УДК 343.9:354.42/44

ЗАХОДИ ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

MEASURES AGAINST ECONOMIC CRIME IN THE INFORMATION TECHNOLOGY SPHERE

Рогозін С.М.,
кандидат юридичних наук,
начальник ГУБОЗ МВС України

Проаналізовано доктрину інформаційного права, а також чинне законодавство у контексті визначення заходів протидії економічній злочинності у сфері інформаційних технологій. Визначено напрями удосконалення чинного законодавства з метою забезпечення своєчасності та ефективності заходів протидії економічній злочинності у сфері інформаційних технологій. Також зроблені відповідні висновки щодо заходів протидії економічній злочинності у сфері інформаційних технологій.

Ключові слова: економічна злочинність, заходи протидії, інформаційні технології, доктрина інформаційного права, чине законодавство.

Проанализирована доктрина информационного права, а также действующее законодательство в контексте определения мер противодействия экономической преступности в сфере информационных технологий. Определены направления совершенствования действующего законодательства в целях обеспечения своевременности и эффективности мер противодействия экономической преступности в сфере информационных технологий. Также сделаны соответствующие выводы относительно мер противодействия экономической преступности в сфере информационных технологий

Ключевые слова: экономическая преступность, меры противодействия, информационные технологии, доктрина информационного права, чине законодательство.

The doctrine of information law and the current legislation in the context of determining the measures to counteraction economic crime in the sphere of information technologies is analyzed in the article. The directions of improvement of the current legislation in order to ensure timely and effective measures to counteraction economic crime in the sphere of information technologies are determined. Also it were made appropriate conclusions regarding measures against economic crime in the sphere of information technologies.

Key words: economic crime, countermeasures, information technologies, doctrine of Information Law, valid legislation.

Постановка проблеми. Сьогодні важко уявити собі практичну діяльність людини без застосування засобів інформаційних технологій. Сучасні інформаційні технології дозволяють автоматизувати робочі процеси, забезпечувати умови для задоволення потреб людини, зменшувати витрати часу для досягнення бажаного результату. Незважаючи на те, що інформаційні технології несуть у собі вагомий потенціал для розвитку науки й техніки, вони також створюють умови для збільшення кількості злочинів у сфері економіки.

Масштаби і локалізація поширення економічної злочинності у сфері інформаційних технологій значно змінилися. Економічна злочинність поширюється переважно у глобальних інформаційних мережах, оскільки злочинці використовують мережу Інтернет для вчинення незаконного доступу до інформаційних баз даних, умисного розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів, що, в свою чергу, призводить до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї тощо. Також проявляється тенденція до значного збільшення кількість злочинів, пов'язаних з використанням у глобальній мережі Інтернет електронних платіжних систем у процесі легалізації або відмивання доходів, одержаних злочинним шляхом.

Слід зазначити, що в цілому об'єктом найбільшої кількості злочинних посягань у сфері інформаційних технологій є малі та середні підприємства з чисельністю працівників менше 500 осіб. Це пов'язано з тим, що спочатку злочинці використовують можливість неефективної системи захисту корпоративної інформації у таких підприємствах, з метою подальшого незаконного доступу вже до інформаційно-телекомунікаційних мереж великих корпорацій, в складі яких знаходиться дане мале чи середнє підприємство.

Наприклад, досить часто трапляються випадки, коли працівник може вимкнути комп'ютер, який вже містить вірус, а при наступному його включенні на екрані монітору з'явиться інформація, що користувач дивився щось незаконне чи переглядав порнографічні сайти. З метою налагодження подальшої роботи комп'ютера, особі запропонується перерахувати з мобільного телефону кошти на певний рахунок, за результатами чого він отримає sms-повідомлення з певним кодом, набравши який особі буде надана можливість користуватися комп'ютером. При цьому, слід мати на увазі, що у багатьох випадках оплата грошових коштів не гарантує подальшу роботу зараженого вірусом комп'ютера. Крім того, оплачуючи певну послугу в мережі Інтернет, користувачу варто пам'ятати, що часто злочинці можуть використовувати певні сайти у всесвітній мережі з метою незаконного доступу до банківських рахунків певної фізичної особи.

Таким чином, економічна злочинність набуває дедалі більш значних проявів і становить загрозу інформаційній безпеці багатьох держав світу, оскільки суспільно небезпечні дії вчиняються переважно в глобальній мережі Інтернет, яка не має кордонів, а тому спостерігається стійка тенденція до формування транснаціональних злочинних організацій, які використовують інформаційне середовище для вчинення злочинів у сфері економіки.

