*conditions the actual problem is the struggle against counteraction of the detection and investigation of a crime by law enforcement.*

*According to the results of the survey among the investigators of the Prosecutor's Office and the Ministry of Internal Affairs of Ukraine, the following forms of the counteraction of the crimes investigation can be highlighted: concealment of crimes, false testimonies, falsification of evidence, destruction of criminal cases, destruction of evidences of a criminal case, threats to witnesses and victims, threats to investigator, prosecutor, judge, corruption among law enforcement officers, negative use of the media, use of physical influence on members of the Criminal Proceedings. The need to overcome obstacles of the counteraction of the crimes investigation becomes relevant and extremely necessary.*

*The modern forms of the counteraction of the investigation of criminal offenses, the ways of the overcoming are analyzed in the researches of famous criminologists and scientists, namely: Bilenchuk P.D. «Means, methods, technologies of overcoming of the counteraction of the investigation of the crimes committed by organized criminal groups», Koval A.V. «Counteraction of the investigation of corruption in Law Enforcement Bodies», Shchur B.V. «Counteraction tactics of the investigation of the crimes committed by organized groups», Bobrakov I.A. «The impact of the criminals on witnesses and victims and criminalistic methods of its overcoming», Zakharchenko O.V. «Application of criminal procedural security measures during a trial», etc.*

**Key words:** *counteraction, investigation of crimes, illegal activity, law enforcement agencies, evidence, falsification, threat, witnesses, mass media, criminal case, investigator, judge.*

*Стаття надійшла 22 лютого 2018 р.*

УДК 004.939

**Т. В. Рудий,**
**В. В. Сеник, А. Т. Рудий, С. В. Сеник**

# ОРГАНІЗАЦІЙНО-ПРАВОВІ, КРИМІНАЛІСТИЧНІ ТА ТЕХНІЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

*Розглянуто нормативно-правові чинники, які становлять правову основу організаційно-технічних принципів протидії кіберзлочинності. Ідентифіковано проблему протидії кіберзлочинності, подано тлумачення основних термінів і норм щодо кваліфікації кіберзлочинів. Проаналізовано специфіку протидії кіберзлочинам, у яких інформація є об'єктом зазіхань, а інформаційні технології і телекомунікаційні сервіси використані як засоби скоєння кіберзлочинів.*

**Ключові слова:** *кіберзлочин, протидія кіберзлочинності, кібербезпека, інформаційна безпека, інформаційні технології*.

**Постановка проблеми.** Віднедавна проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кіберзлочинців сягнули сотень мільярдів доларів. З огляду на постійний розвиток законодавства та посилення покарання у сфері кіберзлочинності на теренах США і Європейського Союзу (ЄС), організовані злочинні угрупування змушені шукати комфортніші умови у країнах із лояльнішою системою протидії кіберзлочинності. Це, на жаль, в Україні, де законодавство у сфері протидії кіберзлочинності та технічного захисту інформації (ТЗІ) потребує детального перегляду та доопрацювання.

Інформаційні відносини давно стали об'єктом правового регулювання, але розвиток інформаційних технологій (ІТ) та апаратних засобів, систем телекомунікацій відбувається швидше, ніж приймаються нормативно-правові акти, якими вони регулюються, що є причиною відповідної правової колізії [1; 2].

Розглядаючи нормативно-правову базу України у сфері регулювання кібербезпеки, можна виокремити деякі проблеми: відсутність єдиного понятійного апарату та норм щодо кваліфікації кіберзлочинів; відсутність у державі розвинутих інститутів програмно-технічної та судово-кібернетичної експертиз у процесі документування та закріплення доказів кіберзлочину; відсутність відповідних науково обґрунтованих методик їх проведення; відсутність необхідного рівня координування та взаємодії між підрозділами правоохоронних структур під час проведення адекватних загрозам запобіжних і правозастосовних заходів; малорозвинена загальнодержавна система протидії кіберзлочинності [3].

**Стан дослідження.** Проблема протидії кіберзлочинності є предметом досліджень багатьох фахівців, насамперед таких військових науковців, як В. Л. Бурячок, В. О. Хорошко, В. Б. Толубко, С. В. Толюпа; а також фахівців Державної служби спеціального зв'язку та захисту інформації України (К. В. Пестов, В. В. Кравчук та ін.).

Особливості організації протидії кіберзлочинності вивчали В. Г. Хахановський, В. С. Цимбалюк, З. Б. Живко, С. В. Демедюк. Вагомий внесок у розвиток теорії захисту інформації й інформаційної безпеки зробили В. Б. Дудикевич, В. М. Максимович, М. П. Карпінський, О. С. Петров.

Проте низка проблем, які стосуються аналізу сучасного стану нормативно-правової бази України, державної політики у сфері кібербезпеки, організації, взаємодії і кординування роботи правоохоронних органів ще потребують ґрунтовного вивчення. Актуальною є проблема

визначення, трактування й імплементації базових термінів у галузі кібербезпеки, а також інформаційної безпеки загалом до законодавста України. Закони повинні відповідати сучасному стану розвитку ІТ, а в ідеалі – випереджати.

