БОРОТЬБА ЗІ ЗЛОЧИННІСТЮ: ТЕОРІЯ ТА ПРАКТИКА

Чернєй Володимир Васильович **–** доктор юридичних наук, доцент, ректор Національної академії внутрішніх справ

РОЛЬ ВІДОМЧОЇ ОСВІТИ ТА НАУКИ В ЗАБЕЗПЕЧЕННІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Обґрунтовано необхідність підвищення уваги до розв'язання проблем у сфері боротьби з кіберзлочинністю. Доведено, що одним із ключових питань у цьому напрямі є налагодження ефективної системи підготовки, перепідготовки й підвищення кваліфікації фахівців відповідного профілю для правоохоронних органів.

Ключові слова: кіберзлочинність; кібертероризм; протидія злочинам; фінансове шахрайство; підготовка кадрів; правоохоронні органи; МВС України; Національна академія внутрішніх справ.

Обоснована необходимость повышения внимания к решению проблем борьбы с киберпреступностью. Доказано, что одним из ключевых вопросов в этом направлении является налаживание эффективной системы подготовки, переподготовки и повышения квалификации специалистов соответствующего профиля для правоохранительных органов.

Ключевые слова: киберпреступность; кибертерроризм; противодействие преступлениям; финансовое мошенничество;

подготовка кадров; правоохранительные органы; МВД Украины; Национальная академия внутренних дел.

The article is devoted to the research of role of departmental education and science in cybercrimes combating support with provision of specialized training programs for law enforcement officers.

The article gives a detailed analysis of the cybercrime genesis and intents pointing out the recent transformation of cyberterrorism into national threat. The fact that current political situation creates specific environment for the cyberattacks to progress and damage the territorial integrity of Ukraine is stressed.

According to the article, the main danger of cyberterrorism stems in low level of the criminals traceability and amount of damage caused by financial fraud in the social sector.

The author comes to the conclusion that one of the key points to efficient cybercrime combating is the development and implementation of specialized training programs based on international experience in law enforcement educational establishments.

Keywords: cybercrime; cyberterrorism; crime combating; financial fraud; law enforcement agencies; Ministry of Interior of Ukraine; National Academy of Internal Affairs.

Ми живемо в епоху глобальної інформатизації, коли комп'ютерні та телекомунікаційні технології використовуються майже в усіх сферах життєдіяльності людини та суспільства, роблячи життя більш комфортним і динамічним. У світі, зокрема в Україні, прискореними темпами розвивається мережа Інтернет. За останні п'ять років кількість регулярних користувачів серед населення нашої держави збільшилася майже втричі й нині становить понад

20 млн осіб (у світі цей показник уже сягнув 5,5 млрд) [1, с. 3]. У структурі фінансового ринку зростає сегмент послуг електронної торгівлі, віртуальних банків, бірж, магазинів, обігу електронних грошей, он-лайн платежів тощо.

Захоплюючись перевагами телекомунікації та глобальної комп'ютерної мережі, людство й не передбачало, які можливості для зловживань надають ці привабливі технології. Кількість злочинів, учинених у кіберпросторі, збільшується прямо пропорційно до кількості користувачів комп'ютерних мереж. Так, за оцінками експертів Інтерполу, темпи зростання рівня злочинності в глобальній мережі Інтернет стали найшвидшими на планеті [2, с. 187]. Жертвами «віртуальних» злочинців сьогодні стають не лише пересічні громадяни, а й цілі відомства з власними системами інформаційної безпеки та навіть окремі держави. Безпека тисяч користувачів комп'ютерними мережами нерідко залежить від примхи кількох «хакерів». Відомими є випадки, коли правопорушники використовували малогабаритні супутникові системи зв'язку, завдяки чому вчиняли свої дії за лічені секунди на значній відстані від об'єкта посягання.

