цими пристроями з етикетками, як на доказах. Етикетка не повинна розміщуватися безпосередньо на механічних частинах цифрового пристрою та не повинна закривати або приховувати важливу ідентифікаційну інформацію. Усі потенційні цифрові докази в зібраних пристроях мають здобути та повинні зберігатися так, щоб гарантувати цілісність цих доказів.

- Якщо можливо, цифрові пристрої з відкритими та рухомими елементами мають бути запечатаними за допомогою етикеток, які запобігають порушенню доказів, прийнятних до цього пристрою, і DEFR повинен підписати запечатування.
- Пристрої з несталими даними, обладнані батареями, мають регулярно перевірятися для гарантування того, що ці пристрої завжди мають достатнє живлення.
- Ідентифікувати та убезпечити цифрові пристрої в контейнері, який за своїм походженням прийнятний цьому пристрою для захисту від потенційних загроз.
- Комп'ютери та цифрові пристрої має бути запаковано так, щоб уникнути пошкодження від удару, вібрації, великих висоти, тепла та опромінення радіочастотами протягом транспортування.
- Магнітні носії для збереження цифрових даних потрібно зберігати в пакуванні, яке є магнітно інертною, антистатичною та вільною від часточок.
- Цифрові докази можуть також містити приховані докази, відбитки чи біологічні докази. Якщо це так, необхідно запровадити відповідні дії для збереження цих потенційних доказів. Необхідно зробити образи цифрового доказу після того, як процеси збирання прихованих доказів, відбитків чи біологічних доказів

було застосовано на цих пристроях. Однак рішення щодо визначення пріоритетів збирання доказів має бути ретельно оцінено з урахуванням можливості збереження цих доказів.

6.9.3.2. Додаткові дії: пакування потенційних цифрових доказів

Додаткові дії, які належать до дуже рекомендованих, має бути виконано.

Протягом пакування DEFR повинен записувати та звертати увагу на такі додаткові дії, якщо їх застосовують:

- Одягнути спеціальні рукавички та гарантувати, що руки є чистими та сухими.
- Захистити цифрові пристрої від впливу електромагнітних джерел (наприклад, поліцейське радіо, гучномовці, рентген-апарати). Середовище пакування має бути вільним від статичної електрики.
- Середовище пакування має бути вільним від пилу, жиру та хімічних забруднювачів, які спричиняють псування через окиснення та конденсації вологи на магнітному шарі.
- Мінімізувати змогу копіефекту (перенесення сигналу від одного рулона стрічки до сусіднього рулона), яке може траплятися, якщо стрічки зберігаються протягом тривалого періоду без активного використання, призводячи до низької якості сигналу.
- Якщо потрібно, місця пакування мають бути вільними від UV-світла. UV може спричинити пошкодження DNA або пошкодження деяких типів середовищ. DEFR повинен розглянути, чи може бути ризик від UV для потенційних цифрових доказів перед вибором місця пакування.
- Цифрові пристрої мають бути надійно захищені від теплового удару.

6.9.4. Транспортування потенційних цифрових доказів

DEFR повинен зберігати зібрані цифрові пристрої та здобуті потенційні цифрові докази протягом транспортування.

Потенційні цифрові докази не повинні залишатися без уваги протягом процесу транспортування. DEFR повинен підтримувати хронологічне документування протягом процесу транспортування для уникнення можливих пошкоджень або псування та підтримувати цілісність та автентичність цифрових пристроїв та потенційних цифрових доказів. Якщо потенційні цифрові докази не транспортуються DEFR або DES, рекомендовано запровадити шифрування.

Примітка. DEFR повинен гарантувати, що збирання чуттєвої інформації та персональних даних виконується відповідно до законів локальної юрисдикції та нормативних документів із захисту інформації.

Протягом пакування та транспортування DEFR повинен бути уважним щодо можливої наявності електростатичних розрядів, які можуть зменшити доказове значення потенційних цифрових доказів. DEFR повинен гарантувати, що комп'ютери та цифрові пристрої запаковано безпечно для уникнення пошкоджень від ударів та вібрації.

Процес транспортування має бути дозволеним для керованого та контрольованого середовища. Рівень вологості, вогкості повітря та температура мають бути прийнятними для цифрових пристроїв. Треба уникати находження потенційних цифрових доказів та цифрових пристроїв у транспортному засобі протягом тривалих періодів та уникати їхнього знаходження за наявності UV.

У деяких юрисдикціях, якщо обставини не дозволяють, DEFR не може супроводжувати докази. У таких випадках може бути використано відповідні та авторизовані механізми транспортного засобу для гарантування належної безпеки доказів протягом транспортування. Документація стосовно транспортування та підтвердження цілісності пакування має бути частиною хронологічного документування.

7. ПРИКЛАДИ ІДЕНТИФІКАЦІЇ, ЗБИРАННЯ, ЗДОБУТТЯ ТА ЗБЕРЕЖЕННЯ

7.1. Комп'ютери, периферійні пристрої та носії для збереження цифрових даних

7.1.1. Ідентифікація

7.1.1.1. Огляд та документування фізичного місця інциденту

У контексті цього розділу комп'ютери розглядають як окремі цифрові пристрої, які приймають, обробляють та зберігають дані й отримують результати. Такі комп'ютери не під'єднано до мережі, але їх може бути під'єднано до периферійних пристроїв, таких як принтери, сканери, веб-камери, MPS-плеєри, GPS-системи, RFID-прилади тощо. Цифрові пристрої, які мають мережевий інтерфейс, але не підключені до мережі під час збирання або здобуття потенційних цифрових доказів, має бути розглянуто (для цілей цього стандарту) як окремий комп'ютер. Якщо комп'ютер має мережевий інтерфейс, але не було знайдено явних підключень, треба виконати дії для ідентифікації пристроїв, до яких він мав бути підключеним у недавньому минулому.

Зазвичай, місця інцидентів містять різні типи носіїв для збереження цифрових даних. Носії для збереження цифрових даних використовують для збереження даних від цифрових пристроїв та вони відрізняються об'ємом пам'яті. Приклади носіїв для збереження цифрових даних включають, але не обмежуються, зовнішні портативні жорсткі дисководи, флеш-носії, CD, DVD, Blu-ray диски, гнучкі диски, магнітні стрічки та карти пам'яті.

Перед тим, як можна запровадити будь-яке здобуття чи збирання, необхідно розглянути питання безпеки потенційних цифрових доказів. Ці питання описано в 6.2.1 та 6.2.2. Однак DEFR повинен бути обережним у переконанні, що пристрій, який виявляється окремим, не був нещодавно підключеним до мережі. Якщо є припущення, що зараз окремий цифровий пристрій був нещодавно відключеним, має бути зроблено спробу обробляти його як мережевий пристрій, щоб впевнитися, що інші частини

мережі працюють правильно. DEFR повинен записувати та звертати увагу хоча б на таке:

- DEFR повинен задокументувати тип та назву будь-якого використовуваного цифрового пристрою та ідентифікувати всі комп'ютери та периферійні пристрої, які потрібно здобути чи зібрати протягом початкової стадії. Має бути також задокументовано серійні номери, номери ліцензій та інші ідентифікаційні позначки (охоплюючи фізичне пошкодження), там, де це можливо зробити.
- На стадії ідентифікації статус комп'ютерів та периферійних пристроїв має залишатися як є. Якщо комп'ютери вимкнено, не треба їх вмикати. Якщо комп'ютери або периферійні пристрої увімкнено, DEFR не повинен їх вимикати, що в іншому разі може зіпсувати потенційні цифрові докази.
- Якщо комп'ютери ввімкнено, DEFR повинен сфотографувати або зробити паперовий документ стосовно того, що зображено на екранах. Будь-який паперовий документ має містити опис того, що реально видно (наприклад, приблизні позиції вікон, назв та контенту).

Пристрої, що мають батареї, які можуть розрядитися, потребують зарядки батарей для гарантування того, що інформацію не буде втрачено.

DEFR повинен також розглянути за допомогою детектора бездротових сигналів питання пошуку та ідентифікації бездротових сигналів від бездротових пристроїв, що може бути приховано. Можуть скластися такі обставини, коли детектор бездротових сигналів не використовують через обмеження вартості та часу, і DEFR повинен це задокументувати. Якщо буде знайдено будь-які мережеві пристрої, DEFR повинен продовжувати процес оброблення доказів, як описано в 7.2.2.2. цього стандарту. Там, де використовують активне сканування (тобто, широкополосне та/або вибіркове) для мережевих

пристроїв, пристрої сканування має бути вимкнено на час оцінювання ймовірності того, що ці пристрої можуть взаємодіяти з іншими пристроями на місці. Члени команди повинні пам'ятати, що певний пристрій на місці може визначити наявність активних пристроїв сканування та використання активного сканування може призвести до тригерних подій, які можуть зіпсувати потенційні цифрові докази та можуть, в екстремальних обставинах, призвести до активації маскувальних дій.

Примітка 1. У деяких юрисдикціях дозволено вмикати цифрові пристрої на місці події для визначення їхньої доречності в розслідуванні, якщо наявна велика кількість цифрових пристроїв. Це відбувається з урахуванням часу оброблення та вартості, які можуть бути недоречними, якщо будуть оброблятися непричетні цифрові пристрої. Якщо пристрій було увімкнено для оцінювання на місці, DEFR повинен гарантувати, що докладні нотатки застосованих дій підтримуються протягом цього процесу.

Примітка 2. Для збереження статусу живлення цифрового пристрою має бути розглянуто результати несталості та процесу визначення пріоритетів. Якщо прийнято рішення, що найкритичніша інформація є сталою інформацією на диску, тоді треба сфотографувати екран консолі цієї працюючої системи та вимкнути її. Якщо наявна нестала інформація в пам'яті, тоді критично важливо залишити систему ввімкнутою, щоб мати змогу виконати здобуття її інформації.

7.1.1.2. Збирання нецифрових доказів

DEFR повинен розглянути збирання нецифрових доказів. Для цього лідер команди повинен ідентифікувати осіб, які відповідають за обладнання на місці. Ці особи можуть надати додаткову інформацію та документацію, таку як паролі до цифрових пристроїв та інші відповідні подробиці. DEFR повинен задокументувати імена та посади цих осіб.

