ПОНЯТТЯ ТА ОСОБЛИВОСТІ ВЗАЄМОДІЇ ПРИ РОЗСЛІДУВАННІ ЕКОНОМІЧНИХ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ НОВІТНІХ ЕЛЕКТРОННИХ ТЕХНОЛОГІЙ

Даниляк Андрій Володимирович - аспірант Харківського національного університету внутрішніх справ

УДК 343.13

В представленной научной статье раскрыты особенности взаимодействия при расследовании экономических преступлений, при совершении которых используются новейшие электронные технологии. Рассмотрена роль Департамента киберполиции Национальной полиции Украины. Раскрыта структура этого аппарата и особенности возложенных на него задач. Отдельно проанализированы особенности подготовки и назначения судебных экспертиз, объектом исследования которых выступает компьютерная техника, программные продукты, телекоммуникационные системы и средства.

Ключевые слова: взаимодействие при расследовании, расследование экономических преступлений, преступления, совершенные организованными группами, киберпреступления, новейшие электронные технологии, киберполиция Украины.

În articolul științific prezentat, sunt cercetate trăsăturile interacțiunii în investigarea crimelor economice, în comiterea cărora sunt utilizate cele mai recente tehnologii electronice. Este examinat rolul Departamentului crimelor informatice a Poliției Naționale a Ucrainei. Sunt dezvăluite structura acestui aparat și caracteristicile sarcinilor care îi sunt atribuite. Se analizează separat specificul pregătirii și desemnării expertizelor judiciare, obiect al cercetărilor cărora fiind tehnica de calcul, produsele software, sistemele și mijloacele de telecomunicații.

Cuvinte cheie: interacțiunea în timpul anchetei, investigarea crimelor economice, crimele comise de grupuri organizate, criminalitatea informatică, cele mai recente tehnologii electronice, poliția crimelor informatice din Ucraina.

The scientific article reveals the features of cooperation in the investigation of economic crimes, in the commission of which the latest electronic technologies are used. The role of the Department of Cyber Police of the National Police of Ukraine is considered. The structure of this apparatus and the features of the tasks performed are disclosed. Separately analyzed are the specifics of the preparation and appointment of forensic examinations, the object of study of which is computer technology, software products, telecommunication systems and means.

Keywords: interaction during investigation, investigation of economic crimes, crimes committed by organized groups, cybercrime, the latest electronic technologies, Cyber Police of Ukraine.

Постановка проблеми та її зв'язок із важливими практичними завданнями. В арсеналі організованих груп, які вчиняють злочини у сфері економіки, знаходиться широкий спектр новітньої комп'ютерної техніки, програмного забезпечення та технологій використання найсучасніших розробок науки і техніки для досягнення злочинного результату. Багато вчених звертало увагу на цей факт і присвячувало свої дослідження проблемам протидії злочи-

нам даної категорії [1; 2; 3]. Кіберпростір давно став віртуальною ареною змагань органів правопорядку і представників кримінального світу. Останні постійно намагаються використовувати простір для власного збагачення, встановлення контролю над бізнесом та глобальними процесами на рівні держав і світу в цілому в той час, коли органи правопорядку намагаються створити систему ефективної протидії цьому. До складу злочинних угруповань, як правило, входять спеціалісти у сфері інформаційних технологій найвищого професійного рівня. Злочинні технології збагачення, які реалізуються у сфері кіберпростору, характеризуються специфікою і вимагають поєднання зусиль слідчих, оперативних та спеціальних підрозділів, провайдерів комп'ютерних мереж і мереж електрозв'язку, а також постійного супроводження оформлення доказів ІТ- спеціалістами та експертами.

Аналіз останніх досліджень і публікацій з даної теми, виділення не вирішених раніше частин загальної проблеми. Особливостям протидії кіберзлочинів, як проблемі сучасності, присвятило свої роботи багато вчених, зокрема О.А. Самойленко, П.П. Андрушко, П.Д. Біленчук, Д.С. Азаров, О.М. Бандурка, В.М. Бутузов, С.О. Орлов, В.В. Марков, О.М. Музичук, Д.В. Пашнєв, І.О. Воронов, М.А. Погорецький, Б.В. Романюк, В.П. Сабаташ, С.В. Дрьомов та багато інших. Але питання взаємодії органів досудового розслідування, спеціальних оперативних підрозділів, експертних служб при розслідуванні економічних злочинів, вчинених з використанням новітніх електронних технологій, залишаються малодослідженими. Крім того, за останні роки суттєво змінилась структура органів правопорядку, створено нові спеціальні підрозділи по боротьбі із кіберзлочинністю. Зазнала змін і процедура взаємодії з цими суб'єктами. Тому розгляду саме цих питань присвячено представлену роботу.

