Комар Олексій Миколайович – здобувач кафедри економічної безпеки навчально-наукового інституту підготовки кадрів кримінальної міліції Національної академії внутрішніх справ

СПРИЯННЯ ОПЕРАТИВНИМ ПІДРОЗДІЛАМ МВС УКРАЇНИ ЩОДО ПРОТИДІЇ ШАХРАЙСТВАМ, УЧИНЮВАНИМ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

Розглянуто особливості взаємодії суб'єктів сфери високих технологій та оперативних підрозділів МВС України в процесі реалізації заходів щодо протидії використанню електронно-обчислювальної техніки при вчиненні шахрайств.

Ключові слова: організація взаємодії; електронно-обчислювальна техніка; учинення шахрайств; заходи протидії.

Рассмотрены особенности взаимодействия субъектов сферы высоких технологий в процессе реализации мероприятий по противодействию использования электронно-вычислительной техники для совершения мошенничества.

Ключевые слова: организация взаимодействия; электронно-вычислительная техника; совершение мошенничества; мероприятия по противодействию.

The article deals with the peculiarities of interaction of high technologies and operational divisions of MIA of Ukraine in the implementation of measures against the use of electronic-computers in committing fraud.

Keywords: organization of interaction; computing appliances; committing fraud countermeasures.

Латентність шахрайств, що вчинюють з використанням електронно-обчислювальної техніки, зумовлює необхідність застосування адекватних заходів щодо їх виявлення. Новий Кримінальний процесуальний кодекс (КПК) України [1] визначає порядок взаємодії оперативних підрозділів та слідчих у рамках кримінального провадження [2], порядок проведення негласних

слідчих (розшукових) дій у процесі досудового розслідування [3]. Але ним не визначено регламентацію порядку отримання первинної оперативної інформації, оскільки це не є кримінальним провадженням (у рамках досудового розслідування). У межах досудового розслідування за необхідності фіксації доказової інформації про ознаки шахрайств з використанням електронно-обчислювальної техніки здійснюють негласні слідчі (розшукові) дії. Питання про проведення негласних слідчих (розшукових) дій вирішується на основі отриманої гласної чи негласної інформації, письмових доручень слідчих та інших уповноважених осіб, запитів міжнародних правоохоронних органів й організацій інших держав. Закон передбачає проведення негласних слідчих (розшукових) дій за наявності необхідних підстав для їх проведення і використання відповідних засобів, тобто для початку цих дій суб'єкти їх проведення повинні мати законні приводи. Законні підстави негласних слідчих (розшукових) дій є гарантією дотримання законності при їх проведенні. Перелік підстав для проведення негласних слідчих (розшукових) дій є вичерпним. Кожна з підстав має свої особливості й різну юридичну значимість, що зумовлено здебільшого завданнями, цілями й способами здійснення кримінального судочинства. Законодавець визначив перелік приводів для застосування підстав проведення оперативно-розшукової діяльності в ст. 6 Закону України "Про оперативно-розшукову діяльність" [4], але не навів підстав для здійснення негласних слідчих (розшукових) дій, тому практично негласні слідчі (розшукові) дії мають підстави, аналогічні підставам проведення оперативно-розшукової діяльності з однією суттєвою відмінністю. Статтею 6 Закону України "Про оперативно-розшукову діяльність" передбачено: "Підставами для проведення оперативно-розшукової діяльності є: наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про: злочини, що готуються; осіб, які готують вчинення злочину..." [4], а підставами для проведення негласних слідчих (розшукових) дій є інформація про вже вчинений або вчинюваний злочин.

Інформацію про шахрайства у сфері високих технологій, що готуються, суб'єкти кримінального судочинства отримують з різних джерел. Це можуть бути заяви й повідомлення громадян, підприємств, установ та організацій, службових осіб, представників влади про підготовку злочину. У низці випадків така інформація може стати приводом для порушення кримінального провадження за готування до злочину (готуванням до злочину визначається підшукання або пристосування засобів чи знарядь або інше умисне створення умов для вчинення злочину). Проте здебільшого отримана з таких джерел інформація потребує перевірки, підтвердження достовірності викладених фактів чи встановлення інших даних, що вказують на наявність ознак злочину. У цих випадках і виникає необхідність залучення оперативних підрозділів для перевірки й оцінювання отриманої інформації. Значний обсяг гласної інформації про готування злочинів може бути отримано з гласних джерел. Але така інформація потребує не тільки офіційного реагування, а й проведення оперативно-розшукових заходів та

негласних слідчих (розшукових) дій з метою перевірки достовірності викладених фактів, документування події та ознак злочину, встановлення винуватості осіб у вчиненні кримінального правопорушення та інших обставин, що мають значення для правильного прийняття законного рішення і реагування.