DEFR може також потребувати збирання деяких доказів в опитуваннях осіб, які можуть мати корисну або потрібну інформацію щодо потенційних цифрових доказів або цифрових пристроїв, що збираються. Будь-які відповіді має бути точно

задокументовано. Ці особи можуть включати системного адміністратора, власника пристрою та користувачів комп'ютера та периферійних пристроїв. Протягом такого вербального збирання доказів DEFR може домагатися інформації такої, як конфігурація системи та пароль адміністратора/рутовий пароль. Така додаткова інформація може бути корисною на стадії аналізування потенційних цифрових доказів. Ці опитування має бути задокументовано для гарантування того, що подробиці є точними та задокументовані твердження не може бути змінено. DEFR повинен бути ознайомлено з відповідними вимогами законодавства стосовно збирання нецифрових доказів.

7.1.1.3. Процес прийняття рішень для збирання та здобуття

Під час прийняття рішення щодо збирання цифрових пристроїв або здобуття потенційних цифрових доказів необхідно розглядати кілька чинників, які охоплюють, але не обмежуються таким:

- несталість потенційних цифрових доказів, що обговорено в 5.4.2 та 6.8;
- наявність шифрування всього диска або зашифрованих частин, де парольна фраза чи ключі зберігаються як несталі дані в RAM, на зовнішніх токенах, смарт-картах, інших пристроях або середовище;
- критичність системи, наведеної в 5.4.4, 7.2.1.2 та 7.1.3.4;
- вимоги законодавства, та
- ресурси, такі як потрібний розмір сховища, наявність персоналу, часові обмеження.

На рисунку 1 зображено огляд процесу прийняття рішення запроваджувати збирання чи здобуття.

7.1.2. Збирання

7.1.2.1. Цифрові пристрої увімкнено

7.1.2.1.1. Загальні положення. DEFR може використовувати кілька настанов для збирання даних, якщо цифровий пристрій увімкнено. Не всі настанови є ідеальними та їх можна використовувати для будь-яких випадків; деякі настанови прийнятні тільки для специфічних випадків. Відповідно,

настанови може бути покласифіковано як основні або додаткові. Основні дії потрібно застосовувати для всіх обставин, у той самий час додаткові дії потрібно запроваджувати, якщо вони доречні, та можуть бути застосовані залежно від унікального приладу чи обставин.

DEFR відповідає за знання сучасних технологій та має бути ознайомлено з настановами стосовно оброблення носіїв для збереження.

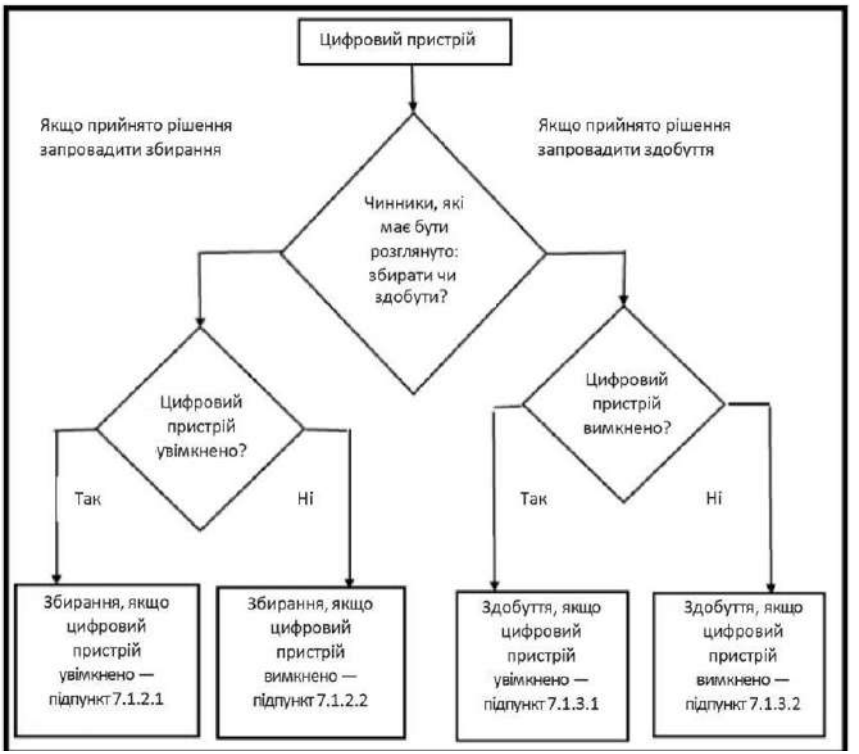

Рис. 1. Настанова для процесу прийняття рішення збирати чи здобути потенційні цифрові докази

7.1.2.1.2. Основні дії. Збирання увімкнених цифрових пристроїв. Такі основні дії має бути запроваджено в усіх випадках стосовно потенційних цифрових доказів. Ці настанови застосовують, якщо DEFR прийняв рішення, що мають збиратися цифрові пристрої, якщо їх увімкнено:

– Розглянути здобуття несталих даних із цифрових пристроїв та поточний стан перед вимкненням системи. Ключі шифрування та інші критичні дані може бути розміщено в активній пам'яті або в неактивній пам'яті, яку не буде очищено. Розглянути логічне здобуття, якщо запроваджено шифрування. У цьому разі треба враховувати, що чинна основна операційна система може бути ненадійною, тому треба розглянути використання відповідних надійних та затверджених інструментів.
– Конфігурація цифрового пристрою може визначати, чи потребує DEFR вимикання цього пристрою за допомогою звичайних адміністративних процедур чи вилку пристрою має бути вилучено з розетки живлення. DEFR може потребувати консультації з DES для визначення найкращого підходу, доречного для специфічних обставин. Якщо прийнято рішення про вилучення вилки з розетки, DEFR повинен вилучити кабель живлення, з початку вилучаючи кінець, підключений до цифрового пристрою, а не кінець, що підключений до розетки. Треба бути обережним, оскільки пристрій, підключений до UPS, може змінювати дані, якщо кабель живлення вилучається з розетки, а не з пристрою.

Примітка 1. Якщо живлення буде відключено від працюючого пристрою, будь-які потенційні докази, що зберігаються в зашифрованому вигляді, будуть недоступні, доки не буде отримано ключ дешифрування. Потенційна цінність «живих» даних може бути також втраченою, що призведе до пошкоджень або втрат людських життів, таких як корпоративні дані або цифрові пристрої, що керують медичним обладнанням. Тому DEFR повинен гарантувати, що несталі дані будуть зібрані до вимкнення живлення.

Примітка 2. Є пристрої, які дозволяють пристрій, що увімкнений, відключити від джерела живлення та перемістити його до портативного UPS без переривання живлення цього пристрою. Є також похитування мишкою, які може бути використано для уникнення активації програми блокування екрана. Обидва ці пристрої надають доречні інструменти, якщо виконують дослідження увімкненого пристрою, де може бути запроваджено шифрування. Якщо увімкнені пристрої збираються так, що живлення підтримується, пакування та транспортування діючих систем повинна мати заходи, пов'язані із забезпеченням охолодження, захисту від механічних ударів тощо.

– Забезпечити позначки, відключення та убезпечення всіх кабелів від цифрового пристрою та забезпечити позначки портів так, щоб систему могло бути реконструйовано пізніше.
– Помістити стрічку поверх вимикача живлення, якщо потрібно, для уникнення зміни стану живлення. Розглянути, чи стан вимикача задокументовано відповідно перед закриттям його стрічкою або переміщенням.

7.1.2.1.3.Додаткові дії: збирання увімкнених цифрових пристроїв. Треба запроваджувати додаткові дії, які є доречними залежно від конфігурації специфічного цифрового пристрою.

– Для ноутбука треба гарантувати, що несталі дані було здобуто перед вилученням батареї. DEFR повинен вилучити основне джерело живлення одразу, замість виключення клавіші живлення на ноутбуці для його перезавантаження. DEFR повинен також звернути увагу, якщо наявний адаптер живлення, та, якщо це так, тоді вилучити адаптер живлення після вилучення батареї.

Примітка 1. Натискання клавіші живлення на цифровому пристрої може бути сконфігуровано так, що буде запущено скрипт, який може змінювати інформацію або видаляти інформацію із системи перед перезавантаженням або надавати засторогу приєднаній системі, що виявлено несподівану ситуацію, яка може призвести до стирання даних, що мають доказове значення,

перед тим, як їх ідентифіковано. Пристрій може бути також сконфігуровано так, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншим присутнім особам.

– Розмістити стрічку поверх слоту гнучких дисків, за наявності.
– Необхідно впевнитися, що лотки слотів CD або DVD розміщено на своїх місцях; звернути увагу, чи ці лотки слотів порожні, містять диски або не перевірялися; та закрити лоток слотів стрічкою для уникнення його відкриття.

Примітка 2. Якщо будь-який завантажуваний носій залишено в слоті, тоді в момент, коли цей пристрій буде увімкнено наступного разу, він може завантажитися із цього носія, а не із жорсткого диска (або з інструментів драйвера гнучкого диска) залежно від установок BIOS комп'ютера.

– DEFR повинен виконувати збирання нецифрових доказів відповідно до законодавчих процедур для гарантування того, що будь-які докази припустимі.

7.1.2.2. Вимкнені цифрові пристрої

7.1.2.2.1. Загальні положення. DEFR може використовувати низку настанов для збирання, якщо цифровий пристрій вимкнено. Не всі дії, що містяться в цих настановах, може бути застосовано для всіх обставин. Отже, необхідно визначити відмінності між тими діями, що може бути застосовано в усіх випадках (основні дії), та тими, що можуть бути застосовані тільки в деяких випадках (додаткові дії).

На рисунку 2 зображено основні та додаткові дії, застосовувані для збирання вимкнених цифрових пристроїв.