Метою роботи є висвітлення особливостей взаємодії органів досудового розслідування, спеціальних оперативних підрозділів, експертних служб при розслідуванні економічних злочинів, вчинених з використанням новітніх електронних технологій.

Виклад основного матеріалу. Для організації ефективної протидії злочинам, при вчиненні яких використовуються новітні електронні технології, створено в апараті Міністерства внутрішніх справ Департамент кіберполіції Національної поліції України (далі – Департамент).

Відповідно до Положення «Про Департамент кіберполіції Національної поліції України», затвердженого наказом Національної поліції від 10.11.2015 року № 85, Департамент є міжрегіональним територіальним органом у структурі Національної поліції і є юридичною особою приватного права. До його складу входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковуються начальникові Департаменту. Функціонують наступні структурні підрозділи: Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах. Для забезпечення міжнародної співпраці та відповідно до Закону України «Про ратифікацію Конвенції про кіберзлочинність»[4] створено при Департаменті сектор Національного контактного пункту з реагування на кіберзлочини.

Департамент завдяки своєму технічному оснащенню і професійному кадровому складу має можливості миттєво виявляти кіберзагрози будь-якого характеру і вчасно реагувати на них. Також працівники Департаменту згідно з європейськими стандартамив проводять міжнародну співпрацю у напрямку знешкодження транснаціональних злочинних угруповань, у тому числі й організованих груп, що займаються економічною злочинною діяльністю.

Відповідно до Положення про Департамент кіберполіції, на нього покладається здійснення наступних завдань:

- визначати, розробляти та забезпечувати реалізацію комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;

- вживати необхідні оперативно-розшукові заходи щодо виявлення причин і умов, які

призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;

- вживати в межах встановлених чинним законодавством заходи зі збирання й узагальнення інформації стосовно об'єктів, у тому числі об'єктів сфери послуг Інтернет, телекомунікацій, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;

- організовувати та контролювати діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;

- проводити серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;

- забезпечувати формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності;

- організовувати виконання, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях;

- розробляти рекомендації для підвищення професійного рівня і поінформованості органів Національної поліції України, а також громадськості про результати діяльності кіберполіції;

- вивчати й узагальнювати вітчизняний і зарубіжний досвід боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та вносити пропозиції керівництву Національної поліції України щодо його впровадження;

- вносити пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також брати участь у розробці та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері;

- створювати та забезпечувати функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі;

- аналізувати та систематизувати дані про кримінальні правопорушення, вчинені у сфері протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та терміналами зворотного зв'язку;

- збирати, узагальнювати, систематизувати та аналізувати інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінювати результати за окремими показниками службової діяльності, звітувати про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань попередження та протидії кіберзлочинам;

- налагоджувати та підтримувати взаємодію і партнерські відносини з органами державної влади, іншими правоохоронними органами, приватним сектором та правоохоронними органами іноземних держав, міжнародними установами та організаціями у сфері протидії кіберзлочинності для ефективного виконання завдань ДКП, а також підвищення довіри населення до органів Національної поліції України;

- забезпечувати своєчасний розгляд звернень та запитів громадян, підприємств, установ, організацій з питань, віднесених до компетенції кіберполіції, здійснювати контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду;

- сприяти правильному підбору, розстановці, навчанню та вихованню кадрів Департаменту та підпорядкованих йому підрозділів;

- брати участь в організації та проведенні навчальних та науково-практичних заходів з питань протидії кіберзлочинності (тренінгів, конференцій, семінарів тощо).

Відповідно до Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затвердженої наказом МВС України 07.07.2017 року №575, досудове розслідування економічних злочинів, які пов'язані з використанням комп'ютерів, систем та комп'ютерних

мереж і мереж електрозв'язку, здійснюється слідчими, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду.