Результати наукових досліджень у галузі розслідування злочинів, скоєних із використанням інформаційних технологій, дослідження цифрових доказів, методів пошуку, отримання та фіксування таких доказів [4; 5; 6] дають підстави виокремити такі криміналістичні проблеми: відсутність науково обґрунтованої методики збирання доказів, які фіксуються під час проведення огляду місця події [3]; встановлення автентичності інформації на матеріальних носіях під час проведення комп'ютерно-технічної експертизи (КТЕ) матеріалів, які отримано шляхом оперативно-розшукових заходів (ОРЗ); коректність теоретичних засад і методик, які були застосовані експертом під час проведення досліджень; нехтування у процесі КТЕ вимогами державних та міжнародних стандартів у галузі ІТ.

**Метою** статті є аналіз сучасного стану нормативно-правової бази України у сфері регулювання кібербезпеки, специфіки протидії кіберзлочинам, у яких інформація є об'єктом зазіхань, а ІТ і телекомунікаційні сервіси використані як засоби скоєння кіберзлочинів.

**Виклад основних положень.** Віднедавна Україна робить певні потуги у напрямі розбудови інформаційного суспільства, гарантування безпеки державних інформаційних активів і протидії кіберзлочинності. Їй необхідно чітко ідентифікувати проблему протидії кіберзлочинності як одну з найнебезпечніших й ухвалити необхідну нормативно-правову базу для захисту інформаційного та кібернетичного простору держави.

У нашій державі діє низка законів та ухвалено ряд концептуальних нормативних документів різних рівнів, які охоплюють проблеми забезпечення інформаційної та кібернетичної безпеки держави, але вони не охоплюють усього спектра сучасних загроз [7; 8]. Зокрема Указ Президента України № 47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»; 5 жовтня 2017 р. Верховна Рада України приймає Закон України «Про основні засади забезпечення кібербезпеки України».

Вважаємо, що Доктрина інформаційної безпеки України є цілком необхідною концепцією для того, щоб протидіяти кіберзлочинності, хоча деякі її положення мають декларативний характер.

За своєю сутністю нормативно-правові чинники становлять правову основу організаційно-технічних принципів протидії кіберзлочинності, формують вимоги до способів і засобів захисту інформаційних активів ІС і накладають обов'язкові вимоги, згідно з чинним українським і міжнародним законодавством, невиконання яких може стати причиною несанкціонованого доступу до інформаційних активів, що тягне адміністративну та кримінальну відповідальність.

Незважаючи на широке використання у науковій літературі термінів із префіксом «кібер», проблема їх визначення на законодавчому рівні залишається актуальною.

Дослідження проблем протидії кіберзлочинності та прийняття адекватних рішень у сфері нормативно-правового забезпечення матиме успіх лише у разі чіткого визначення основних понять і термінів. У вітчизняній нормативно-правовій сфері стосовно кібернетичної та інформаційної безпеки вживаються терміни без жодних пояснень або посилання на них. Проблеми з розумінням, тлумаченням термінів і визначень можуть стати вагомими перешкодами у створенні нормативно-правового забезпечення у зазначеній галузі.

З огляду на вказане, а також з урахуванням результатів проведеного аналізу [7; 8] розумітимемо під поняттями:

– кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використання мережі Інтернет та/або інших глобальних мереж передачі даних;

– кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

– кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціоно-

ваного доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів і засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту (алгоритм реалізування кібератаки [6] на незалежну складову ІС унаочнює рис. 1);

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

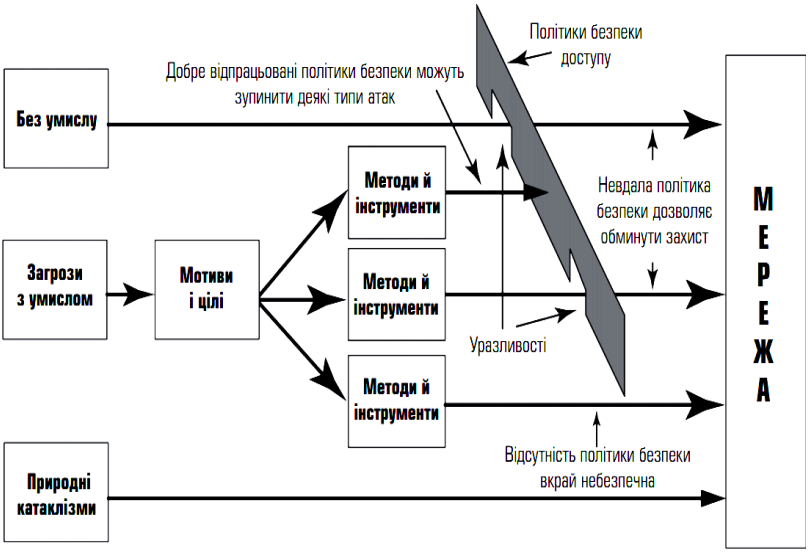


*Рис. 1. Алгоритм реалізування кібератаки на незалежну складову ІС*

Такий стан речей зумовлює ґрунтовні зміни у ставленні більшості держав світу до безпеки свого інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її оброблення та кіберсередовища, в якому ця інформація циркулює, визначення об'єктів впливу (див. рис. 2), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки [6].