Стан дослідження. Окремі аспекти протидії економічній злочинності у сфері інформаційних технологій висвітлювались у працях таких науковців, як Т. В. Авер'янова, В. Б. Вєхова, Ю. В. Гавриліна, В. О. Голубєва, О.Ю. Дрозда, О. Г. Кальмана, В. В. Коваленка, О. В. Копана, В. О. Мещерякова, В. О. Мілашева, О. І. Мотляха, Л. П. Паламарчука, В. Ю. Рогозіна, О. А. Самойленка, С. А. Шепетька та інших. Однак, не дивлячись на беззаперечну теоретичну й практичну значимість зазначених наукових праць, у цілому можна констатувати недостатню розробленість змістовних характеристик економічної злочинності у сфері інформаційних технологій та недостатню визначеність підходів до її аналізу з позицій визначення ефективних заходів протидії їй.

Тому на сьогодні одним із пріоритетних напрямів діяльності спеціальних підрозділів по боротьбі з економічної злочинністю є протидія економічній злочинності у сфері інформаційних технологій. При цьому, зважаючи на збільшення кількості проявів транснаціональних злочинів у сфері економіки, вчинених за допомогою засобів інформаційних технологій, ключовими елементами протидії повинні стати ефективне міжнародне співробітництво, координація й взаємодія в цій діяльності правоохоронних органів України з уповноваженими органами іноземних держав. Саме це й обумовлює мету даної статті – визначити заходи протидії економічній злочинності у сфері інформаційних технологій.

Виклад основного матеріалу. Зарубіжний досвід діяльності правоохоронних органів з протидії економічній злочинності свідчить про необхідність запровадження у практичну діяльність правоохоронних органів системи негайного збереження даних, які містяться в комп'ютері (ноутбуці, нетбуці, смартфоні, планшеті) під час виявлення протиправних дій, збирання й вилучення доказів у електронній формі, отримання правової та оперативної інформації щодо фактів і обставин вчинення злочинів у сфері економіки, установлення й затримання осіб, підозрюваних у вчиненні злочину.

У свою чергу, важливим моментом у протидії економічній злочинності є налагодження взаємодії з уповноваженими правоохоронними органами зарубіжних держав, адже швидке виявлення злочину суттєво ускладнюється, якщо його вчинено в мережі Інтернет. Тому ефективність протидії економічній злочинності у сфері інформаційних технологій залежить від рівня технічної оснащеності правоохо-

ронних органів сучасними інформаційно-телекомунікаційними засобами та відповідним програмним забезпеченням, наявністю автоматизованих баз даних, використанням негласних слідчих (розшукових) заходів, ефективності обміну інформаційними даними між правоохоронними органами зарубіжних держав.

Таким чином, особливе значення має координація діяльності спеціальних підрозділів по боротьбі з економічною злочинністю. Цю координацію здійснюють шляхом утворення мережі пунктів цілодобової контактної взаємодії у сфері протидії економічній злочинності. Така мережа дозволяє спеціальним підрозділам правоохоронних органів по боротьбі з економічною злочинністю цілодобово обмінюватися інформацією в режимі «он-лайн» протягом семи діб на тиждень з правоохоронними органами зарубіжних держав.

У процесі функціонування мережі пунктів цілодобової контактної взаємодії у сфері протидії економічній злочинності слід забезпечити належний захист даних щодо «трафіку» (процесу отримання-передачі інформації у мережі Інтернет) в інтересах правоохоронних органів. Для цього слід прийняти відповідні нормативно-правові акти, які будуть захищати інтереси вітчизняних правоохоронних органів щодо захисту інформації, яка використовувалася під час виявлення та розслідування злочину в сфері економіки, вчиненого за допомогою засобів інформаційних технологій.

Отже, доцільно наявні проблеми, що існують у сфері протидії економічній злочинності, вирішувати шляхом приведення норм чинного законодавства у відповідність до міжнародних правових норм, які передбачають необхідність здійснення обміну інформацією двадцять чотири години на добу протягом семи діб на тиждень. Крім того, на законодавчому рівні слід прийняти окремий нормативно-правовий акт, спрямований на врегулювання відносин, пов'язаних зі здійсненням координації та взаємодії спеціальних підрозділів правоохоронних органів України по боротьбі з економічною злочинністю з уповноваженими органами іноземних держав у сфері протидії економічній злочинності.

Слід також вирішити й практичні проблеми у сфері виявлення та розслідування злочинів, пов'язаних із організацією належної взаємодії спеціальних підрозділів правоохоронних органів України в їх діяльності з протидії економічній злочинності у сфері інформаційних технологій. Адже правоохоронні органи України під час здійснення заходів оперативно-розшукової діяльності, провадження досудового розслідування, а також у процесі доказування, не обмежуються територією власної держави, тому що докази можуть бути одержані на території іноземної держави в результаті здійснення міжнародного співробітництва під час кримінального провадження.

