відкриває широкі можливості. Існує необхідність їх подальшого якнайшвидшого впровадження у практику проведення техніко-криміналістичних досліджень. Як ми можемо побачити комп'ютерні технології вже впровадженні в майже у всіх сферах роботи. Найбільшим недоліком цих систем в наш час є те що їх оновлення під сучасний лад, їх спрощення, оптимізація рухається дуже повільно. Ми будемо сподіватись що вітчизняні науковці будуть розвивати даний напрямок і тим спрощувати і оптимізувати роботу експертів.

Список використаних джерел

1. Іванов В.Г., Іванов С.М., Карасюк В.В. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посіб. - Х.: Право, 2010. 240 с.

2. Хахановський В. Г. Теорія і практика криміналістичної інформатики: авто-реф. дис. д-ра. юрид. наук. К., 2011. 28 с.

3. Ковальова О. В. Діджиталізація, як один з напрямів удосконалення судово-експертної діяльності. Актуальні питання судової експертології, криміналістики та кримінального процесу: мат. міжн. наук.-практ. конф. (м.Київ, 5.11.2019 р.). К.: КНДІСЕ Мінюста України, 2019. С. 265–271.

Васюта Юлія Володимирівна,
здобувач ступеня вищої освіти магістра
навчально-наукового інституту № 1
Національної академії внутрішніх справ
Науковий керівник: ***Чорноус Юлія Миколаївна,*** професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ,
доктор юридичних наук, професор

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Інформаційні процеси, що відбуваються в нашому суспільстві у зв'язку з глобальною інформатизацією, набувають широкого масштабу. Але разом з позитивними досягненнями, інформатизація супроводжується побічними, негативними явищами криміногенного характеру, до яких відносять комп'ютерну злочинність. На міжнародному рівні кіберзлочинність загрожує не лише національній безпеці окремих країн, але й безпеці людства та правопорядку.

Розслідуючи злочини міжнародного характеру, реалізація завдань кримінального провадження практично неможлива без залучення допомоги компетентних органів іноземних держав, представництв міжнародних організацій. Наприклад, під час розслідування може знадобитися інформація про особу іноземця, його характеристика, вирішуватимуться завдання з ідентифікації особи, перевірки за криміналістичними обліками. Важливого значення

набуває проведення процесуальних дій у порядку міжнародної правової допомоги, а також здійснення заходів з видачі особи (екстрадиції), перейняття кримінального провадження [5, с. 210].

Досліджуючи визначення кіберзлочинів або ІТ-злочинів, можемо встановити, що це протиправні суспільно небезпечні діяння, тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією, які забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача На підставі класифікації мотивів можна впорядкувати злочини, вчинені у кіберпросторі, на відповідні групи [4, с. 11–12]:

1) злочини, вчинені з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі;

2) злочини, вчинені з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі;

3) злочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі;

4) злочини, вчинені з ідейних мотивів, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

Особливе місце в методиці розслідування кіберзлочинів надається початковому етапу, який має на меті вирішення низки завдань: встановлення відсутності/наявності події злочину (час, місце, спосіб та інші обставини вчинення злочину); встановлення складу визначеного злочину (час, місце, спосіб, мета/мотив, повторність, вчинення групою осіб/організованою групою, наслідки й інші обставини вчинення злочину); встановлення фактичних даних, які вказують на конкретну особу, що могла вчинити злочин (форма вини, мотив і мета вчинення злочину особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру); забезпечення здійснення кримінального провадження; встановлення злочинної діяльності в повному обсязі; встановлення характеру й тяжкості обвинувачення щодо кожного суб'єкта злочину [4, с. 33].

У свою чергу до основних завдань наступного етапу розслідування кіберзлочинів можемо віднести встановлення характеристик особи/осіб, яких обвинувачують, зокрема, ступеня та характеру сприяння підозрюваного/обвинуваченого в проведенні кримінального провадження щодо нього або інших осіб; встановлення інших обставин, які враховує прокурор під час вирішення питання про укладення угоди про визнання винуватості [4, с. 34].