Учинення шахрайства з використанням електронно-обчислювальної техніки є тяжким злочином, тому при його розкритті може бути застосований весь арсенал і оперативно-розшукової діяльності, і кримінального судочинства, але суттєвою проблемою є те, що застосування заходів, які обмежують конституційні права людини, неможливе на стадії підготовки злочину (якщо в діях особи не міститься складу іншого кримінального правопорушення), оскільки шахрайство ще не вчинено. При фіксації шахрайств із використанням електронно-обчислювальної техніки обов'язковим є використання спеціальних технічних заходів, тому діяльність оперативних підрозділів на етапі отримання первинної оперативної інформації та її попередньої перевірки, а також при фіксації факту підготовки до вчинення шахрайства суттєво ускладнюється. З метою ефективної протидії зазначеним злочинам необхідно використовувати можливості інших державних та недержавних суб'єктів, наприклад, завдяки інформаційно-комунікативним можливостям, Інтернет є одним з ефективних інструментів отримання первинної оперативної інформації та її перевірки. Крім цього, низка суб'єктів приватної форми власності, що діють у сфері застосування високих технологій (електронного банкінгу, телекомунікаційного зв'язку тощо), мають широкі можливості щодо отримання первинної інформації, її перевірки та попередньої фіксації (а за необхідності – правових підстав і процесуальної фіксації).

Ураховуючи нагальну потребу у взаємодії з такими суб'єктами, доцільно визначити вже напрацьовані шляхи сприяння зазначеним суб'єктам оперативно-розшукової діяльності оперативних підрозділів при викритті шахрайств, що вчиняють з використанням електронно-обчислювальної техніки, а також запропонувати інші способи розв'язання проблеми.

Одним з варіантів ефективного співробітництва є взаємодія із суб'єктами контролю системи електронних платежів. У зв'язку з тим, що банки-члени платіжних систем не приділяють значної уваги безпеці розрахунків, захисту інформації, не здійснюють належним чином моніторинг і відеонагляд за банкоматами та продовжують емітувати спеціальні платіжні засоби з магнітною смугою, що є недостатньо захищеними, лише у 2010 р. 43 банки-члени платіжних систем зазнали збитків, а кількість шахрайських операцій з використанням платіжних карток становила 2916 операцій, зі збитками за цими операціями в сумі 6 304 000 грн [5]. Унаслідок цього, на адресу Національного банку України (НБУ), МВС України, Генеральної прокуратури України надходили скарги громадян щодо несанкціонованого списання коштів з рахунків, невидачі готівки банкоматами, неналежного моніторингу за їх роботою та неможливості оперативного врегулювання спірних ситуацій під час звернення до банків тощо.

Ураховуючи ситуацію, що склалася, НБУ за участю представників МВС України та банків-членів платіжних систем 17 лютого 2011 р. було проведено міжвідомчу нараду з питань запобігання та протидії шахрайським діям з використанням платіжних карток. На міжвідомчій нараді були досягнуті домовленості щодо: вжиття банками України заходів щодо максимального забезпечення безпеки здійснення операцій з використанням платіжних карток через платіжні пристрої; співпраці з фахівцями МВС України для протидії шахрайським та злочинним діям з використанням платіжних карток; дотримання рекомендацій щодо запобігання та протидії шахрайським діям.

Відповідно до рішення Міжвідомчої наради з питань запобігання та протидії шахрайським діям з використанням платіжних карток, МВС України та Українською міжбанківською асоціацією членів платіжних систем "ЄМА" було затверджено "Порядок взаємодії членів та учасників Української міжбанківської асоціації членів платіжних систем "ЄМА" та Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України", яким визначено спільні заходи у сфері протидії шахрайським використанням платіжних карток на території України [6]. Згідно з цим документом, банки зобов'язані: для оперативного отримання та передачі інформації про зафіксовані випадки шахрайства приєднатися до захищеної міжбанківської системи обміну інформацією про шахрайства "Exchange-online" та забезпечити відповідальних працівників банку доступом до зазначеної системи; сприяти взаємному інформуванню банків, Асоціації "Український союз учасників НСМЕП" та Асоціації "ЄМА" (зокрема, шляхом використання системи "Exchange-online") про виявлені випадки шахрайства; забезпечити належну перевірку інформації про компрометацію платіжних карток, банкоматів, платіжних терміналів та надання результатів перевірки Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України, Асоціації "Український союз учасників НСМЕП" та Асоціації "ЄМА" для проведення аналізу із залученням виробників обладнання; емітентам та еквайрам забезпечити постійний моніторинг за операціями з використанням спеціальних платіжних засобів, які здійснюються через банкомати; провести інструктаж співробітників служб моніторингу про необхідність інформування Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України стосовно випадків виявлення фактів учинення шахрайських дій для оперативної організації затримання осіб, причетних до них; забезпечити постійний контроль за роботою працівників, які здійснюють моніторинг роботи банкоматів та їх обслуговування; установити контроль за підбором та роботою працівників, які за функціональними обов'язками мають доступ до інформаційних систем банків, ключової документації, а також мають можливість уносити зміни до їх інформаційних масивів; установити відеоспостереження на банкомати, а в разі необхідності – додаткове освітлення приміщень тощо; установити антивірусне програмне забезпечення на банкомати (розробник програмного забезпечення банкоматів повинен надати перелік антивірусного програмного забезпечення, сумісного з розробленим програмним забезпеченням, а