Так, відповідно до ч. 1 ст. 545 КПК України, Генеральна прокуратура України звертається із запитами про міжнародну правову допомогу в кримінальному провадженні під час досудового розслідування та розглядає відповідні запити іноземних компетентних органів. Крім того, відповідно до ч. 1 ст. 550 КПК України, документи, які направляються у зв'язку із запитом про міжнародне співробітництво, якщо їх складено, засвідчено у відповідній формі офіційною особою компетентного органу запитуючої сторони або запитуваної сторони і скріплено гербовою печаткою компетентного органу, приймаються на території України без додаткового засвідчення (легалізації) у разі, якщо це передбачено міжнародним договором України. Згідно з ч. 2 ст. 550 КПК України, відомості, які містяться в матеріалах, отриманих у результаті виконання дій, передбачених у запиті про міжнародне співробітництво, органами іноземної держави та за процедурою, передбаченою законодавством запитуваної держави, не потребують легалізації і визнаються судом допустимими, якщо під час їх отримання не було порушено засади справедливого судочинства, права людини та основоположні свободи.

Наприклад, міжнародне співробітництво в рамках Меморандуму про співробітництво між Генеральною прокуратурою України і Генеральною прокуратурою Республіки Сербія у боротьбі з транснаціональною організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом, здійснюється на підставі запитів про надання інформації. Кожна Сторона без попереднього прохання може надіслати іншій Стороні інформацію, коли вона вважає, що така інформація може допомогти Стороні, якій вона надається, в порушенні чи проведенні розслідування. Сторона, яка надає відповідно до положень цього Меморандуму інформацію та документи, може зажадати від іншої Сторони гарантій дотримання конфіденційності при їх використанні. Якщо інформація та матеріали необхідні запитуючій Стороні для використання у судовому процесі, то вона повинна звернутись із запитом про надання правової допомоги відповідно до правил, встановлених міжнародним правом та її внутрішнім законодавством [1].

Слід зазначити, що поряд із використанням доказів, отриманих на території іноземної держави, істотне значення для виявлення й розслідування злочину в сфері економіки має інформація, яка використовувалася злочинцем під час вчинення злочину в глобальній мережі Інтернет, визначення засобів, які використовувалися особою для незаконного доступу до інформаційно-телекомунікаційної системи, що стала об'єктом злочинного посягання.

Так, наприклад, оперативними заходами правоохоронці встановили особу жінки, яка організувала такий своєрідний «бізнес». 32-річна місцева мешканка налаштувала надання сексуальних послуг іноземним громадянам через мережу Інтернет. У самому центрі м. Миколаєва жінка орендувала квартиру, в якій облаштувала три «робочих» місця з комп'ютерною технікою та веб-камерами. До виконання еротичних замовлень користувачів мережі Інтернет зловмисниця запросила малозабезпечених дівчат приємної зовнішності. Порностудія працювала у режимі онлайн цілодобово, дівчата за допо-

могою спеціального еротичного приладдя та інших речей задовольняли пристрасті іноземних клієнтів, які, у свою чергу, оплачували їх послуги через систему електронних грошей. Кожна з дівчат отримувала кошти за виконану роботу в залежності від кількості «задоволених» клієнтів [2].

Правоохоронці завітали до приміщення порностудії у той час, коли одна з дівчат «спілкувалась» у режимі «онлайн» з чоловіками. Оперативними заходами затримано організаторку порностудії та самих дівчат-працівниць. На місці розпусти вилучено речові докази: спецприладдя, комп'ютерну техніку та грошові кошти, отримані злочинним шляхом [2].

Таким чином, ураховуючи доступність і масову поширеність засобів інформаційних технологій у побуті людей, важливо, щоб оперативно-розшукові й розшукові (слідчі) дії, які застосовуються спеціальними підрозділами правоохоронних органів з метою протидії проявам економічної злочинності у сфері інформаційних технологій, були своєчасними та ефективними. З цією метою досвідом з українськими правоохоронцями ділилися фахівці однієї з британських компаній, яка є одним зі світових лідерів у сфері інформаційної безпеки, комп'ютерної криміналістики, а також пов'язаних з цим областей знань. Під час навчального тренінгу його учасники розглянули питання протидії кіберзлочинам через виявлення та знешкодження шкідливого програмного забезпечення, виявлення сторонніх і підозрілих процесів у роботі ЕОМ і їх джерел тощо. Крім того, іноземні та вітчизняні фахівці обговорили практичні аспекти документування злочинів, скоєних у віртуальному просторі, методику сканування шкідливих програм за допомогою спеціалізованих локальних та он-лайн інструментів, збору і фіксації доказів у кримінальних провадженнях за фактами скоєння кіберзлочинів [3].