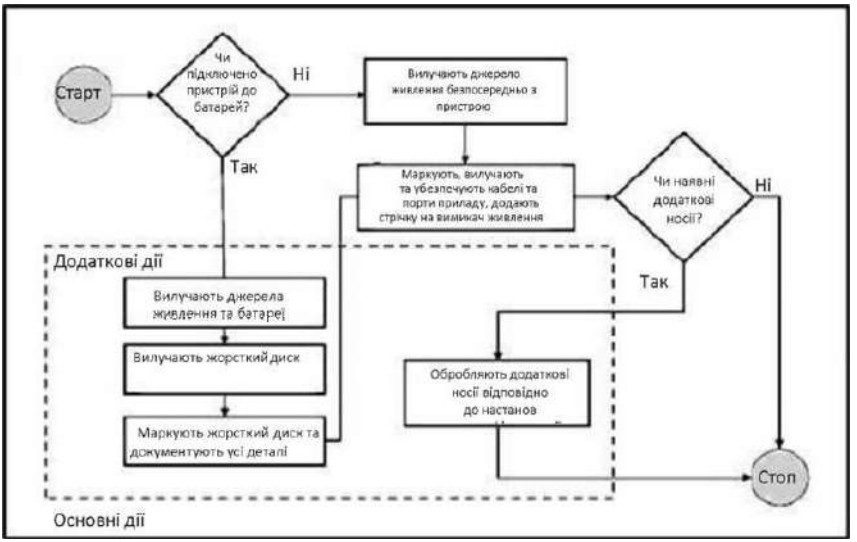

Рис. 2. Настанови для збирання вимкнених цифрових пристроїв

7.1.2.2.2. Основні дії: збирання вимкнених цифрових пристроїв. Такі дії є рекомендованими основними діями для збирання, якщо цифровий пристрій вимкнено:

- Вилучити кабель живлення так: з початку вилучити кінець, підключений до цифрового пристрою, а не кінець, підключений до розетки.
- Вилучити та убезпечите всі кабелі від цифрових пристроїв та помістити позначки на портах так, щоб систему могло бути реконструйовано пізніше.
- Помістити стрічку на вимикачі живлення, за потреби, для уникнення зміни стану вимикача. Упевнитися, чи стан вимикача було правильно задокументовано перед тим, як він був закритий стрічкою або відкритий.

Примітка. Зазвичай носій для збереження не повинен бути вилученим із блока цифрового пристрою до того, як буде зроблено здобуття потенційних цифрових доказів, оскільки його вилучення

збільшує ризик пошкодження або плутанини його з іншими носіями для збереження. Має бути розроблено та запроваджено локальні процедури стосовно потреби вилучення носіїв для збереження даних із цифрових пристроїв.

7.1.2.2.3. Додаткові дії: збирання вимкнених цифрових пристроїв. Такі дії є додатковими діями, які є доречними для збирання вимкнених цифрових пристроїв залежно від конфігурації специфічного цифрового пристрою:

- З початку треба впевнитися, що ноутбук дійсно вимкнено, оскільки деякі з них можуть бути в режимі очікування. Треба бути обережними, оскільки деякі ноутбуки можуть вмикатися в разі відкриття кришки. Потім перейти до вилучення основної батареї живлення ноутбука.
- Якщо умови на місці дослідження потребують вилучення жорсткого диска, DEFR повинен бути обережним під час заземлення цифрового пристрою для уникнення впливу статичної електрики щодо пошкодження дисководу жорсткого диска. В іншому разі, дисковод жорсткого диска не повинен вилучатися на місці. Розмістити позначку на дисководі жорсткого диска, як підозрілого диска, та задокументувати всі деталі, такі як тип, назва моделі, серійний номер та розмір дисковода жорсткого диска.
- Розмістити стрічку поверх слота гнучких дисків, за наявності.
- Необхідно впевнитися, що лотки слотів CD або DVD розташовано на своїх місцях; звернути увагу, чи ці лотки слотів порожні, містять диски або не перевірялися; та закрити лотки слотів стрічкою для уникнення його відкриття.

Примітка. Якщо будь-який завантажуваний носій залишено в слоті, тоді в момент, коли цей пристрій буде увімкнено наступного разу, він може завантажуватися з носія, а не з жорсткого диска (або з інструментів драйвера гнучкого диска) залежно від установок BIOS комп'ютера.

7.1.3. Здобуття

7.1.3.1. Увімкнені цифрові пристрої

7.1.3.1.1. Загальні положення. Є три сценарії, у яких може виникнути потреба здобуття цифрових доказів: якщо цифровий пристрій увімкнено, якщо цифровий пристрій вимкнено та якщо цифровий пристрій увімкнено, але не може бути вимкнено (таких як критичні цифрові пристрої).

У всіх цих сценаріях DEFR потребує отримання точної копії цифрових доказів з носія для збереження цифрового пристрою, який підозрюється в тому, що він містить потенційні цифрові докази.

Якщо неможливо зробити образ цифрового пристрою, необхідно здобути точні копії специфічних файлів, які можуть містити потенційні цифрові докази. Ідеально, має бути зроблено як затверджену майстер-копію, так і робочу копію. Майстер-копію не можна використовувати знову, хоча вона потрібна для підтвердження контенту робочої копії або виконання заміни робочої копії після пошкодження першої робочої копії.

DEFR може запроваджувати низку настанов для здобуття, якщо визначено, що цифровий пристрій увімкнено. Не всі настанови є ідеальними та підходять для всіх випадків; деякі настанови може бути застосовано тільки для специфічних випадків. Відповідно, настанови може бути покласифіковано як основні або додаткові. Необхідно розглянути можливість того, що увімкнені системи може бути введено в режим блокування екрана чи автоблокування та що існують приховані значення до будь-яких спроб для уникнення цього. Наприклад, коливання мишкою буде потребувати встановлення USB-ключа для реєстрації та найімовірніше може викликати модифікацію за будь-яких інших дій. Використання доречних методів буде мінімізувати приховані значення таких дій.

На рисунку 3 зображено основні та додаткові дії, застосовувані для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях.

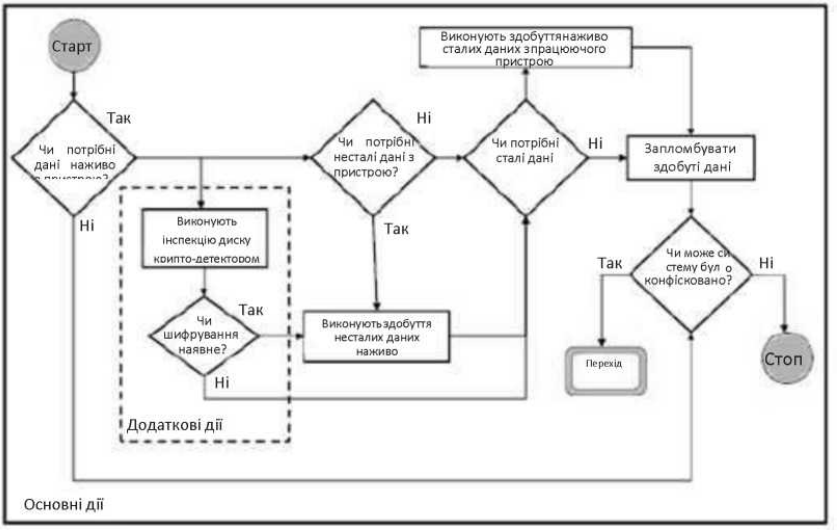

Рис. 3. Настанови для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях

7.1.3.1.2. Основні дії: здобуття потенційних цифрових доказів на увімкнених цифрових пристроях. Такі дії є основними діями, які має бути запроваджено DEFR у всіх випадках здобуття потенційних цифрових доказів на увімкнених цифрових пристроях:

– З початку розглянути здобуття потенційних цифрових доказів, які можуть бути втраченими, якщо цифровий пристрій буде вимкнено. Також відомо для несталих даних, таких як дані, що зберігаються в RAM, запущених процесах, мережевих з'єднаннях та установках дати/часу. Якщо необхідно здобути сталі дані з пристроїв, які ще працюють, має бути розглянуто здійснення здобуття на ввімкнених системах.
– Запровадження здобування наживо необхідно для здобуття даних наживо від пристроїв, які ще працюють. Здобуття несталих даних наживо в RAM дає змогу

відновлення важливої інформації, такий як статус мережі, декодовані прикладні програми та паролі. Ці процеси відрізняються та потребують використання різних наборів інструментів.

– DEFR повинен ніколи не довіряти програмам у системах. Із цієї причини, там, де це можливо, рекомендовано користуватися затвердженим інструментом, отриманим DEFR (для статичного бінарного коду). DEFR повинен мати компетенцію застосування затверджених інструментів та бути компетентним щодо врахування впливу таких інструментів на систему (наприклад, переміщення потенційних цифрових доказів, контент пам'яті, яка під час завантаження програмного забезпечення змінює нумерацію сторінок, тощо). Усі виконані дії та отримані зміни, зроблені в потенційних цифрових доказах, має бути задокументовано та зрозуміло. Якщо неможливо визначити подібні впливи на систему задіяних інструментів або зміни, що є результатом дій, не може бути визначено однозначно, це також має бути задокументовано.
– Під час здобуття несталих даних DEFR повинен адаптувати використання логічного файлового контейнера, де це можливо, та задокументувати їхні геш-значення, коли контейнер містить файл(и) несталих даних. Там, де це неможливо, потрібно використовувати контейнер, такий як ZIP-файл; потім для цього файла має бути обчислено геш-значення і це значення задокументовано. Отриманий файловий контейнер має зберігатися на носії для збереження цифрових даних, підготований для цієї цілі, тобто відформатований.
– Застосувати процес створення образу наживо для сталого збереження з використанням затверджених інструментів створення образу. Отримана копія цифрового доказу має зберігатися на носії для збереження цифрових даних, підготованого для цієї цілі. Краще використовувати нові

носії для збереження цифрових даних, застосування копій цифрових доказів від затверджених процесів гарантує цілісність даних під час реконструкції. Тому очищені носії для збереження цифрових даних будуть недоречними. Якщо образ збережено в логічному файловому контейнері, DEFR повинен гарантувати, що цей образ не може бути зіпсованим або пошкодженим.