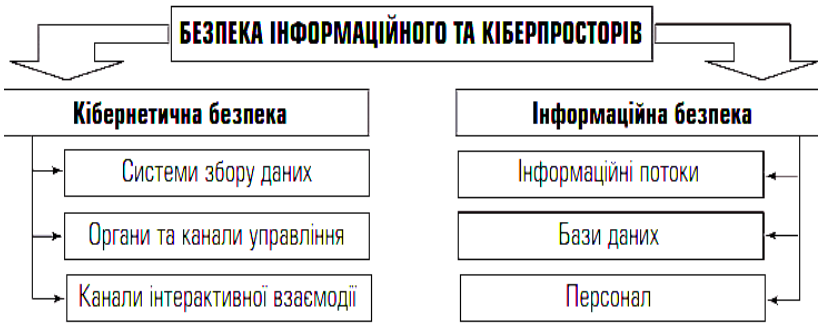


*Рис. 2. Об'єкти впливу в інформаційному та кіберпросторі*

Невизначеними у нормативно-правовому забезпеченні є питання стосовно методології підходів до проблематики забезпечення інформаційної безпеки. На перше місце потрібно поставити співвідношення понять «інформаційна безпека» та «кібербезпека». Українська наука чітко обґрунтувала необхідність розгляду національного сегмента кіберпростору як складової інформаційного простору держави [9]. З цього випливає і логічність розгляду питань кібербезпеки в контексті інформаційної безпеки (рис. 3) [6].

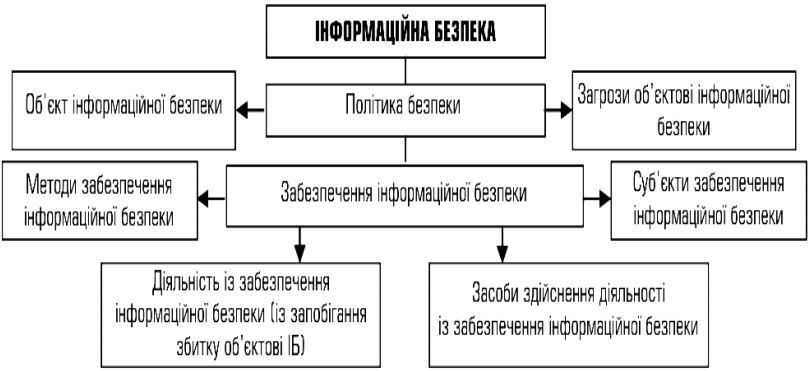


*Рис. 3. Структура поняття інформаційна безпека*

Графічну інтерпретацію взаємозв'язку інформаційного та кіберпростору подамо, [6] так (див. рис. 4).


*Рис. 4. Взаємозв'язок інформаційного та кіберпростору*

Основою кіберзлочинів є передбачені Кримінальним кодексом (КК) України суспільно небезпечні діяння і закріплені в окремому Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». З погляду кримінального права, до кіберзлочинів належать лише злочини, передбачені Розділом XVI КК України, а в межах криміналістики доцільно включити до цього поняття інші злочини, для скоєння яких використовуються ІТ. Проте у Розділі немає понять, пов'язаних із кіберзлочинністю, натомість є лише деякі поняття злочинів, які вчиняються за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку [10].

Подавши визначення, які закріплені на законодавчому рівні, і тлумачення основних термінів предметного поля на основі аналізу літературних джерел, можемо розглянути причини, що окреслюють особливості й скоєння кіберзлочинів, й заходів із протидії цим злочинам.

Характерними особливостями протидії кіберзлочинності є: необхідність широкого застосування спеціальних знань із виявлення та фіксування слідів злочину в цифровій формі; організованість і транскордонність (широкі міжрегіональні та міжнародні зв'язки) кіберзлочинців; висока латентність, спричинена небажанням по-

терпілих інформувати про такі злочини через недовіру до потенційних можливостей Національної поліції та небажання визнати прогалини у своїх системах безпеки, а також прогалини у правовому забезпеченні протидії кіберзлочинності, які дають змогу злочинцям уникнути відповідальності за скоєння злочинів; високий рівень фахової підготованості й технічного забезпечення кіберзлочинців.

Для протистояння кіберзлочинності у світі створюються спеціальні підрозділи та структури. Їхні повноваження постійно розширюються, а технічні можливості нарощуються.

З огляду на динаміку поширення кіберзлочинності й інцидентів у сфері захисту інформаційного простору, в Державній службі спеціального зв'язку та захисту інформації (ДССЗЗІ) діє Державний центр кіберзахисту та протидії кіберзагрозам, при РНБО діє Національний координаційний центр із питань кібербезпеки, створено Департамент кіберполіції Національної поліції України (ДКНПУ).

Отже, структури створено, але їх завдання розпорошені, а головний орган із координування дій не визначений. Крім того, у цих установах працює недостатньо кваліфікованих фахівців.

Новостворений ДКНПУ повинен забезпечувати реалізацію державної політики у сфері протидії кіберзлочинності, організовувати та здійснювати оперативно-розшукову діяльність відповідно до положень чинного законодавства. Одним із головних завдань ДКНПУ є протидія кіберзлочинності в таких сферах: електронних платіжних систем; електронної комерції та господарської діяльності; інтелектуальної власності; інформаційної безпеки. Детальніше розглянемо останній пункт.