На Департамент кіберполіції покладено одне з основних завдань – виявлення і документування кримінальних правопорушень, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. Працівники структурних підрозділів Департаменту в рамках оперативно-розшукової діяльності зобов'язані при виявленні фактів таких злочинів задокументувати їх і направити матеріали ОРС до слідчого підрозділу для початку та здійснення досудового розслідування. Матеріали при цьому мають містити наступні документи.

1. Письмове пояснення заявника, в якому детально зафіксовані всі відомі дані про вчинення кримінального правопорушення, включаючи час, місце, спосіб вчинення злочину, розмір нанесеного збитку, причетні особи, дані про свідків тощо. До пояснення обов'язково приєднуються відповідні додатки, що містять відомості, які підтверджують його вчинення. Такими, зокрема, можуть виступати роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм, а також документи, що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби та інші дані.

2. Установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку, включаючи логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо) [5].

При виявленні економічних злочинів, вчинених з використанням новітніх електронних технологій, для організації ефективного розслідування утворюється слідчо-оперативна група за участю слідчих, які спеціалізуються на розслідуванні таких злочинів, та оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом. Відповідний наказ про створення такої групи підписують керівники органу досудового розслідування та Департаменту. Якщо виявлені злочини пов'язані із багатоепізодною складною діяльність організованої групи досудове розслідування у такому кримінальному провадженні здійснюється слідчими Головного слідчого управління. Слідчо-оперативна група у таких випадках утворюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України - начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції.

Старшим такої спеціалізованої слідчо-оперативної групи є слідчий, якому доручено керівником органу досудового розслідування здійснення досудового розслідування злочину.

Керівник Департаменту кіберполіції або його структурного підрозділу, оперативний працівник якого включений до складу слідчо-оперативної групи або за матеріалами оперативно-розшукової діяльності якого розпочато кримінальне провадження, забезпечує взаємодію з органом досудового розслідування.

У Департаменті, крім оперативних співробітників, працюють інспектори, які, по суті, є не атестованими штатними IT-спеціалістами. Проведене опитування слідчих, які спеціалізувались на розслідуванні розглядуваної категорії злочинів, дає підстави стверджувати про те, що тісна взаємодія з інспекторами Департаменту у багатьох випадках забезпечувала перспективу направлення кримінального провадження із обвинувальним вироком до суду. Якщо слідчий з самого початку звертався за допомогою, консультацією до інспектора, і якщо той супроводжував підготовку ключових тактичних операцій - це ставало запорукою доведеності причетності підозрюваних до вчинення складних схем злочинного збагачення.

За результатами опитування найбільш ефективною і результативною була співпраця слідчого з інспекторами Департаментів при розробці і проведенні тактичної операції із затримання співучасників за місцем знаходження комп'ютера, з якого проводились незаконні

операції. Ключовим моментом для працівника Департаменту є збереження інформації на комп'ютері та електронних носіях, а також забезпечення доступу до неї. Тому вся силова частина операції по проникненню у приміщення і фізичному захопленню співучасників планується з урахуванням двох важливих обставин.

По-перше, захоплення повинно відбуватись у той момент, коли увімкнений комп'ютер, ноутбук, смартфон чи інший пристрій, що належить злочинцям. Цей момент ретельно відстежується, адже повинні бути введені паролі відкриття пристроїв.

По-друге, захоплення передбачає такий спосіб, який не допустить можливість вимкнути пристрій злочинцем, або запустити програму знищення цінної інформації.

Вивчення практики розслідування таких злочинів свідчить про те, що група захоплення, яка виїжджала для проведення вказаної тактичної операції, вижидала час, коли підозрюваний, працюючи за комп'ютером, відходив від нього через природні потреби. В цей час здійснювалось миттєве проникнення і захоплення злочинця, а інспектор Департаменту отримував доступ до всієї наявної інформації комп'ютерного пристрою. Можливості ІТ-спеціаліста при цьому важко уявити, адже вони масштабні. Доказування ґрунтується саме на вдалому проведенні цієї операції.

У подальшому вилучені комп'ютерні пристрої, програмне обладнання і інформація підлягають експертному дослідженню.

У підготовці об'єктів для експертизи, формулюванні питань слідчим також надають кваліфіковану допомогу працівники Департаменту. Основними експертизами у кримінальних провадженнях про економічні злочини, при вчиненні яких використовувались новітні електронні технології, були: а) експертиза комп'ютерної техніки і програмних продуктів; б) експертиза телекомунікаційних систем та засобів.