Примітка. Якщо пристрій заблоковано, фізичний доступ може здійснюватися за допомогою інших засобів, які мають змогу прямого доступу, наприклад, Firewire інтерфейс.

7.1.3.1.3. Додаткові дії: здобуття потенційних цифрових доказів на ввімкнених цифрових пристроях. Такі дії є додатковими діями, які є доречними для здобуття потенційних цифрових доказів на ввімкнених цифрових пристроях залежно від конфігурації специфічного цифрового пристрою:

- Розглянути здобуття несталих даних з RAM, якщо підозрюють наявність шифрування. З початку перевіряють, чи дійсно це саме такий випадок, за допомогою перевірення необробленого диска чи за допомогою деяких утиліт для пошуку зашифрованої інформації. Якщо це саме такий випадок, треба враховувати, що працююча основна операційна система може бути ненадійною та треба розглянути використання відповідних надійних та затверджених інструментів.
- Використовувати надійне джерело часу та документувати час кожної здійсненої дії.
- Може бути доречним об'єднати DEFR зі здобутими потенційними цифровими доказами за допомогою цифрових підписів, біометрії та фотографії.

Примітка 1. Натискання клавіші живлення на цифровому пристрої може бути сконфігуровано так, що буде запущено скрипт, який може змінювати інформацію або віддаляти інформацію із системи перед перезавантаженням або надавати засторогу

приєднаній системі, що виявлено несподівану ситуацію, яка може призвести до стирання даних, що мають доказове значення перед тим, як їх ідентифіковано. Пристрій може бути також сконфігуровано в такий спосіб, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншим присутнім особам

7.1.3.2. Вимкнені цифрові пристрої

7.1.3.2.1. Загальні положення. Легше обробляти вимкнені цифрові пристрої, ніж увімкнені цифрові прилади, оскільки нема потреби здобуття несталих даних. На рисунку 5 зображено дії, які може бути застосовано для здобуття потенційних цифрових доказів з вимкнених цифрових приладів.

7.1.3.2.2. Здобуття з вимкнених цифрових пристроїв. Такі дії є діями зі здобуття потенційних цифрових доказів, якщо цифрові пристрої вимкнено:

- Упевнитися, що пристрій дійсно вимкнений.
- Якщо потрібно, вилучити носій із вимкненого цифрового пристрою, якщо цього ще не було зроблено. Розмістити позначку на носії, як підозрілому носії, та задокументувати всі деталі, такі як тип, назва моделі, серійний номер та розмір носія.
- Створити образ за допомогою затверджених інструментів створення образу для формування копії цифрових доказів з підозрілого диску.

Примітка. Здебільшого носій не вилучається із цифрового пристрою, доки виконується здобуття потенційних цифрових доказів, оскільки його вилучення збільшує ризик пошкодження або плутанини його з іншими носіями для збереження даних. Має бути розроблено та запроваджено локальні процедури стосовно потреби вилучення носія для збереження із цифрових пристроїв.

7.1.3.3. Критичні цифрові пристрої

У деяких випадках цифрові пристрої не може бути вимкнено через критичну природу в системах. Це системи, такі як сервери в дата-центрах, які також надають послуги невинним клієнтам, системи життєзабезпечення, медичні системи та багато інших, які можуть надати критичний вплив, якщо вони перервуть

роботу чи їх буде вимкнено. Треба бути особливо обережними під час роботи з такими системами.

Якщо цифровий пристрій не може бути вимкнено, виконують здобуття наживо та/або часткове здобуття потенційних цифрових доказів, як описано в 7.1.3.1.2 та 7.1.3.4.

7.1.3.4. Часткове здобуття

Часткове здобуття може здійснюватися внаслідок кількох причин, таких як:

- системне сховище є дуже великим, щоб бути здобутим (наприклад, сервер баз даних);
- система є дуже критичною, щоб бути вимкненою;
- якщо вибрані дані, що мають бути здобутими, містять інші недоречні дані в середині тої самої системи; або
- якщо законодавчі обмеження повноважень, такі як судове розпорядження на розслідування, яке обмежує сферу застосування здобуття.

Якщо прийнято рішення щодо здійснення часткового здобуття, дії з такого здобуття охоплюють, але не обмежуються, такими:

- Ідентифікувати папку(-и), файл(и) чи будь-які доречні власні системні опції, доступні для здобуття бажаних даних.
- Виконати логічне здобуття цих ідентифікованих даних.

7.1.3.5. Носії для збереження цифрових даних

На місці інциденту може бути знайдено різні типи носіїв для збереження цифрових даних. Зазвичай є найменш несталі типи даних та вони можуть мати найнижчий пріоритет протягом збирання та здобуття. Це не означає, що вони є неважливими, оскільки в багатьох випадках зовнішні носії для збереження цифрових даних містять докази, досліджувані аналітиками. DEFR повинен гарантувати таке:

- Перевірити та задокументувати місце (наприклад, відсік дисководів, кабелі та конвектори, USB-слоти тощо) виробника, модель та серійних номер (якщо є) для кожного знайденого носія для збереження цифрових даних.

- Прийняти рішення чи збирати ідентифіковані носії для збереження цифрових даних або виконати здобуття на місці; рішення має бути прийнято на основі природи інциденту та доступних ресурсів. Для виконання здобуття потенційних цифрових доказів (з основного жорсткого диска) на місці, див. рисунок 3.
- Якщо DEFR прийняв рішення та має дозвіл збирати носії для збереження цифрових даних, зібрані носії має бути запаковано або розміщено у відповідному пакуванні.
- Нанести позначки на носії для збереження цифрових даних та будь-які пов'язані з ним частини. Позначки доказів не повинно бути розміщено безпосередньо на механічних частинах носія для збереження цифрових даних, не повинні закривати або маскувати важливу інформацію, таку як серійний номер, номер моделі та номери частин. Усі зібрані носії має бути здобуто та збережено так, щоб гарантувати цілісність зібраних носіїв. Якщо можливі докази має бути запаковано за допомогою пломб, що порушуються від втручання, тоді DERF або задіяний персонал, повинні підписати ці позначки.
- Зібрані носії для збереження цифрових даних потрібно зберігати в середовищі, прийнятному для збереження даних.
- DEFR повинен бути обізнаним стосовно допустимого максимального періоду часу, визначеному відповідним законодавством, стосовно можливості збереження даних на носії для збереження цифрових даних.

7.1.4. Збереження

Після завершення процесу здобуття DEFR повинен запечатати здобуті дані з використанням функцій верифікації або цифрових підписів для визначення того, що цифрові копії еквівалентні оригіналам. Додатково, аспекти безпеки потребують застосування засобів безпеки, які здійснюють збереження конфіденційності, цілісності та надійності потенційних цифрових

доказів. Для захисту від псування, властивості середовища відповідати належним вимогам. DEFR потребує гарантування такого:

- Використання відповідних функцій верифікації, щоб надавати докази, скопійовані файли еквівалентні оригіналам.
- Може бути доречним об'єднати DEFR зі здобутими потенційними цифровими доказами за допомогою цифрових підписів, біометрії та фотографії.

Усі зібрані цифрові прилади має бути належно збережено. Різні типи потенційних цифрових доказів можуть потребувати різних методів збереження. Потенційні цифрові докази необхідно зберігати протягом їхнього часу життя, який може змінюватися в різних юрисдикціях та організаційних політиках.

Примітка. Як альтернатива опечатування здобутих даних із затвердженими функціями верифікації або цифровими підписами, DEFR також може використовувати біометричні дані. Біометрія використовує фізичні характеристики та особливості поведінки для визначення ідентифікації особи. Якщо біометричні дані долучено до здобутих потенційних цифрових доказів, можна гарантувати, доказ не може бути скомпрометованим без компрометації біометричних даних.

7.2. Мережеві пристрої

7.2.1. Ідентифікація

7.2.1.1. Загальні положення

У контексті цього розділу мережеві пристрої розглядають як комп'ютери або інші цифрові пристрої, підключені до мережі в дротовому чи бездротовому режимі. Такі мережеві прилади можуть охоплювати мейнфрейми, сервери, настільні комп'ютери, комутатори, концентратори, маршрутизатори, мобільні прилади, PDA, PED, Bluetooth прилади, CCTV системи тощо. Зазначимо, що якщо цифровий пристрій підключено до мережі, важно визначити, де саме потенційні цифрові докази, які необхідно розглянути, зберігаються. Ці дані може бути розміщено будь-де в мережі.

Ідентифікація цифрових пристроїв містить компоненти, такі як логотипи виробника, серійні номери, шини й адаптери живлення. DEFR може розглянуті такі аспекти, як засоби ідентифікації:

- Характеристики пристрою: Модель та виробник цифрового пристрою іноді може бути ідентифікований за його видимими характеристиками, особливо якщо є унікальний дизайн елементів.
- Інтерфейс пристрою: Конектор живлення часто є специфічним для виробника та може надавати допомогу в ідентифікації.
- Позначки пристрою: Для вимкнених мобільних пристроїв може бути доречною інформація, отримана із середини порожнини блока батареї, особливо коли її пов'язано з відповідними базами даних. Наприклад, IMEI є номером з 15 цифр, який показує виробника, тип моделі та країну затвердження для GSM-пристроїв; ESN – це унікальний 32-бітний ідентифікатор, задокументований на безпечному чипі в мобільному телефоні виробником – перші 8...14 біт ідентифікують виробника та решткі бітів ідентифікують приписаний серійний номер.
- Зворотний пошук: У разі мобільних телефонів, якщо телефонний номер цього телефону відомий, зворотний пошук може бути використано для ідентифікації мережевого оператора.

Завдяки загальним малим розмірам мобільних пристроїв DEFR повинен бути особливо обережним під час ідентифікації всіх типів мобільних пристроїв, які можуть бути причетними в цьому разі. DEFR повинен убезпечити місце інциденту та гарантувати, що ніхто з осіб не виніс мобільні та будь-які інші цифрові пристрої з місця інциденту. Цифрові пристрої, які можуть містити цифрові докази, має бути захищено від несанкціонованого доступу.

Примітка. У деяких випадках комунікація не повинна перериватися. Треба поінформувати авторизованих осіб щодо можливих проблем (наприклад, попередити невідомих осіб стосовно вимкнення пристроїв).