До сфери інформаційної безпеки належить соціальна інженерія. Стрімкий технологічний розвиток інформаційного суспільства зумовлює зростання обсягів інформації, яка циркулює, накопичується й обробляється в інформаційному та кіберпросторі. На підставі аналізу відкритих джерел розкрито основні аспекти, особливості, способи і методи проведення розвідки інформаційно-телекомунікаційних систем (ІТС) та визначено, що вона буде визнана найефективнішим засобом виявлення, профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями та загрозами. Найдієвішим і потужним способом розвідки ІТС на найближчу перспективу буде кіберрозвідка, а найбільш результативним, з огляду на скоєння кіберзлочинів, – метод соціальної інженерії, призначений для організації доступу до захищених інформаційних активів [6].

Соціальна інженерія є багатоаспектним і складним способом отримання конфіденційної інформації від користувачів із поєднанням застосування методів соціології, психології й ІТ.

Даючи кримінологічну характеристику кіберзлочинів, треба визнати, що більшість виявлених кіберзлочинів розпорошені у звітності різних підрозділів Національної поліції і це не дає можливості комплексно проаналізувати й охарактеризувати кіберзлочинність. Нещодавно створено Управління кримінального аналізу Національної поліції для консолідації всіх розрізнених джерел оперативної інформації з подальшим глибоким аналізом, що повинно стати вагомим чинником у протидії кіберзлочинності.

Досягнення у сфері ІТ створюють нові суспільні відносини, які стають предметом кіберзлочинів. Злочини (наприклад, крадіжка грошей) тепер можуть вчинятися з використанням програмно-апаратних засобів і телекомунікаційних технологій, мережі Інтернет. Суть і предмет злочинів залишаються попередніми, новими стають лише засоби. Так, сформувався та виокремився розділ криміналістики, що вивчає кіберзлочини і називається *«computer forensics»*, комп'ютерна криміналістика або форензика [3].

Форензика (комп'ютерна криміналістика) – прикладна наука, основною метою якої є аналіз і розслідування кіберзлочинів. Вона вивчає методи отримання та дослідження доказів, обґрунтовує збір і аналіз даних у інформаційних системах (ІС), комунікаційних потоках, системах управління базами даних та зберігання інформації в порядку, допустимого в суді.

Уперше запропонував її поділ на цифрову та мережеву форензику Н. Н. Федотов [5]. На початковому етапі цифрову та мережеву форензику розглядали як пов'язані технології, але з'ясувалося, насправді, що вони дуже відрізняються. Цифрова криміналістика розвивається значною мірою завдяки потребам силових структур і повинна надати достовірні (неспростовні) докази для розкриття кіберзлочинів. Мережева криміналістика розвинулась у процесі протидії хакерським загрозам і пов'язується з архітектурою інформаційної безпеки (виявлення втручань у ІС, оцінювання загроз, попередження модифікування та НСД до даних).

Традиційні розділи криміналістики розвиваються тривалий час і накопичили великий досвід та науково обґрунтовані методики досліджень, а деякі особливості криміналістичних технологій закріплені на законодавчому рівні.

Комп'ютерна криміналістика є новим науковим напрямом, де лише починає накопичуватися практичний досвід та технології і розв'язуються такі основні завдання [5]:

– розроблення криміналістичних характеристик злочинів, пов'язаних з інформаційними відносинами;

– розроблення тактики оперативно-розшукових заходів (ОРЗ), агентурної роботи і слідчих дій, пов'язаних з інформаційними відносинами;

– розроблення методів, програмно-апаратних засобів для збору й дослідження доказів скоєння кіберзлочинів.

Основним напрямом комп'ютерної криміналістики є накопичення, дослідження і формування доказів для суду, а також збір інформації, отриманої внаслідок ОРЗ й агентурної діяльності, яка не використовуватиметься як докази в суді.

У комп'ютерній криміналістиці застосовуються і спеціальні методи досліджень, які притаманні тільки цій галузі:

– створення спеціалізованих криміналістичних ІС, перенаалаштування і використання під час проведення ОРЗ та слідчих діях ІС подвійного призначення [11];

– створення віртуального користувача для проведення ОРЗ і агентурної роботи;

– збір хеш-функцій відомих файлів для розмежування їх від файлів, які містять оригінальну користувацьку або модифіковану інформацію;

– архівування повного вмісту фізичних носіїв з метою подальшого розслідування імовірних інцидентів;

– емулювання мережевих сервісів корпоративних комп'ютерних мереж (КМ) і VPN-мереж із віддаленим доступом для експертного дослідження вилученого програмно-технічного забезпечення у лабораторних умовах.

Процес збирання доказів у кримінальній справі передбачає їх виявлення, фіксування і вилучення. Цей процес має певну специфіку. Пояснюється це, передусім тим, що сліди злочинної діяльності, спрямованої на порушення роботи ІС, через її специфічність зрідка позначаються на змінах зовнішнього середовища. Однак це не означає, що матеріальних слідів не буває взагалі. Передовсім вони є на фізичних носіях інформації і відтворюють усі зміни порівняно з початковим станом ІС. Ідеться про сліди модифікування інформації у базах даних, програмах, текстових файлах.