Кіберзлочини зазвичай мають корисливе спрямування, їм властиве постійне збільшення розмірів завданих збитків (лише в першому кварталі 2014 р. зафіксовано факти несанкціонованого списання коштів із рахунків підприємств, учинених шляхом утручання в роботу мережі «Клієнт-Банк», на загальну суму понад 20 млн грн) [3, с. 156]. Ідеться про різні вияви фінансового шахрайства, зокрема «фішінг» (отримання доступу до конфіденційних логінів і паролів користувачів), використання номерів чужих кредитних карток, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж фінансових установ, порушення авторських і суміжних прав, виготовлення й розповсюдження шкідливих програм, «електронне вимагання», поширення в мережі забороненого контенту, зокрема порнографічних творів, тощо.

Хоча більшість кіберзлочинів мають корисливе спрямування, останніми роками, з огляду на ускладнення соціально-політичної ситуації в країні, збільшилася кількість випадків «кібертероризму», коли комп'ютерні технології використовують для вчинення терористичних актів, екстремістської та іншої соціально шкідливої діяльності, що загрожує безпеці, конституційному ладу, обороноздатності, територіальній цілісності держави.

Залежно від намірів «кібертерористів», такі діяння можуть бути пов'язані з поширенням закликів до вчинення терористичних актів, створенням терористичних угруповань, а також будь-яким сприянням їх діяльності шляхом вербування учасників, забезпечення зв'язку, фінансування (ст. 258–258[5] Кримінального кодексу України). За допомогою ресурсів мережі Інтернет зацікавлені особи (безпосередньо або за допомогою «підставних» організацій) нерідко розпалюють національну, расову чи релігійну ворожнечу та ненависть, принижують національну честь і гідність (знущаються над історією, культурою, звичаями, традиціями нації, етнічної спільноти, релігійної конфесії), розповсюджують матеріали із закликами до насильницької зміни чи повалення конституційного ладу, захоплення державної влади, зміни меж території або державного кордону України (ст. 109, 110, 161 Кримінального кодексу України).

Серед способів «кібертероризму» найбільш поширеними можна вважати такі: збирання інформації для вчинення злочинів терористичного спрямування; формування фондів коштів для сприяння терористичним рухам; створення сайтів, що містять відомості про осіб, які підтримують тероризм; залучення до терористичної діяльності широкого кола осіб, зокрема користувачів соціальних мереж (які не завжди усвідомлюють, до яких наслідків може призвести їх необачливість у кіберпросторі).

Небезпека «кібертероризму» полягає, насамперед, у тому, що це явище не має територіальних обмежень, а отже, діяння

терористичного спрямування можуть учинюватись у будь-якому місці світу. Зазвичай виявити винних в інформаційному просторі мережі Інтернет дуже складно, оскільки вони діють через кілька пристроїв зі зміненими (за допомогою спеціального програмного забезпечення) IP-адресами, що ускладнює ідентифікацію підозрюваних і встановлення їх фактичного місця перебування.

Унаслідок значних афер у кіберпросторі злочинці одержують чималі суми грошей, що приваблює до цього бізнесу дедалі більше осіб, які мають спеціальні знання в галузі інформаційних технологій. Поступово формується нове покоління кіберзлочинців, які активно борються за перерозподіл сфер кримінального впливу. Про це свідчать викриті численні схеми незаконних оборудок із грошовими коштами, факти легалізації злочинних доходів, розширення мережі віртуальних фіктивних фірм і «конвертаційних» центрів. Найнебезпечніші вияви «кібертероризму» можуть бути пов'язані з блокуванням діяльності комунальних, диспетчерських та інших служб масового обслуговування, а також «замовними» кібератаками на бізнес, органи влади й оборонний сектор.

Серед проблем у сфері організації розслідування злочинів цієї категорії вчені виокремлюють недостатній рівень обізнаності працівників правоохоронних органів, передусім територіальних їх підрозділів, щодо особливостей реалізації протиправних схем, а також відповідних методик їх виявлення й документування [4].