також рекомендації щодо можливості використання антивірусної перевірки в режимі реального часу та/або повного сканування жорстких дисків, режимів оновлення антивірусних баз та антивірусного програмного забезпечення); провести тестування комп'ютерів спеціальними програмними засобами аналізу захищеності для забезпечення захисту їх локальних ресурсів, що входять до складу банкомату, від несанкціонованого доступу (за результатами тестування розробити додаткові вимоги та рекомендації щодо усунення вразливостей операційної системи для відповідної програмно-апаратної реалізації комп'ютера банкомату – ці вимоги мають бути виконані постачальниками відповідного термінального обладнання); у випадку встановлення на комп'ютер банкомату операційної системи, яка дозволяє розмежування прав доступу (Windows 2000, Windows XP тощо), програмне забезпечення доцільно запускати від імені користувача операційної системи, який не має адміністративних повноважень; унеможливити несанкціоновану заміну штатного програмного забезпечення банкомату на інше та встановлення додаткового програмного забезпечення; забезпечити автоматичне ведення програмним забезпеченням банкомату захищеного від несанкціонованої модифікації протоколу всіх дій (журналів) (у разі використання в банкоматі журнального принтера на його стрічку не виводити конфіденційну інформацію); ужити додаткових заходів щодо збереження банкоматів від пошкодження, демонтажу або викрадення.

Унаслідок організації взаємодії в низці суб'єктів з'явилася нормативна база для сприяння оперативним підрозділам при протидії шахрайствам, що вчиняють з використанням електронно-обчислювальної техніки. Відповідно, рішенням Міжвідомчої наради з питань запобігання та протидії шахрайським діям з використанням платіжних карток від 17 лютого 2011 р. передбачено:

НБУ: забезпечить доведення до відома банків та асоціацій інформації про збитки банків, держателів платіжних карток і торговців через незаконні дії/сумнівні операції з платіжними картками; щодо рішення міжвідомчої наради та рекомендацій (наданих листом МВС України від 28 лютого 2010 р. № 24349-Пп), які необхідно враховувати банкам у своїй роботі щодо запобігання та протидії шахрайствам з використанням електронно-обчислювальної техніки;

Асоціація "ЄМА": на підставі щоквартальних засідань Форуму з безпеки розрахунків інформуватиме НБУ про поточні тенденції та виявлені факти шахрайства з платіжними картками та надаватиме пропозиції щодо заходів, яких доцільно впроваджувати банкам-членам платіжних систем;

банки України: максимально прискорять перехід на застосування смарт-карток та поступово обмежать обслуговування карток з магнітною смугою; з урахуванням рекомендацій, наданих листом МВС України, забезпечать виконання зазначених заходів; розроблять і розмістять у доступному для клієнтів місці та на офіційній сторінці банку в мережі Інтернет рекомендації щодо безпеки здійснення операцій з використанням платіжних карток у банкоматах, безготівкової оплати

товарів і послуг, у тому числі через мережу Інтернет; дотримуватимуться запропонованих заходів про співпрацю та забезпечуватимуть (з урахуванням вимог законодавства про банківську таємницю й захист персональних даних) належний обмін інформацією з МВС України та Асоціацією "ЄМА" про випадки шахрайства в порядку, передбаченому протоколом про взаємодію.

Таким чином, НБУ, керуючись ст. 42 Закону України "Про платіжні системи та переказ коштів в Україні", зобов'язав банки вжити відповідних заходів щодо запобігання і протидії шахрайствам з використанням спеціальних платіжних засобів, ураховуючи рекомендації МВС України.