Результати аналізу практичної діяльності слідчих підрозділів щодо розслідування кіберзлочинів доводять, що дослідження технологічного обладнання ІС доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконають спеціально відібрані та підготовані фахівці [3].

Криміналістичний процес, який супроводжують спеціалісти та експерти, прийнято поділяти на чотири етапи: збирання; дослідження; аналіз; подання [5].

Перший етап стосується первинного збору інформації як такої, а також фізичних носіїв інформації. Цей процес супроводжується позначками атрибутів, відзначенням джерел походження даних й об'єктів (включаючи отримані шляхом ОРЗ). У процесі збору повинні забезпечуватися повнота та цілісність (незмінність) інформації, а у деяких випадках її таємність. Інколи у процесі збору доводиться застосовувати спеціальні заходи для фіксування «недовговічної» інформації (наприклад, поточних мережевих IP-з'єднань або вмісту оперативної пам'яті робочої станції КМ).

Другий етап полягає в експертному дослідженні зібраної інформації (об'ктів-носіїв) і передбачає зчитування її з носіїв, декодування та вилучення необхідної інформації, що стосується справи. У процесі дослідження також повинна забезпечуватися цілісність інформації.

На третьому етапі вибрана інформація аналізується для отримання відповідей на поставлені експерту запитання. Під час аналізу повинні використовуватися лише апробовані методи, наукова достовірність застосування яких є підтвердженою.

Четвертий етап передбачає оформлення результатів досліджень й аналізу у встановленій законом і зрозумілій для третьої сторони формі документа (висновку).

Докази, пов'язані з кіберзлочинами, які були вилучені з місця злочину, можуть легко змінитися, і через помилки під час їх вилучення, і в процесі їх дослідження. Щоб подати такі докази належно для використання у судовому процесі, потрібні спеціальні знання і відповідне вишколення. Не можна недооцінювати роль експертизи, яка могла б дати кваліфікований висновок і відповіді на поставлені слідством запитання.

Відсутність розвинених інститутів згаданих експертиз та науково обґрунтованих методик їх проведення призводить до суттєвих помилок у процесі документування та закріплення доказів кіберзлочину.

Об'єкт і завдання комп'ютерно-технічної експертизи (КТЕ) є визначеними, але враховуючи розвиток цифрової і мережевої криміналістики, цей перелік необхідно розширити, що і диктуватиметься стрімким розвитком ІТ.

До основних завдань КТЕ належать [12]:

– установлення робочого стану комп'ютерно-технічних засобів;

– 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;

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Але для того, щоб отримати таку експертизу, потрібен час не тільки на її проведення, а й на пошук відповідних фахівців. Треба мати на увазі, що під час вилучення програмно-апаратних засобів ІС визначальним чинником, який дає змогу зберегти необхідну доказову інформацію, є раптовість та оперативність. Участь фахівців у проведенні ОРЗ і слідчих діях, наприклад, зняття інформації з технічних каналів зв'язку виконується не за участю, а безпосередньо відповідним фахівцем [3].

Сучасна парадигма розвитку ІТ передбачає відчуження користувача від управління роботою ІС, а подальший розвиток програмно-апаратних засобів іде у напрямі глобального абстрагування інтерфейсу користувача від реальних процесів у ІС. Водночас криміналістичні дослідження полягають, властиво, у глибокому вивченні суті фізичних процесів, які відбуваються в ІС і телекомунікаційному обладнанні КМ. Автори переконані в тому, що у процесі ОРЗ, агентурній роботі, слідчих діях стосовно інформаційних процесів залучення відповідних фахівців є обов'язковим.

Важливою вимогою у роботі експерта є застосування детермінованого, повторюваного процесу дослідження, який є зрозумілим, виразним і простим. Дотримання цієї вимоги і використання науково обґрунтованих методик дослідження є найціннішою позитивною рисою для експерта [5]. Застосування визначеного та перевіреного процесу передбачає використання експертом таких елементів:

– перехресна перевірка виявлених результатів (використання альтернативних програмних засобів для перевірки результатів);

– правильне поводження з доказами – експерт повинен подати докази у такій же незмінній та цілісній формі, у якій вони були зібрані раніше (наприклад, фіксування криптографічних хеш-функцій із досліджуваних файлів є схожими до «відбитків пальців»);

– повнота дослідження (після виконаних досліджень експерт повинен довести їхню повноту і завершеність);

– управління архівами;

– технічна компетентність (точні визначення й обґрунтування процесу потрібні для повноцінного розуміння засобів і результатів дослідження третьою стороною);

– дотримання чинного законодавства України, нормативних документів, посадових настанов;

– гнучкість (з огляду на різноманітність інцидентів, експертові потрібно освоювати нові технології та програмно-апаратні засоби для успішного вирішення поставлених завдань).

Програмне забезпечення технічних засобів складових інформаційної інфраструктури, телекомунікаційних сервісів, яке використовується експертом, повинно відповідати таким головним вимогам: модульність; відкритість; сумісність із попередніми додатками; масштабованість; незалежність від операційних платформ; наявність вмонтованої діагностики програмних закладок на робочих станціях КМ і веб-серверах; наявність ефективної системи відновлення працездатності ІС у позаштатних ситуаціях тощо [3].