Огляд місця події як основна слідча (розшукова) дія при розслідуванні кіберзлочинів має свої особливості. Наприклад, по-перше, на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти «сховану» в комп'ютері інформацію без ризику її

знищення складно, а тому обов'язковою є участь спеціалістів; по-друге, як понятих слід запрошувати людей, обізнаних в комп'ютерній техніці. Поняті повинні володіти мінімально необхідними спеціальними знаннями в сфері обробки комп'ютерної інформації; по-третє, необхідно підготувати відповідну комп'ютерну техніку, яка буде використовуватися для зчитування та збереження вилученої інформації (окрім комп'ютера, потрібен кабель та спеціальне програмне забезпечення, яке дає змогу здійснювати копіювання та експрес-аналіз інформації на місці) [2, с. 305].

Окрема увага має приділятися особі злочинця, якщо така є, адже можливо, що нею передбачені засоби знищення інформації шляхом натиснення на комп'ютері однієї лише клавіші. Бажано, щоб підозрюваний був присутній при огляді, оскільки він може надати найважливішу інформацію про систему [2, с. 305–306].

Варто зазначити, що для ефективності розслідування кіберзлочинів призначається комп'ютерно-технічна експертиза. Відповідно до завдань та специфіки об'єктів дослідження в рамках цього роду експертиз доречними є два види: 1) технічна експертиза комп'ютерів і їх комплектуючих; 2) експертиза даних і програмного забезпечення [2, с. 308].

У разі проведення будь-яких слідчих дій, пов'язаних із розслідуванням злочинів у сфері використання комп'ютерних технологій, доцільним є залучення фахівця у галузі інформаційних технологій від самого початку досудового розслідування, оскільки цілеспрямована діяльність слідчого, оперативних працівників, особливо на початковому етапі, забезпечує успіх подальшого розслідування кіберзлочинів [2, с. 310].

Законодавство України у сфері кібербезпеки передбачає можливість надання правоохоронними органами інформації з питань, пов'язаних із розслідуванням кіберзлочинів, іноземній державі на підставі запиту, навіть без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні злочинів з використанням кіберпростору [3]. Відповідно до ст. 541 Кримінального процесуального кодексу України, таке співробітництво здійснюється за принципами міжнародної правової допомоги – тобто проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою [1].

Отже, інституційний механізм міжнародного співробітництва держав при розслідуванні кіберзлочинів здійснює спільні заходи щодо запобігання високотехнологічним злочинам, а також нарощування потужностей у визначеній сфері. Для розслідування кіберзлочинів необхідні добре підготовлені кадри і вдосконалене законодавство, які б створили ефективну правову основу для забезпечення слідчої,

оперативно-розшукової діяльності правоохоронних органів, а також потрібні оперативні дії, що спираються на координацію зусиль національних центрів із запобігання і розслідування транснаціональних кіберзлочинів з аналогічними міжнародними центрами в інших країнах.

Список використаних джерел

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. URL: https://ips.ligazakon.net/document/T124651.

2. Методика розслідування окремих видів злочинів: навч. посібник / О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова та ін.; за заг. ред. Є. В. Пряхіна. 2-ге вид., перероб. та допов. Львів: ЛьвДУВС, 2019. 312 с.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://ips.ligazakon.net/document/T172163.

4. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект [Текст]: навчально-методичний посібник / О. А. Самойленко. Одеса, 2020. 133 с.

5. Чорноус Ю. М. Характеристика кіберзлочинів та торгівлі людьми як злочинів міжнародного характеру. – С. 206-211. Актуальні питання протидії кіберзлочинності та торгівлі людьми: збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. Нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. – Харків: ХНУВС, 2018. – 436 с.

Дідовець Ярина Олексіївна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту № 2 Національної академії внутрішніх справ
Науковий керівник: ***Приходько Юрій Павлович,*** доцент кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ, кандидат юридичних наук, доцент

ОСОБЛИВОСТІ ПОПЕРЕДНЬОГО ДОСЛІДЖЕННЯ ГЛАДКОСТВОЛЬНОЇ ВОГНЕПАЛЬНОЇ ЗБРОЇ НА МІСЦІ ПОДІЇ

Огляд вогнепальної зброї та слідів її застосування проводять за участі спеціаліста, який володіє спеціальними знаннями в галузі судової балістики, залучення якого регламентовано статтею 71 КПК та наказами МВС України.

Метою такого огляду є виявлення, фіксація, вилучення зброї, патронів та їх складових елементів, слідів пострілу, а за необхідності, і дослідження таких слідів на місці події .