Інший шлях можна обрати з урахуванням можливості контролю складових, що використовують для вчинення зазначених злочинів: мережі Інтернет (як сфери шахрайських зазіхань); електронно-обчислювальної техніки (комп'ютер особистий та корпоративний; обслуговуюче обладнання); комп'ютерних програм. Ураховуючи розвиток цієї системи, держава повинна вживати обмежувальні заходи щодо використання сфери високих технологій при вчиненні шахрайств. Якщо на мережу Інтернет, або поширення ЕОМ, держава вплинути не в змозі, то процес використання певних комп'ютерних програм повинен контролюватися. Держава має можливість впливати на інформаційно-технічну складову, зокрема, це стосується використання певних комп'ютерних програм. Наприклад, при вчиненні фішингу шахраї розсилають повідомлення електронною поштою від імені інтернет-компаній з допомогою яких, а також посилань на підроблені сайти, що містяться в них, отримують особисті дані користувача. В інтернет-провайдерів є технологічні можливості обмежувати або блокувати шахрайські розсилки. Наприклад, DMARC створює механізм, з допомогою якого перевіряється справжність домена – відправника листа й використовуваних цифрових підписів на повідомленнях, унаслідок чого поштові сервіси можуть виявляти й блокувати шахрайські листи. Справжність електронних листів установлюється з допомогою так званих доменних ключів (Domain Keys) – зашифрованих пакетів даних, що містять інформацію про відправника листа, яка дає змогу отримувачу переконатися в тому, що відправник не є спамером. Хоча технології доменних ключів існують давно, є кілька різних, несумісних один з одним способів їх реалізації, але специфікація, розроблена DMARC, описує єдиний метод інтеграції зазначених технологій у поштові системи.

Інший аспект проблеми – правова основа таких дій. Якщо інтернет-компанії практично впливають на можливість шахраїв використовувати власні потужності, то такий контроль з боку держави потребує певного правового обґрунтування. У розвинених країнах ця робота ведеться. Наприклад, критерії визначення безпеки комп'ютерних програм (англ. Trusted Computer System Evaluation Criteria) – стандарт Міністерства оборони США, що встановлює головні умови оцінювання ефективності засобів комп'ютерної безпеки, що містяться в комп'ютерній системі. Критерії використовують для визначення, класифікації та вибору комп'ютерних програм, призначених для обробки, збереження та

пошуку важливої чи таємної інформації. Критерії, що згадуються як Оранжева книга, посідають головне місце серед публікацій "райдужної серії" Міністерства оборони США. Аналогом Оранжевої книги є міжнародний стандарт ISO/IEC 15408, опублікований у 2005 році. Це універсальніший та досконаліший стандарт, але, усупереч поширеній думці, він не замінює Оранжеву книгу у зв'язку з різною юрисдикцією документів – Оранжеву книгу використовує винятково Міністерство оборони США, водночас ISO/IEC 15408 ратифікували більшість країн, у тому числі Росія. Вона ухвалила закон, відповідно до якого державні органи (Роскомнагляд) можуть здійснювати позасудове закриття сайтів, через які поширюється інформація про підготовку та вчинення злочинів. Тобто існують технологічні можливості контролю та є приклади створення правової бази, проте не вистачає відповідної організації.

Підсумовуючи викладене, на нашу думку, необхідно визначити процедуру ліцензування комп'ютерних програм, що використовують у сфері високих технологій в Україні. Для цього необхідно створити незалежний державний орган, який би спочатку сертифікував та ідентифікував програмний продукт, що впроваджують та використовують органи державної влади в Україні, захищаючи авторські права правовласника, а також додатково визначаючи його якість, ступені захисту від різноманітних шахрайських дій та ціну. У разі створення відповідної правової бази необхідною умовою використання будь-якої комп'ютерної програми стане її сертифікація, а відповідно, і контроль держави за її використанням. У свою чергу, несертифіковані програми будуть автоматично блокуватися за договором з інтернет-компаніями, які неодноразово об'єднувалися для боротьби з шахраями.

Таким чином, ураховуючи інтереси інших суб'єктів, які використовують електронно-обчислювальну техніку в повсякденній діяльності (і мають вплив на можливість її використання із злочинною метою), ми запропонували варіант сприяння оперативним підрозділам зазначеними суб'єктами (як державної, так і приватної форм власності) у процесі виявлення ознак та фіксації фактів учинення шахрайств у сфері високих технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. [Електронний ресурс]. – Режим доступу : http://gska2.rada.gov.ua.

2. Про організацію взаємодії органів досудового розслідування з іншими органами та підрозділами внутрішніх справ у попередженні, виявленні та розслідуванні кримінальних правопорушень: наказ МВС України від 14 серп. 2012 р. № 700.

3. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ Генеральної прокуратури України, МВС України, СБУ, Адміністрації прикордонної служби України,

Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5.

4. Про оперативно-розшукову діяльність : Закон України від 4 груд. 1990 р. [Електронний ресурс]. – Режим доступу : http: //www.rada.gov.ua.

5. Щодо безпеки ринку платіжних карток України : лист НБУ № 25-312/943-5139 // Електронна пошта: Департамент платіжних систем – банкам України від 15 квіт. 2011 р.

6. Щодо протидії шахрайським операціям із застосуванням платіжних карток : лист НБУ № 25-312/2323-11725 // Електронна пошта: Генеральний департамент регулювання платіжних систем та розрахунків, Департамент платіжних систем – банкам України від 6 жовт. 2011 р.