Відповідно до Закону України «Про стандартизацію» [13] та на виконання Програми робіт з національної стандартизації на 2016 рік [14], прийнято національні стандарти України у галузі ідентифікування, збору, накопичення, оброблення та захисту, збереження цифрових судово-медичних даних, гармонізовані з міжнародними нормативними документами, методом підтвердження з наданням чинності з 10 жовтня 2016 року.

Головним із них є ДСТУ ISO/IEC 27037:2016 – Інформаційні технології. Методи захисту. Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів [15]. Цей стандарт надає інструкції щодо ідентифікування, збору (збирання), накопичення, оброблення та захисту, збереження цифрових судово-медичних даних, тобто цифрових даних, які можуть бути доказами у суді.

Основна мета стандартів цифрової судово-медичної експертизи (термін, який використовується у ДСТУ ISO/IEC 27037:2016) полягає в тому, щоб пропонувати методи та процедури для криміналістичного накопичення та дослідження цифрових доказів. Стандартизація, в кінцевому підсумку, призведе до прийняття ідентичних підходів на міжнародному рівні, що полегшить порівняння, поєднання та протиставлення результатів таких досліджень, навіть, якщо вони виконуються різними експертами або організаціями, які є в різних юрисдикціях [15].

Одним із найважливіших завдань цифрової судової експертизи є накопичення та збереження доказів так, щоб забезпечити їх цілісність. Як і у випадку звичайних фізичних даних, важливо зберегти ланцюг контролю над усіма цифровими доказами, гарантуючи, що вони збираються та захищаються через структуровані процеси, прийнятні для судів. Це вимагає, щоб був досягнутий визначений базовий рівень контролю безпеки інформації.

Цифрові судово-медичні докази можуть накопичуватися з довільних електронних носіїв або засобів зв'язку. За своєю природою цифрові криміналістичні докази є уразливими – вони можуть бути легко пошкоджені або модифіковані через неправильне поводження, випадково або з певною метою.

Стандарт надає детальні вказівки щодо ідентифікування, збору та/або накопичення, маркування, зберігання, транспортування та збереження електронних доказів, зокрема, для збереження їх цілісності. Він визначає й описує процеси, за допомогою яких визнаються та ідентифікуються докази, документування місця злочину, збирання та збереження доказів, а також упакування та транспортування доказів.

Сфера дії охоплює «традиційні» ІТ-системи та засоби масової інформації, а не системи автомобілів, хмарних обчислень тощо.

Цей стандарт стосується початкового накопичення цифрових доказів і доповнюється такими стандартами відповідності (табл.) [15]:

– ISO/IEC 27041 пропонує вказівки щодо забезпечення цифрових криміналістичних аспектів, наприклад, забезпечення правильного використання відповідних методів та інструментів;

– ISO/IEC 27042 охоплює процеси, які відбуваються після збору цифрових доказів, тобто їх аналіз та інтерпретування;

– ISO/IEC 27043 охоплює більш широкі заходи з розслідування інцидентів, у межах яких проводяться судові процеси.

*Таблиця*

**Державний стандарт ДСТУ ISO/IEC 27037:2016 зі стандартами відповідності**

| | | |
|---|---|---|
| 1 | ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) | Інформаційні технології. Методи захисту. Настанови щодо ідентифікування, збирання, накопичення та збереження цифрового доказу. – Вперше. |
| 2 | ДСТУ ISO/IEC 27041:2016 (ISO/IEC 27041:2015, IDT) | Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування. – Вперше. |
| 3 | ДСТУ ISO/IEC 27042:2016 (ISO/IEC 27042:2015, IDT) | Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу. – Вперше. |
| 4 | ДСТУ ISO/IEC 27043:2016 (ISO/IEC 27043:2015, IDT) | Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів. – Вперше. |

У процесі первинного накопичення експертами цифрових доказів важливим є використання вказівки щодо оцінювання рівня необхідної валідації та підстав, необхідних для проведення валідації цифрових доказів, які викладені у стандарті ISO/IEC 27041.

Положення стандарту ISO/IEC 27042 надають вказівки і настанови щодо аналізу, інтепретування та верифікування експертами цифрових доказів на основі реалізування аналітичних процесів неперервності, вірогідності, відтворюваності та повторюваності. Аналіз, інтепретування та верифікування цифрових доказів є дуже складним процесом і тому вибір застосованих експертом методів досліджень повинен бути науково обґрунтованим. Стандарт містить практичне реалізування рекомендацій стосовно відповідних механізмів демонстрування кваліфікаційного рівня та компетентності експертів.

В Україні розроблені власні національні рекомендації та процедури для накопичення та захисту електронних доказів. Однак це створює проблеми під час розслідування транскордонних кіберзлочинів, оскільки цифрові криміналістичні докази, отримані в одній країні, можуть знадобитися для подання у суди іншої. Модифіковані цифрові докази, які могли бути накопичені або захищені без необхідного рівня безпеки інформації, можуть бути неприйнятними з правового пункту бачення.