7.2.1.2. Дослідження та документування фізичного місця інциденту

Перед тим, як може бути зроблено здобуття чи збирання, місце інциденту має бути задокументовано візуальним способом за допомогою фотографування, відеозйомки або схематичного зображення місця, яким воно було на вході. Метод документування потребує збалансування обставин, вартості, часу, наявних ресурсів та пріоритетів. DEFR повинен задокументувати всі інші елементи на місці інциденту, які можуть містити потенційно доречні матеріали, такі як короткі записки, стикери, щоденники тощо.

- DEFR повинен задокументувати типи, бренди, моделі та серійні номери будь-яких використовуваних пристроїв та ідентифікувати всі цифрові прилади, які можуть потребувати здобуття потенційних цифрових доказів і збирання, на цій початковій стадії. Усі мобільні пристрої та їхні відповідні елементи, такі як карти пам'яті, SIM-карти, зарядні пристрої та шини, знайдені на цьому місці, їхні відповідні серійні номери та будь-які ідентифікаційні особливості має бути задокументовано та зібрано, якщо потрібно. Постаратися також знайти оригінальне паковання мобільних телефонів; вона може містити нотатки з PIN та PUK-кодами.
- Якщо пристрій є мережевим, DEFR повинен ідентифікувати послуги, що надаються цими пристроями, для розуміння залежності та визначення критичності цього пристрою в середині мережі перед тим, як прийняти рішення стосовно відключення цього пристрою від мережі. Це є важливим, якщо цей пристрій надає послуги з критичних функцій, що не можуть бути терпимими до будь-яких відключень або для уникнення пошкодження потенційних цифрових доказів. Однак, якщо виявляється змога здійснення мережевих загроз цьому пристрою, DEFR може потребувати прийняття рішення стосовно відключення

цього пристрою від мережі для захисту потенційних цифрових доказів.

- Якщо мережевим пристроєм є CCTV-система, DEFR повинен записати номери камер, підключених до системи, а також те, які із цих камер дійсно працюють. DEFR повинен також записати тип моделі, модель та основні установки системи, такі як установки дисплея, установки поточного запису та розміщення місця збереження інформації так, щоб полегшити процес збирання та здобуття в разі, якщо зміни має бути зроблено; це потім надасть можливість повернути систему до первісного стану.
- Статус цифрових пристроїв має залишатися таким, який він є. Зазвичай, цифрові пристрої вимкнені, DEFR не повинен їх вмикати та, якщо їх увімкнено, DEFR не повинен їх вимикати. Це може запобігти небажаному псуванню цифрових доказів. Пристрій, який має батареї, що можуть розрядитися, потребують зарядження для гарантування того, що інформацію не буде втрачено. DEFR повинен ідентифікувати потенційні зарядні пристрої та кабелі протягом цієї стадії. Якщо пристрій буде транспортуватися та перевірятися в деяку невизначену дату, може бути доречним вимкнути його для мінімізації можливості пошкодження даних, які містяться в цьому пристрої.
- DEFR повинен також розглянути використання детектора бездротових сигналів для виявлення та ідентифікації бездротових сигналів від бездротових пристроїв, що можуть бути прихованими. Можуть бути обставини, коли детектор бездротових сигналів не використовують через вартості та обмежень часу, та DEFR повинен задокументувати цей факт.

7.2.2. Збирання, здобуття та збереження

7.2.2.1. Загальні положення

DEFR повинен прийняти рішення, чи збирати або здобувати потенційні цифрові докази від цифрових пристроїв. Якщо

DEFR прийняв рішення стосовно відключення пристроїв, процес збирання або здобуття потенційних цифрових доказів буде виконано, як описано в 5.4. Якщо пристрої не може бути відключено від мережі через критичність їх функцій або ймовірності порушення потенційних цифрових доказів, DEFR повинен виконати здобуття наживо, доки пристрої залишаються підключеними до мережі.

Примітка. Критично важливо мати чинні, стандартні процедури, які використовують затверджені інструменти, разом із прийнятною документацією та DEFR, який пройшов навчання та має відповідний досвід.

Збирання та здобуття потенційних цифрових доказів від мережевих мобільних пристроїв ускладнено, оскільки вони можуть бути в багатьох станах та режимах взаємодії, таких як Bluetooth, радіочастотному, сенсорному та інфрачервоному. Додатково, різні виробники мобільних пристроїв використовують різні типи операційних систем, які потребують різних методів здобуття доказів. Є також широкий діапазон карт пам'яті, використовуваних у мобільних пристроях, та видалення цих карт пам'яті з увімкнених мобільних пристроїв може взаємодіяти із запущеними процесами.

Зазвичай, мобільні пристрої, такі як PDA та мобільні телефони мають бути увімкненими, щоб здобути потенційні цифрові докази. Ці пристрої можуть безперервно змінювати своє операційне середовище, коли їх увімкнено, наприклад, може бути оновленим час. Пов'язаною проблемою є те, що дві копії цифрових доказів одного й того самого пристрою можуть не пройти стандартні функції верифікації, такі як розрахунок геш. У такій ситуації може бути застосовано альтернативні функції верифікації, які ідентифікують елементи співпадіння та різниці.

Важливо, щоб DEFR не вносив Wi-Fi та Bluetooth пристрої на місце розслідувань, які можуть змінювати подібну інформацію на пристроях з потенційними доказами. Це має особливу

важливість, якщо дослідникам необхідно знати, які прилади були підключеними до мережі.

Якщо DEFR прийняв рішення застосовувати процес здобуття, мережеві пристрої мають залишатися працюючими для подальшого аналізування для визначення інших пристроїв, підключених до цього мережевого пристрою. DEFR повинен розглянути можливість саботажу через активні мережеві з'єднання та прийняти рішення моніторити систему або відключитися.

7.2.2.2. Настанови для збирання мережевих пристроїв

У деяких обставинах може бути доцільним залишити мережеві пристрої підключеними до мережі, так щоб DEFR бо DES з відповідними правами змогли моніторити та документувати їхню активність. Якщо такої потреби немає, пристрої мають збиратися, як описано нижче:

- DEFR повинен ізолювати пристрій від мережі, коли відомо, що потрібні дані буде перезаписано за допомогою таких дії та це не призведе до неправильного функціонування важливих систем (таких як системи керування обладнанням у госпіталях). Це може бути зроблено за допомогою відключення дротових мережевих з'єднань до телефонних систем або мережевих портів або зробити неможливим з'єднання з точкою бездротового доступу.
- Перед відключенням від дротових мереж DEFR повинен відстежувати підключення до цифрових пристроїв та позначити порти для подальшої реконструкції мережі в цілому. Пристрій може мати більше ніж один метод комунікацій. Наприклад, комп'ютер може мати дротове підключення до LAN, бездротовий модем та карти мобільного телефона. PED може бути підключено до мережі через Wi-Fi, Bluetooth з'єднання або з'єднання через мобільну телефонну мережу. DEFR повинен спробувати ідентифікувати всі методи комунікацій та застосувати відповідні дії для захисту від пошкоджень потенційних цифрових доказів.

- Треба бути обережним, оскільки видалення живлення від мережевих пристроїв у цьому місці може пошкодити несталі дані, такі як працюючі процеси, мережеві з'єднання та дані, що зберігаються в пам'яті. Основна операційна система може бути ненадійною та надавати фальшиву інформацію. DEFR повинен захопити цю інформацію за допомогою довірчих затверджених методів перед відключенням живлення від пристроїв. Якщо DEFR є впевненим, що потенційні цифрових доказів не буде втрачено в результаті, з'єднання від цього цифрового пристрою може бути видалено.
- Якщо збирання має переваги над здобуттям та відомо, що пристрій містить несталу пам'ять, пристрій має бути безперервно підключеним до живлення.
- Якщо мобільний пристрій вимкнено, обережно запакувати, запечатати та надайте позначки. Це надасть змогу уникнути випадкових або навмисних операцій з ключами або клавішами. Як додаткову передбачливість, DEFR повинен також розглянути використання пакування Фарадея або екранувальний бокс.
- У деяких обставинах мобільний пристрій має бути вимкнено протягом збирання для запобігання зміненню даних. Це може бути через вихідні або вхідні з'єднання або команди, які можуть спричинити пошкодження потенційних цифрових доказів.
- Пізніше кожен цифровий пристрій може бути оброблено як окремий пристрій (див. 7.1) протягом його досліджень.

Примітка. Можливо запровадити вид мережі з використанням пересувного пристрою для збереження як транзитне середовище. DEFR повинен розглянути, чи можна зібраний пристрій використовувати так та шукати інформацію стосовно інших пристроїв у такому таємничому стані.

7.2.2.3. Настанови для здобуття з мережевих пристроїв

Якщо цифрові пристрої підключено до мережі, є змога ці прилади підключити до більше ніж однієї (1) фізичної або віртуальної мережі. Наприклад, пристрій, який, як здається, підключено до однієї (1) видимої фізичної мережі, може фактично працювати у віртуальній приватній мережі (VPN) та з віртуальною машиною з більше ніж однією (1) IP-адресою. У такому разі перед відключенням цього пристрою від мережі, DEFR повинен виконати логічне здобуття даних, пов'язаних із логічним мережевим з'єднанням (наприклад, інтернет-сполучення). Ці пов'язані дані охоплюють, але не обмежуються, IP-конфігурацію та таблиці маршрутизації.

Для мережевих пристроїв, які потребують безперервного увімкненого живлення, пристрій має бути захищено від взаємодії з бездротовими радіомережами, охоплюючи пристрої із GPS. DEFR повинен користуватися методами, дозволеними локальним законодавством, для ізоляції радіосигналів. Однак треба бути обережним для гарантування того, що пристрій має відповідне джерело живлення, оскільки методи ізоляції можуть призвести до використання додаткової енергії за спроб підключення до мережі. Методи ізоляції можуть охоплювати, але не обмежуватися, такі:

– Використання пристроїв блокування, які можуть заблокувати передачу за допомогою створення сильної інтерференції, коли пристрій випромінює сигнали в тому самому діапазоні частот, які використовують мобільні пристрої.