Відповідно до Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки матеріалів та призначення судових експертиз, затвердженої наказом Міністерства юстиції України від 29.12.2006, № 126/5, головними завданнями експертизи комп'ютерної техніки і програмних продуктів є наступне: а) установлення технічного стану комп'ютерно-технічних засобів; б) установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;- в) виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; г) установлення відповідності програмних продуктів певним параметрам [6].

Слідчим, прокурором або слідчим суддею з метою забезпечення проведення експертного дослідження інформації, що міститься на комп'ютерних носіях, експертові обов'язково надається сам комп'ютерний носій, а також комп'ютерний комплекс, до складу якого входить досліджуваний носій. В окремих випадках експертові для дослідження може надаватися тільки комп'ютерний носій.

Якщо експертові на вирішення ставляться питання стосовно дат та часу певних дій користувача, особа, яка веде досудове розслідування, зобов'язана надати інформацію щодо показів годинника реального часу комп'ютера, з якого вилучено носій. З метою забезпечення встановлення відповідності програмних продуктів певним параметрам, а також вартості програмного продукту експертові необхідно надати наступні об'єкти:

- комп'ютерний носій з копією досліджуваного програмного продукту;

- еталонну копію програмного продукту, що реалізується на вітчизняному ринку програмних засобів.

У випадках, коли дистрибутивна копія програмного продукту відсутня, не слід відмовлятися від призначення експертизи, оскільки в окремих випадках експерт може вирішити питання і без неї.

Для забезпечення вирішення питань стосовно технічного стану комп'ютерно-технічних засобів, а також визначення їх ринкової вартості експертові необхідно надати саму комп'ютерну техніку, а також технічну документацію до неї.

Відповідно до Інструкції про призначення та проведення судових експертиз та екс-

пертних досліджень та Науково-методичних рекомендацій з питань підготовки матеріалів та призначення судових експертиз, експертиза телекомунікаційних систем та засобів має наступні головні завдання і можливості: визначати характеристику та параметри телекомунікаційних систем та засобів; встановлювати факти та способи передачі (отримання) інформації в телекомунікаційних системах; встановлювати факти та способи доступу до систем, ресурсів та інформації у сфері телекомунікацій; визначати якість телекомунікаційних послуг; встановлювати технічний стан телекомунікаційних систем та засобів; встановлювати тип, марку, модель та інші класифікаційні категорії телекомунікаційних систем та засобів; досліджувати алгоритми обробки інформації та її захисту у сфері телекомунікацій.

Об'єктами експертизи телекомунікаційних систем та засобів можуть виступати телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється.

Висновки. Звичайно, нами висвітлені не всі аспекти розслідування економічних злочинів, вчинених з використанням новітніх електронних технологій, але представлені результати можуть бути одним із кроків на загальному шляху розробки механізму протидії цьому виду злочинності.

Література

1. Самойленко О. А. Особливості розслідування викрадень майна, вчинених з використанням комп'ютерних технологій: дис… канд. юрид. наук: 12.00.09 / Олена Анатоліївна Самойленко; Донецький юридичний ін.-т ЛДУВС. – Донецьк, 2006. – 250 с.

2. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В.М. Бутузов. – К. : КИТ, 2010. – 408 с.

3. Шеломенцев В.П. Особливості взаємодії при запобіганні, виявленні та розслідуванні економічних злочинів у сфері високих технологій // Взаємодія при розслідуванні економічних злочинів : монографія / А.Ф. Волобуєв,- І.М. Осика, Р.Л. Степанюк, - Х.: Курсор, 2009. – С. 147-181.

4. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 року, редакція від 14.10.2010 // Урядовий кур'єр від 30.09.2005, - 2005. - №185.

5. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затверджена наказом МВС України 07.07.2017 року №575, зареєстр. в Міністерстві юстиції України 31.07.2017 за №937/30805, [Електроний ресурс] - Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/RE30805.html

6. Про внесення змін до Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки матеріалів та призначення судових експертиз : Наказ Мін'юст України від 29.12.2006, № 126/5, реєстрація: Мін'юст України від 29.12.2006, № 1393/13267, Офіційний сайт Верховної ради України [Електроний ресурс], - Режим доступу : http://zakon5.rada.gov.ua/laws/show/z1393-06