Не зовсім зрозумілим є рішення підкомітету SC 27 «Методи захисту ІТ» Міжнародної організації зі стандартизації спільно з Міжнародною електротехнічною комісією з розроблення кількох криміналістичних стандартів, які охоплюють різні аспекти криміналістики, якщо насправді вони є взаємодоповнюючими частинами одного і того ж процесу. Багатофункціональний стандарт був би сприйнятливішим.

Окремий акцент у процесі проведення ОРЗ та агентурної роботи необхідно зробити на залученні кіберзлочинців для протидії іншим кіберзлочинцям як «фахівців» із використання ІТ для скоєння злочинів. Злочинець чітко знає методи скоєння злочину, розуміє уразливості, психологію злочинця і орієнтується на «ринку» відповідних послуг. Такий контингент своїми знаннями є ефективним у протидії кіберзлочинності [16].

Потрібно визнати, що сьогодні кримінальні структури володіють доволі потужними системами несанкціонованого доступу, збору інформації, високоефективними технічними засобами та найголовніше – якісно, у професійному розумінні, підготованими фахів-

цями. Кіберзлочинність перетворюється у цілу індустрію, яка володіє перспективними методиками і яка проникає майже в усі сфери політичної й економічної діяльності.

Розкриваючи злочини, які скоєні з використанням ІТ, аналізуючи наявну інформацію, працівники слідчих підрозділів зустрілися з проблемою, коли зловмисники, з метою приховування злочинних діянь, захищають свою інформацію цілком надійною системою криптографічного захисту інформації (КЗІ). Системи КЗІ, програмні продукти та технологічні засоби на їх основі набули поширення та стали легкодоступними не тільки для фахівців у галузі захисту інформації (СБУ, МО, МВС), але й для зацікавлених користувачів, зокрема й для кримінальних структур. Використання стандартного математичного підходу до розшифрування такої закритої інформації є неефективним.

Необхідно зауважити, що методи КЗІ дають можливість гарантувати і конфіденційність, і цілісність даних, забезпечуючи неспростовність здійсненого ідентифікування або автентифікування.

Аналізуючи поставлену проблему, хочемо виокремити два її аспекти: загальні помилки, які допускають працівники слідчих підрозділів під час розслідування злочинів, пов'язаних із використанням ІТ; захист інформації (зокрема й криптографічний), встановлюваний їх безпосередніми користувачами [1; 3].

Підлягають ґрунтовному аналізу питання правомірності використання засобів шифрування, електронних цифрових підписів.

Дедалі частіше особовий склад слідчих підрозділів Національної поліції України звертаються за практичною допомогою до провідних фахівців із проблемами доступу до КЗІ. Хоча проблема не є новою, але ефективних наукових методик і тактики поведінки працівників слідчих підрозділів під час роботи з системами КЗІ немає. На відміну від звичайних «хакерів», працівники правоохоронних органів мають право, згідно з чинним законодавством, застосувати оперативно-розшукові методи, які нині є єдиним ефективним методом доступу до такої інформації.

Визначальними щодо цього є правові та нормативні чинники – закони, стандарти, інфраструктурні рішення, бібліотеки кращих практик і методик тощо. Мета в них одна – законодавчо забезпечити кримінальний процес, зокрема, правила збирання, фіксування і подання доказів, включаючи ті, які отримані внаслідок ОРЗ і агентурної роботи [3].

Чинне законодавство України досі не передбачає чіткого трактування складових обігу інформаційних ресурсів у процесі інфор-

маційних відносин, не визначені критерії їх належності до категорій державних і недержавних. Розробники законодавства у сфері інформаційних відносин та інформаційної політики держави не зовсім компетентні у програмно-технічному забезпеченні новітніх ІТ і, як наслідок, – орієнтування на зовнішні запозичення, які, своєю чергою, не є досконалими [17].

Зазначимо, що високий фаховий рівень підготованості особового складу слідчих підрозділів Національної поліції України у галузі ІТ стане запорукою ефективної протидії і розкриття кіберзлочинів.

**Висновки.** Сутність викладеного дає підстави стверджувати, що недосконалість національного законодавства та відсутність єдиної правової бази правоохоронних органів у протидії кіберзлочинності – одна з головних причин зростання кількості злочинів.

Дослідження проблем протидії кіберзлочинності та прийняття адекватних рішень у сфері нормативно-правового забезпечення буде мати успіх лише за умови чіткого визначення і трактування основних понять, термінів.

Проведений аналіз засвідчує, що серед криміналістичних проблем головними є: відсутність науково обґрунтованих методик і тактики збирання цифрових доказів; інтерпретування та верифікування експертами цифрових доказів на основі реалізування аналітичних процесів неперервності, вірогідності, відтворюваності та повторюваності під час проведення КТЕ матеріалів, які отримано шляхом ОРЗ; нехтування вимогами державних стандартів стосовно оцінювання рівня необхідної валідації та підстав, необхідних для проведення валідації цифрових доказів.

Залучення експертів до участі у формулюванні питань, що ставляться на експертне дослідження, є необхідною реальністю, яка пояснюється швидким розвитком і галузі інформаційних технологій, і відсутністю усталених уявлень про можливості комп'ютерно-технічної експертизи.