Примітка 1. Використання пристроїв блокування може порушувати законодавчі вимоги в деяких юрисдикціях.

Примітка 2. Використання пристроїв блокування може негативно впливати на поведінку електронних приладів, таких як медичне обладнання.

– Використання екранованих робочих місць для здійснення перевірянь безпечно на фіксованому місці. Екранування

може бути зроблено для повного робочого місця або за допомогою встановлення тента Фарадея, який дає змогу зробити це портативно. Кабелі живлення в цьому тенті є проблематичними, однак, оскільки без належної ізоляції вони можуть діяти як антена, скасовуючи цілі тента. Робоче місце може бути також дуже обмежувальним.

– Використання екранованих робочих місць для здійснення перевірянь безпечно у фіксованому місце. Радіочастотне екранування робочого простору або контейнера (контейнер Фарадея) може бути використано для уникнення з'єднань з мережею.

Примітка 3. Усі методи блокування бездротового доступу до мереж має бути затверджено для використання на відповідних частотах. Таке затвердження має також розповсюджуватися на кабелі, які проходять через екранування.

– Використання замінника (U)SIM, який імітує ідентифікацію оригінального приладу та попереджує доступ мережі до цього пристрою. Такі карти мають змогу обдурювати цей пристрій в прийманні його за оригінальний (U)SIM та дозволяти, щоб перевіряння відбувалися безпечно в будь-якому місці. (U)SIM має бути затвердженим для цього пристрою та мережі перед його користуванням.
– Заблокувати послуги мережі за допомогою домовленості з оператором мобільних послуг та ідентифікації деталей послуг, що будуть заблоковані (наприклад, ідентифікація обладнання, ідентифікація передплатника чи номер телефону). Однак така інформація не завжди легкодоступна, коли процес координації та підтвердження може заподіяти затримування.

DEFR може здійснити здобуття наживо для мобільного пристрою перед тим, як вилучити батарею (наприклад, за допомогою доступу до SIM-карти). Це може бути зроблено для уникнення втрати потенційно важливої інформації в RAM телефону або для прискорення процесу перевірення (наприклад,

там, де вважають, що пристрій може бути захищено PIN та/або PUK, що потребує значного часу для їхнього отримання).

Примітка 4. DEFR повинен гарантувати, що збирання та здобуття потенційних цифрових доказів відповідає локальним законам та нормативним документам, що потребує врахування конкретних обставин.

7.2.2.4. Настанови для збереження мережевих пристроїв

З урахуванням природи цифрових пристроїв та потенційних цифрових доказів, настанови для збереження мережевих пристроїв подібні збереженню комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних. Див. 7.1.4 для докладної настанови стосовно збереження пристроїв.

7.3. Збирання, здобуття та збереження для CCTV

DEFR повинен розуміти, що підхід до вилучення відеопослідовностей з комп'ютера, вбудованого до DRV CCTV-системи, відрізняється від вилучення звичайного здобуття цифрових доказів з комп'ютера. Нижче наведено специфічні настанови для здобуття потенційних цифрових доказів із CCTV-систем:

- Перед початком процесу здобуття DEFR повинен з початку визначити, чи задокументувала система відеопослідовність, що викликає інтерес. Потім DEFR повинен визначити фрагмент часу потрібного відеоматеріалу та порівняти системний час із правильним часом та записати будь-які відмінності. DEFR повинен також визначити, які камери потрібні, та чи може здійснити процес здобуття окремо з кожної камери. DEFR повинен записати тип та модель системи. Ця інформація може бути потрібною, щоб визначити правильну відповідь програмного забезпечення.
- DEFR повинен здобути всі записи всіх доречних камер протягом часу, який зумовлює інтерес, для збереження інформації, яку буде додатково досліджено пізніше. DEFR

повинен записати всі камери, підключені до системи та визначити, чи дійсно вони вели записи або не вели записів.

DEFR повинен визначити розмір носія для збереження цифрових даних, а також коли система повинна за процедурою перезаписувати відеоінформацію.

Ця інформація буде надавати DEFR знання того, як довго ця відеопослідовність буде залишатися в системі перед тим, як її буде втрачено. Цю дію має бути зроблено для гарантування того, що доказ не було змінено. Для цифрових відеодоказів захист записів має бути зроблено на місці.

– Є кілька опцій, які DEFR може вибрати для здобуття потенційних цифрових доказів від CCTV-систем:
  1) Здобути відеофайли за допомогою запису їх на CD/DVD/Blu-ray диск, але це може бути непрактичним, якщо відеофайли занадто великі.
  2) Здобути відеофайли за допомогою запису їх на зовнішній носій для збереження цифрових даних.
  3) Здобути відеофайли через мережеве з'єднання. Це може бути зроблено, якщо CCTV-систему обладнано мережевим портом.
  4) Застосувати здатність CCTV-системи до експорту відеофайлів в інші формати (зазвичай MPEG або AVI), які є стиснутою версією відеопослідовності. Це може бути використано тільки як останню спробу, оскільки відновлення зі стиснутого стану може змінити оригінальні дані та завжди вилучає деталі зображення. Не рекомендовано залучати відновлені дані для перевіряння, якщо є оригінальні дані та вони доступні для аналізування.

Примітка 1. Якість вилученої відеопослідовності може бути не такою гарною, як якість оригіналу.

  5) Там ще неможливе пряме здобуття цифрових доказів за допомогою копіювання файлів на записувальному пристрої, DEFR та DES повинні спробувати здобути

аналогові копії з аналогового виходу, який є на оригінальному пристрої, що здійснив запис з використанням доречних аналогових пристроїв для запису.

- Протягом комплектації здобуття, здобуті файли мають бути перевірені для підтвердження того, що були здобуті правильні файли або частини файлів. Файли мають бути також перевірені за допомогою програмного забезпечення програвача (для форматів файлів цифрових пристроїв) для можливості їхнього програвання на інших системах – більшість CCTV систем є унікальними та файли не можуть бути обов'язково програватися з використанням іншого програмного забезпечення програвача. Правильне програмне забезпечення для програвання може бути доступним для завантаження із CCTV-системи разом із даними.
- Носій для збереження цифрових даних, який містить здобуті файли, має оброблятися як майстер-копія цифрових доказів. Якщо файли завантажено на ноутбук або карту пам'яті/USB пристрій, тоді постійну майстер-копію має бути зроблено із цих пристроїв якнайшвидше.
- Потім DEFR повинен перезавантажити CCTV-систему, якщо її вимкнено. Це має бути зроблено в присутності авторизованих осіб.

Якщо непрактично виконувати здобуття на місці, DEFR може прийняти рішення стосовно збирання носіїв для збереження цифрових даних. Швидким методом є заміна жорсткого диска CCTV-системи на порожній диск або клон жорсткого диска. Однак DEFR повинен оцінити серйозні ризики перед застосуванням цього методу, такі як сумісність нових дисководів жорстких дисків із системою та сумісність вилученого дисководу жорсткого диска з іншими системами для досліджень.

Примітка 2. Деякі системи мають пересувний дисковод жорсткого диска в кеді, але такий дисковод може потребувати обладнання системи для програвання.

Якщо жоден із наведених вище методів є неможливим, тоді CCTV-систему в цілому має бути вилучено в місця інциденту та процес здобуття має бути виконано в судовій лабораторії. Це буде останньою спробою та припущенням для DEFR, що це фізично можливо зробити, оскільки деякі CCTV-системи є дуже великі та складні. Знову DEFR повинен оцінити ризики стосовно законодавчого прийняття та гарантії перед вилученням системи.

З урахуванням походження цифрових пристроїв та потенційних цифрових доказів, настанови для збереження CCTV-системи подібні збереженню комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних. Див. 7.1.4 для докладної настанови стосовно збереження пристроїв.

МІНІМАЛЬНІ ВИМОГИ ДО ПЕРЕМІЩЕННЯ ДОКАЗІВ

DEFR повинен відповідати за здобуті дані та цифрові пристрої протягом усього часу, коли вони знаходяться під його захистом. Для підтримання цього контролювання DEFR повинен бути відповідно авторизований, навчений та кваліфікований. Однак, оскільки локальні закони є визначним чинником у змозі DEFR відповідати всім трьом очікуваним вимогам, компетенція DEFR може змінюватися від одної юрисдикції до іншої. Це може призвести до того, що вимоги до документації для переміщення цифрових доказів між юрисдикціями не будуть однаковими в різних юрисдикціях.

Відповідно, потрібно визначити мінімальний набір вимог до документації для забезпечення обміну потенційними цифровими доказами між юрисдикціями. Ці вимоги до документації необхідно розглядати стосовно наведених у розділі 6.6. Оскільки цей стандарт не замінює специфічних вимог законодавства в будь-якій юрисдикції, він залишається практичною настановою для переміщення потенційних цифрових доказів скрізь кордони юрисдикцій.

Примітка 1. Мінімальна документація для комунікації складається з: доречних імен та адрес відповідних органів; стан

авторизації, навчання та кваліфікації DEFR; цілі перевірення; того, які дії виконано; хто робив це та коли; хронологічне документування, яке стосується специфічного розслідування; описовий перелік потенційних цифрових доказів та носіїв для збереження цифрових даних, які було зібрано та здобуто; та інформація стосовно будь-яких перевірень, тестів або досліджень, застосованих для створення копій доказів. Специфічні вимоги юрисдикції можуть охоплювати таке: якщо докази розглядають як думку експерта, підтвердження відповідного Expert Witness Code of Conduct; та ордер суду, де визначено, яку документацію потрібно перемістити та причини для цього переміщення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08. Київ, 2002. 246 с.

Алєксєєва-Процюк Д. О., Брисковська О. М. Особливості проведення тимчасового доступу до речей та документів для отримання інформації від операторів мобільного зв'язку. *Митна справа*. 2013. № 1. С. 58–65.

Бабанін С. В. Кіберзлочинність, Комп'ютерна злочинність. *Велика українська юридична енциклопедія* : у 20 т. Харків, 2019. Том 18. 544 с.