Слід зазначити, що своєчасність та ефективність заходів протидії економічній злочинності у сфері інформаційних технологій залежить від: 1) забезпечення функціонування системи резервного копіювання даних, які створюються та розповсюджуються за допомогою засобів інформаційних технологій у діяльності підприємства, установи чи організації; 2) налагодження міжнародного співробітництва з іноземними правоохоронними органами у сфері збирання й вилучення доказів в електронній формі під час кримінального провадження щодо злочинів, учинених з транснаціональними зв'язками; 3) функціонування режиму «онлайн» щодо отримання правової та оперативної інформації щодо фактів і обставин вчинення економічних злочинів у сфері інформаційних технологій; 4) міжнародного співробітництва з іноземними правоохоронним органами щодо встановлення місцезнаходження й затримання осіб, підозрюваних у вчиненні транснаціональних економічних злочинів у сфері інформаційних технологій; 5) налагодження системи швидкого обміну збереженими та отриманими даними, а також інформацією щодо проявів економічної злочинності у сфері інформаційних технологій між вітчизняними й іноземними спеціальними підрозділами правоохоронних органів по боротьбі з економічною злочинністю.

Реалізація зазначених заходів дозволить забезпечити ефективну протидію проявам економічної злочинності у сфері інформаційних технологій, а також належне міжнародне співробітництво спеціальних підрозділів правоохоронних органів по боротьбі з економічною злочинністю України з уповноваженими органами зарубіжних держав. З цією метою доцільно налагодити ефективне функціонування цілодобової контактної мережі, яка забезпечує обмін інформацією щодо виявлення та розслідування злочинів у сфері економіки, вчинених засобами інформаційно-комунікаційних технологій.

Так, в Управлінні боротьби з кіберзлочинністю МВС України за ініціативи Посольства Федеративної Республіки Німеччина в Україні відбулася низка робочих зустрічей зі зв'язковим офіцером федерального кримінального відомства поліції і комісарами цього ж відомства. Під час робочих зустрічей фахівці обговорили питання взаємодії між Національними контактними пунктами з реагування на кіберзлочини Німеччини та України. Піднімались і проблемні питання. Зокрема, щодо обміну оперативною інформацію між Управлінням боротьби з кіберзлочинністю МВС України та Федеральним кримінальним відомством під час виявлення і розслідування кримінальних правопорушень, пов'язаних із розповсюдженням програм, що містять шкідливий код (вірус), втручанням у роботу банківських систем дистанційного обслуговування «клієнт-банк», фішингом, розповсюдженням дитячої порнографії і заняттям забороненими видами господарської діяльності в мережі загального користування Інтернет, порушенням авторських і суміжних прав тощо. Для того, щоб запобігти та протидіяти кримінальним правопорушенням, які скоюють із використанням електронно-обчислювальної техніки, налагодити ефективну взаємодію між Управлінням боротьби з кіберзлочинністю МВС України та правоохоронними органами Німеччини, фахівці УБК планують продовжити обмін досвідом з іноземними колегами [4].

Висновки. Отже, з метою ефективної протидії економічній злочинності у сфері інформаційних технологій слід забезпечити: 1) організацію належної взаємодії спеціальних підрозділів правоохоронних органів по боротьбі з економічною злочинністю з уповноваженими органами іноземних держав у частині надання правової та оперативної інформації щодо фактів і обставин учинення або готування злочину в сфері економіки, а також установлення й затримання підозрюваних осіб під час кримінального провадження; 2) швидкий обмін даними щодо виявлення та розслідування злочинів у сфері економіки, а також передовим досвідом протидії цим суспільно небезпечним діянням; 3) підвищення ефективності міжнародного співробітництва в протидії транснаціональній економічній злочинності у сфері інформаційних технологій як на національному, так і міжнародному рівнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Меморандум про співробітництво між Генеральною прокуратурою України і Генеральною прокуратурою Республіки Сербія у боротьбі з транснаціональною організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом від 1 берез. 2006 р. [Електронний ресурс] / Офіц. веб-сайт Генеральної прокуратури України. – Режим доступу : http://www.gp.gov.ua/ua/department_agreements.html.

2. Працівниками відділу боротьби з кіберзлочинністю у м. Миколаєві виявлена порностудія працівниці якої, у режимі онлайн, надавали сексуальні послуги іноземним громадянам [Електронний ресурс] / Офіц. веб-сайт Міністерства внутрішніх справ України. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/publish/article/847679.

3. Навчальний семінар з питань протидії кримінальним правопорушенням у віртуальному просторі для співробітників оперативних підрозділів боротьби з кіберзлочинністю відбувся в МВС за ініціативи Посольства Великої Британії в Україні від 16 трав. 2013 [Електронний ресурс] / Офіц. веб-сайт Міністерства внутрішніх справ України. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/publish/article/846629.

4. Українські та німецькі правоохоронці об'єднались у боротьбі з кіберзлочинами [Електронний ресурс] / Офіц. веб-сайт Міністерства внутрішніх справ України. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/publish/article/845532.