---

1. Рудий Т. В., Захарова О. В., Зачек О. І., Рудий А. Т. Принципи організації системи захисту інформаційних систем підрозділів МВС. *Науковий вісник ЛьвДУВС. Серія юридична* / гол. ред. М. М. Цимбалюк. Львів: ЛьвДУВС, 2012. Вип. 2 (2). С. 309–316.
2. Рудий Т. В., Захарова О. В., Сеник В. В., Сеник С. В., Ізьо М. І. Організаційно-правовий супровід захисту інформаційних систем підрозділів

національної поліції України на основі міжнародних стандартів. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична* / гол. ред. Р. І. Благута. Львів: ЛьвДУВС, 2017. Вип. 2. С. 213–225.

3. Рудий Т. В., Захарова О. В., Кулешник Я. Ф., Сеник В. В., Бичинюк І. В. Протидія комп'ютерним злочинам: посібник. *Львівський державний університет внутрішніх справ*. Львів, 2016. 176 с.

4. Форос Г. В. Правове регулювання протидії кіберзлочинам. *Правова держава.* 2016. № 24. С. 164–169.

5. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007. 360 с.

6. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В. Б. Толубка. К.: ДУТ, 2015. 288 с.

7. Про Доктрину інформаційної безпеки України: Указ Президента України № 47/2017 про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року.

8. Про основні засади забезпечення кібербезпеки України: Закон України. *Відомості Верховної Ради (ВВР).* 2017. № 45. Ст. 403.

9. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби з кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/454/

10. ІТ-законодавство, проблеми, пріоритети, напрями розвитку. URL: http://aphd.ua/publication-180/.

11. Головань С. М., Петров О. С., Хорошко В. О., Чирков Д. В. Нормативне забезпечення інформаційної безпеки: підручник / за ред. проф. В. О. Хорошка. К.: ДУІКТ, 2008. 533 с.

12. Про підготовчі заходи та алгоритм дій при призначенні комп'ютерно-технічної експертизи: Експертна служба МВС України. Інформаційний лист. URL: http://ndekc.kiev.ua/wp-content/uploads/2016/08/Інформ. лист_підготовчі-дії-КТЕ-А-2016.pdf

13. Про стандартизацію: Закон України від 05.06.2014 р. № 1315-VII. URL: http:// www.search.ligazakon.ua/l_doc2.nsf/link1/T141315.html

14. Програма робіт з національної стандартизації. ДП УкрНДНЦ. URL: http://ukrndnc.org.ua/index.php?option=com_content&task=blogcategory&id=39&Itemid=235

15. ISO/IEC 27000:2016 – Інформаційні технології. URL: https:// www.iso.org

16. Мороз С. М., Кобзар О. Ф. Алгоритмізація використання в кримінальному провадженні інформації отриманої конфідентами та штатними негласними працівниками під час кримінальної розвідки. *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід*: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 29 квітня 2016 р.). Одеса: ОДУВС, 2016. С. 164–166.

17. Рудий Т. В., Кулешник Я. Ф. Організаційні принципи управління інформаційною безпекою інформаційних систем спеціального призначення. *Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки)* / за ред. М. Ф. Кропивка. Мелітополь: Вид-во Мелітопольська типографія «Люкс», 2012. № 2 (18). Т. 2. С. 347–354.

**Rudyy T. V., Senyk V. V., Rudyy A. T., Senyk S. V. Organizational and legal, criminalistic and technical aspects of opposition of cybercrime in Ukraine**

*The normative-legal factors that form the legal basis of organizational and technical principles of combating cybercrime are considered, the problem of cybercrime counteraction is identified.*

*Considering the normative and legal basis of Ukraine in the field of regulation of cybersecurity, the following problems were noted: the lack of a single conceptual apparatus and norms regarding the qualification of cybercrime; the absence in the state of developed institutes of software and technical and forensic cybernetics in the process of documenting and consolidating evidence of cybercrime; absence of appropriate scientifically substantiated methods of their conducting; lack of necessary level of coordination and interaction between units of law enforcement structures while carrying out adequate threats of preventive and enforcement measures; the underdeveloped nationwide system for combating cybercrime.*

*The problem of specificity of counteraction to cybercrime in which information is the object of infringements is considered. Information technologies and telecommunication services are used as means of committing cybercrime.*

*The analysis of the basic forensic problems is singled out and analyzed: lack of scientifically grounded method of collecting digital evidence; verification of the identified information on material carriers during the computer-technical examination of materials received through operational-search activities; the correctness of the theoretical foundations and techniques used by the expert during the research; neglect of computer-technical expertise in the process of compliance with the requirements of state and international standards in the field of information technology.*

*A separate emphasis was placed on the process of carrying out an operative-search activities and assignment work, on the need to involve cybercriminals in countering other cybercriminals as «specialists» in using information technology for committing crimes.*

*The offender clearly knows the methods of committing a crime, understands the vulnerability, the psychology of the offender and is guided by the «market» of the relevant services.*

**Key words:** *cybercrime, counteraction to cybercrime, cybersecurity, information security, information technology.*

*Стаття надійшла 22 лютого 2018 р.*