Багрій М. В., Луцик В. В. Негласні слідчі (розшукові) дії у кримінальному провадженні : монографія. Тернопіль, 2014. 308 с.

Багрій М. В., Луцик В. В. Процесуальні аспекти негласного отримання інформації : вітчизняний та зарубіжний досвід : монографія. Харків : Право, 2017. 376 с.

Безпека дітей в Інтернеті. URL : https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti

Берназюк О. О. Цифрові технології у праві: тенденції та перспективи розвитку : дис. ... д-ра юрид. наук: 12.00.07. Ужгород, 2021. 541 с.

Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посібник. Київ : Українська академія внутрішніх справ, 1994. 71 с.

Білєнький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняль-

но-правове дослідження) : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2016. 20 с.

Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посібник / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія]. Київ : КИТ, 2010. 407 с.

Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : автореф. дис. ... канд. юрид. наук: 12.00.01 – Теорія та історія держави і права; історія політичних і правових учень. Івано-Франківськ, 2018. 25 с.

Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2 (10–11). С. 276–282.

Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рекомендації / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

Використання можливостей операторів стільникового (мобільного) зв'язку для розкриття та розслідування злочинів [Текст] : метод. рекомендації / [Чернявський С. С., Татаров О. Ю., Алексеєва-Процюк Д. О. та ін.]. Київ : Нац. акад. внутр. справ, 2012. 58 с.

Воронов І. О. Організаційно-тактичні основи протидії злочинам у сфері високих інформаційних технологій : монографія. Одеса : ОДУВС. 2010. 216 с.

Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2000. С. 50–53.

Гаркуша А., Каланча І. Як вилучати електронні носії інформації під час обшуку з користю для слідства і без шкоди для бізнесу. алгоритм прийняття рішень. URL : https://justtalk.com.ua/post/yak-viluchati-elektronni-nosii-informatsii-pid-chas-obshuku-z-koristyu-dlya-slidstva-i-bez-shkodi-dlya-biznesu-algoritm-prijnyattya-rishen

Головкін Б. М. Види злочинності. *Журнал східноєвропейського права*. 2015. №. 18. С. 14–21. URL : http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf

Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. 250 с.

Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. … канд. юрид. наук.: спец. 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність Київ, 2013. 20 с.

Гребенькова М. С. Актуальні проблеми електронних відображень у соціальних мережах як джерела доказів у кримінальному провадженні. *Право і суспільство*. 2021. № 6. С. 251–257.

Грошевий Ю. М., Стахівський С. М. Докази і доказування у кримінальному процесі: наук.-практ. посібник. Київ : КНТ, 2006. 272 с.

Давидюк П. П., Кубай І. Ю. Висунення і перевірка слідчих версій про цифрове алібі підозрюваного (обвинуваченого). *Молодий вчений.* 2017. № 5.1 (45.1). С. 29–32. URL : http://molodyvcheny.in.ua/files/journal/2017/5.1/7.pdf.

Денькович О. І. Поняття кіберзлочину у зарубіжній кримінології. Проблеми державотворення і захисту прав людини в Україні : матеріали XXIII звітної науково-практичної конференції (7–8 лютого 2017 р.) : у 2 ч. Ч. 2. Львів : Юридичний факультет Львівського національного університету імені Івана Франка, 2017. С. 130–133.

Діордіца І. В. Поняття та зміст кіберзлочинності. URL : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/

Дохід від кіберзлочинів в одинадцять разів перевищує витрати на безпеку. URL : https://cybercalm.org/novyny/dohid-vid-kiberzlochyniv-v-odynadtsyat-raziv-perevyshhuye-vytraty-na-bezpeku/

Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ, 2014. 328 с.

Єськов С. В. Аудіо-, відеоконтроль особи як різновид втручання у приватне спілкування : системно-структурний аналіз. URL : www.corp-lguvd.lg.ua/d130203.html

За рік карантину кількість українців у соцмережах зросла на сім мільйонів. URL : https://www.dw.com/uk/za-rik-karantynu-kilkist-ukraintsiv-u-sotsmerezhakh-zrosla-na-sim-milioniv/a-56899697

Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL : https://www.npu.gov.ua/assets/userfiles/files/zvity/zvit_NPU_2019.pdf

Інформаційне право та правова інформатика : курс лекцій / [В. Г. Хахановський, І. В. Мартиненко, В. М. Смаглюк та ін.] ; за заг. ред. Є. М. Моісеєва. Київ : Київ. нац. ун-т внутр. справ, 2007. 253 с.

Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1. С. 140–144.

Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посібник. Київ : Атіка, 2010. 168 с.

Кіберполіція викрила шахраїв, що за допомогою СМС-розсилки ошукували громадян. URL : https://cyberpolice.gov.ua/

news/kiberpolicziya-vykryla-shaxrayiv-shho-za-dopomogoyu-sms-rozsylky-oshukuvaly-gromadyan-foto-2963

Кількість користувачів Інтернету у світі сягнула 4,66 млрд. URL : https://root-nation.com/ua/news-ua/it-news-ua/ua-new-internet-records/#lwptoc

Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посібник. Львів : Львівський державний університет внутрішніх справ, 2022. С. 36–37.

Ключові представники суб'єктів національної системи кібербезпеки України обговорили організаційно-технічну модель кіберзахисту. URL : https://cip.gov.ua/ua/news/klyuchovi-predstavniki-sub-yektiv-nacionalnoyi-sistemi-kiberbezpeki-ukrayini-obgovorili-organizaciino-tekhnichnu-model-kiberzakhistu

Конвенція про кіберзлочинність від 23.11.2001. URL : http://zakon0.rada.gov.ua

Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки: схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

Кормич Б. А. Інформаційне право : підручник. Харків, 2011. 334 с.

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

Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 155–166. URL : http://dspace.univd.edu.ua/xmlui/handle/123456789/3848

Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків, 2016. 212 с.

Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка,

О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.

Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін. ; за заг. ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.

Кримінальний процесуальний кодекс України : наук.-практ. коментар / за заг. ред. професорів В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. Київ : Юстініан, 2012. 1223 с.

Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т. 1 / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків : Право, 2012. 767 с.

Куц В. Поняття злочинності. *Науковий часопис Національної академії прокуратури України*. 2016. № 2 С. 34–39. URL : http://www.chasopysnapu.gp.gov.ua/ua/pdf/10-2016/02/kuts.pdf

Лисенко В. В., Лисенко О. В. Проблеми використання у кримінальному судочинстві інформації, що містить у електронному вигляді. *Напрями удосконалення протидії правопорушенням у сфері господарської діяльності* : зб. наук. праць за матеріалами міжнар. наук.-практ. конф., (Київ, 26–27 лист. 2010 р.). Київ, 2010. С. 243–249.

Лисюк Ю. В. Аудіо-, відеоконтроль як різновид втручання у приватне спілкування під час здійснення негласних слідчих дій у кримінальному провадженні. *Науковий вісник Херсонського державного університету.* 2014. Вип. 6-1. Т. 4. С. 77–78.

Литвинов М. Ю. Понятие компьютерных средств и определение направлений их использования в ОРД. *Вісник ЛДУВС*. 2008. Спец. вип. 4, ч. 1. С. 114–127.

Марущак А. І. Інформаційне право: доступ до інформації : навч. посібник. Київ, 2007. 531 с.

Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104–110.

Мещеряков В. О. Основи методики розслідування злочинів в сфері комп'ютерної інформації : автореф. дис. … д-ра юрид. наук : спец. 12.00.09. Воронеж, 2001. 30 с.

Негласні слідчі (розшукові дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні : навч.-практ. посібник [Текст] / Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Харків : Оберіг, 2015. 424 с.

Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навчально-практичний посібник / Б. І Бараненко, О. В. Бочковий, К. А. Гусєва та ін. ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. 416 с.

Никифорчук Д. Й. До питання використання результатів оперативно-розшукової діяльності у кримінальному судочинстві. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. Вип. 22. С. 61–66.

Оперативно-розшукова компаративістика : монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. Харків : Золота миля, 2013. 352 с.

Основи кібергігієни. URL : https://osvita.diia.gov.ua/courses/cyber-hygiene

Острушко О. В. Організаційні аспекти методики розслідування злочинів у сфері комп'ютерної інформації : автореф. дис. … канд. юрид. наук : спец. 12.00.09. Волгоград, 2000. 15 с.

Правила надання та отримання телекомунікаційних послуг, затверджених постановою Кабінету Міністрів України № 295 від 11 квітня 2012 р.: [із змінами і доповненнями на 08.04.2013] *Офіційний вісник України*. 2012. № 29. Ст. 1074.

Підсумки 2018 року в цифрах. Кіберполіція. Національна поліція України. URL : https://cyberpolice.gov.ua/results/2018/

Постанова Верховного суду від 19.05.2021 р. у справі № 204/4521/18. URL : https://ips.ligazakon.net/document/c018840

Постанова Верховного Суду від 10.09.2020 року у справі № 751/6069/19. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/91722819

Постанова Верховного суду від 16.03.2021 р. у справі № 364/673/18. URL : https://ips.ligazakon.net/document/c017923?an=&ed=&dtm=&le=.

Постанова Верховного суду від 18.06.2020 року у справі № 711/7900/17. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/Review/89929158

Постанова Верховного суду від 24.09.2020 р. у справі №306/2629/17. URL : https://ips.ligazakon.net/document/c015095?an=2

Постанова Верховного Суду від 29.03.2021 р. у справі № 554/5090/16-к. URL : https://ips.ligazakon.net/document/C017482?an=178

Постанова Верховного суду від 31.03.2021 р. у справі № 333/1539/16-к. URL : https://ips.ligazakon.net/document/c018510?an=88

Постанова Пленуму Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ № 3 від 07 лютого 2014 року «Про узагальнення судової практики щодо розгляду слідчим суддею клопотань про дозвіл на проведення негласної слідчої (розшукової) дії». URL : http://zakon3.rada.gov.ua/laws/show/v0003740-14

Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : Проєкт Закону України № 4004 від 01.09.2020. URL : http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69771&pf35401=533919

Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України

№ 2137-IX від 15.03.2022. *Офіційний сайт Верховної ради України*. URL : https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 13.08.2023).

Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL : https://zakon.rada.gov.ua/laws/show/2939-17

Про електронні комунікації : Закон України № 1089-IX від 16 грудня 2020 року [із змінами і доповненнями]. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text

Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL : https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування (2014–2021 рр.: офіційний вебсайт Офісу генерального прокурора. URL : https://www.gp.gov.ua/ua/stat_n_st?dir_id=114368&libid=100820&c=edit&_c=fo

Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 : [із змінами і доповненнями на 01.07.2022]. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Ст. 403.

Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. URL : http://zakon3.rada.gov.ua/laws/show/2824-15.

Про телекомунікації : Закон України № 1280-IV від 18 листопада 2003 [із змінами і доповненнями на 23.02.2014]. *Офіційний вісник України*. 2003. № 51. Ст. 2644.

Рекомендації кіберполіції. URL : https://cyberpolice.gov.ua/articles/

Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рекомендації

/ [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рекомендації / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки : зб. наук. праць. Київ : Вид. поліграф. центр «Київ. ун-т», 2009. Вип. 19. URL : http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf

Самбор М. А. Негласні слідчі (розшукові) дії, пов'язані із зняттям інформації з транспортних телекомунікаційних мереж та встановленням місцезнаходження радіоелектронного засобу: підстави для проведення та умови гарантування прав і свобод людини та громадянина як споживача послуг рухомого (мобільного) зв'язку. *Вісник Дніпропетровського університету ім. А. Нобеля*. 2013. № 1. (Серія «Юридичні науки»). С. 74–81.

Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. 324 с.

Сербінов О. С. Окремі види інформації про абонента, яка знаходиться у користуванні операторів мобільного зв'язку та може бути отримана у ході проведення оперативно-розшукових заходів або слідчих дій. *Адвокат.* 2009. № 1. С. 36–39.

Серіал для батьків «Безпека дітей в Інтернеті». URL : https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey

Скибун О. Ж. Кібергігієна як складова формування цифрової держави. *Вісник НАДУ*. 2021. № 2. С. 39–46. (Серія «Державне управління»).

Сліпченко В. І. Тимчасовий доступ до речей і документів: процесуальний порядок отримання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2013. № 2. С. 507–514.

Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.

Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни: затверджено указ Президента України від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання*. 2015. № 5. Т. 49. С. 37–70.

Тагієв С. Р. Негласні слідчі (розшукові) дії у кримінальному судочинстві України : монографія [Текст]. Київ : ВД «Дакор», 2015. 440 с.

Тагієв С. Р. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 13–24.

Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. 192 с.

Теплицький Б. Б. Завдання, об'єкти та питання комп'ютерно-технічної судової експертизи. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2. С. 24–32.

Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних

мереж і мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.09. Київ, 2021. 268 с.

Тертишник В. М. Концептуальні проблеми реформи кримінального судочинства *Право і суспільство.* 2013. № 1. С. 136–140.

Ткачик А. Б. Таємниця спілкування та її обмеження в кримінальному провадженні : дис. … д-ра філос. за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 – Право). Львівський державний університет внутрішніх справ, Львів, 2021. 185 с.

Уваров В. Г. Втручання у приватне життя шляхом зняття інформації з електронних інформаційних систем: новели нового КПК України та євро стандарти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2012. № 3. С. 439–445.

Уваров В. Г. Зняття інформації з електронних інформаційних систем: новели КПК України та євростандарти. *Форум права*. 2012. № 4. С. 939–943.

Уваров В. Г. Зняття інформації з технічних каналів зв'язку. *Зовнішня торгівля: економіка, фінанси, право.* 2013. № 2. С. 177–181.

Уваров В. Г. Інститут втручання у приватне життя шляхом аудіо-, відео контролюю. *Право і безпека.* 2012. № 5 (47). С. 190–194.

Хакери «злили» дані клієнтів великої української ІТ-компанії. *Економічна правда*. URL : https://www.epravda.com.ua/news/2020/09/17/665235/

Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві. *Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства* : матеріали між- нар. наук.-практ. конф. (Одеса, 30 травня 2008 р.). Одеса. 2008. С. 206–209.

Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 256–260.

Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. № 3. С. 158–162.

Чернявський С. С., Фінагеєв В. О. Проблеми тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 179–185.

Шалева О. І. Електронна комерція : навч. посібник. Київ : Центр учб. літ., 2011. 216 с.

Шумейко Д. О. Негласний елемент у системі тактичної операції по документуванню прийняття пропозиції (обіцянки) та одержання неправомірної вигоди. *Наше право*. 2015. № 3. С. 104–111.

Юхно О. О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2. С. 86–95.

Як не стати жертвою шахраїв в Інтернеті та що робити, якщо Ви потрапили в пастку. URL : https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku

Al-garadi M. A., Varathan K. D., Ravana S. D. Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in human behavior*. 2016. Vol. 63. P. 433–443.

Al-Khater W. A., Al-Maadeed S., Ahmed A.A., Sadiq A. S., Khan M. K. Comprehensive Review of Cybercrime Detection Techniques. *IEEE access*. 2020. Vol. 8. P. 137293–137311.

Anton P. Cybercrime annual revenue is 3 times bigger than Walmart's. URL : https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts

April M. M. Norm Origin and Development in Cyberspace: Models Of Cybernorm Evolution. *Washington University Law Quarterly*. 2000. No. 78. P. 59–80.

Babak Akhgar. Cyber crime and cyber terrorism investigator's handbook. Waltham, 2014. 282 p.

Barlow J. P. A Declaration of the Independence of Cyberspace. URL : https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration

Bernik I. Cybercrime and Cyberwarfare. John Wiley & Sons, ISTE Ltd. 2014. 176 p.

Brenner W Susan. Cybercrime and the law: challenges, issues, and outcomes. Northeastern University Press, 2012. 198 p.

Calderoni F. The European legal framework on cybercrime: striving for an effective implementation. URL : https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation

Cascavilla G., Tamburri D. A., Van Den Heuvel W.-J. Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & security.* 2021, Vol. 105. P.102258.

Casey E. Digital evidence and computer crime: fo- rensic scene, computer, and the Internet. – 2nd ed. Amsterdam: Elsevier Academic Press, 2004. 690 p.

Digital Evidence: Standards and Principles. *Forensic Sciennce Communications*. 2000. Vol. 2. № 2. URL : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm.

Edwards G. Cybercrimes Investigators Handbook. Hoboken, New Jersey : John Wiley & Sons, Incorporated. 2020. 297 p.

Hong Y., Neilson W. Cybercrime and Punishment. *The Journal of legal studies*. 2020. Vol. 49 (2). P. 431–466.

Internet Organised Crime Threat Assessment (IOCTA), Europol, 2021. URL : https://www.europol.europa.eu

Internet Organised Crime Threat Assessment (IOCTA). URL : https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Kai-Lung Hui, Seung Hyun Kim, Qiu-Hong Wang. Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. MIS Quarterly. Vol. 41. No. 2 (June 2017). P. 497–524.

Meyerowitz S. A. Cybercrime. *The Banking law journal*. 2019. Vol. 136 (6). P. 299–301.

Microsoft Digital Defense Report, October 2021. P. 53. URL : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Scientific Working Group on Digital Evidence. URL : http // www.swgde.org/. Title from the screen.

The Hidden Costs of Cybercrime 2020. P. 3. URL : https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Tropina T., Callanan C. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer International Publishing AG Switzerland, 2015. 109 p.

Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation / Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (Doha, 12–19 Appril, 2015 r. A/CONF.222/12). 10–11 p. URL : https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf

ПРЕДМЕТНИЙ ПОКАЖЧИК

ПРО АВТОРІВ

Головкін Богдан Миколайович
(*розділ 1, підрозділ 1.3*)
Завідувач кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого, доктор юридичних наук, професор.
Сфера наукових інтересів: теорія кримінології, боротьба з економічною, організованою та кіберзлочинністю, протидія корупції, віктимологія.

Денькович Ольга Іванівна
(*розділ 1, підрозділи 1.1, 1.2*)
Доцент кафедри кримінального права і кримінології юридичного факультету Львівського національного університету імені Івана Франка, кандидат юридичних наук, доцент.
Сфера наукових інтересів: питання кримінального права, зокрема принципів кримінального права та кримінально-правових ризиків здійснення господарської діяльності; міжнародне кримінальне право; міжнародні стандарти кримінально-правової охорони прав людини, практика Європейського Суду з прав людини з питань кримінального права і процесу.

Луцик Василь Васильович
(*розділ 3, підрозділ 3.2*)
Доцент кафедри кримінального процесу та криміналістики факультету Львівського національного університету імені Івана Франка, кандидат юридичних наук, доцент.
Сфера наукових інтересів: негласні слідчі (розшукові) дії, прокурорське право, порівняльний кримінальний процес.

Цехан Дмитро Миколайович
(*розділ 2, розділ 3, підрозділ 3.1*)
доцент кафедри криміналістики Національного університету "Одеська юридична академія", кандидат юридичних наук, доцент
Сфера наукових інтересів: доказування у кримінальному провадженні; цифрові докази; використання високих інформаційних технологій у протидії злочинності; пенітенціарна злочинність; оперативно-розшукова діяльність в установах виконання покарань.

Електронне навчальне видання

Удосконалення магістерської програми з кримінальної юстиції

Головкін Богдан Миколайович,
Денькович Ольга Іванівна,
Луцик Василь Васильович,
Цехан Дмитро Миколайович

КІБЕРЗЛОЧИННІСТЬ ТА ЕЛЕКТРОННІ ДОКАЗИ

Навчальний посібник

За редакцією
кандидата юридичних наук, доцента Ольги ДЕНЬКОВИЧ,
доктора права, професора Габріеле ШМЕЛЬЦЕР

Редактор *Уляна Крук*
Комп'ютерне верстання *Світлани Сеник*

Формат 60x84/$_{16}$. Ум. друк. арк. 17,32. Тираж 300 пр. Зам.

Видавець та виготовлювач:
Львівський національний університет імені Івана Франка
вул. Університетська, 1, м. Львів, 79000.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції.
Серія ДК № 3059 від 13.12.2007 р.