З метою підвищення ефективності виявлення органами внутрішніх справ злочинів, пов'язаних із високими технологіями, ще в 2001 р. у структурі Державної служби боротьби з економічною злочинністю МВС України було створено підрозділи по боротьбі з правопорушеннями у сферах комп'ютерної інформації, електронних платежів і телекомунікацій. Пізніше, під впливом світових тенденцій

розвитку кіберпростору, стало зрозумілим, що злочинній діяльності, пов'язаній із використанням високих технологій, не можна активно протидіяти звичайними «традиційними» правоохоронними засобами. Для боротьби з цією специфічною формою кримінального бізнесу потрібні відповідно підготовлені фахівці вузькоспеціалізованих підрозділів, здатні застосовувати сучасні методи документування. З огляду на це, у структурі МВС України в 2009 р. було створено відділ (нині – Управління) боротьби з кіберзлочинністю, на який покладено організаційне та практичне забезпечення реалізації державної політики стосовно попередження та протидії злочинам і правопорушенням, що вчиняють із використанням інформаційних технологій і телекомунікаційних мереж, а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень.

Політика протидії кіберзлочинності протягом усього часу вирізнялася крайньою нестабільністю, відсутністю зваженої науково обґрунтованої концепції впливу на це явище, що має загрозливі тенденції до поширення. Позначаються прогалини в законодавчому, відомчому (міжвідомчому) регулюванні, слабка взаємодія відповідних органів, відсутність параметрів інформування зацікавлених сторін про порушення, повільне усунення причин та умов їх учинення, недостатній професіоналізм під час виявлення й розслідування злочинів. На державному рівні було неодноразово наголошено на необхідності налагодження взаємодії правоохоронних органів та інших суб'єктів у сфері запобігання і протидії кіберзлочинності, визначено завдання та роль у цьому процесі освітян, науковців, аналітиків і практиків. Специфіку та результати роботи МВС України в цьому напрямі доведено до відповідних установ і населення через засоби масової інформації, завдяки виступам на брифінгах і прес-конференціях.

З метою підвищення ефективності діяльності правоохоронних органів на Конференції Ради Європи щодо

співробітництва у сфері протидії кіберзлочинності (м. Страсбург, Франція) пріоритетними визнано заходи щодо підготовки, перепідготовки та підвищення кваліфікації співробітників відповідної спеціалізації для правоохоронних органів, здатних застосовувати сучасні методи оперативно-технічного документування та розкриття комп'ютерних злочинів, що потребує запровадження суттєвих новацій стосовно змісту й методів навчання [5, с. 241].

Специфікою підготовки працівників правоохоронних органів, які здійснюють протидію кіберзлочинам, є те, що вони повинні опанувати навички як оперативників (слідчих), так і спеціалістів у галузі комп'ютерних технологій. Крім того, зважаючи на транснаціональний характер відповідних діянь і специфіку інформаційного середовища в мережі Інтернет, такі фахівці повинні опанувати іноземні мови, насамперед англійську, а також володіти іншими технічними навичками та спеціальними знаннями.

Провідним навчальним закладом із підготовки фахівців-правоохоронців щодо протидії кіберзлочинності визначено Національну академію внутрішніх справ. Відповідно до доручень МВС України, академія з листопада 2010 р. запровадила нову спеціалізацію «Протидія кіберзлочинності» (освітньо-кваліфікаційного рівня «Спеціаліст» за спеціальністю «Правознавство»).

У вересні 2013 р. на базі навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ було створено навчально-тренувальний центр підготовки фахівців для підрозділів боротьби з кіберзлочинністю, обладнаний сучасними програмно-технічними засобами, що використовуються на практиці, новітнім навчально-методичним та наочним забезпеченням. Набір курсантів академії для навчання за новою спеціалізацією здійснюється за результатами тестування з інформатики та англійської мови, а також співбесіди, під час якої виявляють здібності курсантів щодо вирішення завдань підвищеної

складності. Водночас ураховуються запити комплектуючих органів і можливість працевлаштування випускників за спеціалізацією в регіонах, у яких широко розвинена інформаційна інфраструктура. Згідно із замовленням Міністерства внутрішніх справ України, в академії відбулося чотири випуски фахівців для підрозділів боротьби з кіберзлочинністю.

Так, розроблено освітньо-кваліфікаційну характеристику й освітньо-професійну програму. Крім «класичних» дисциплін, у межах підготовки оперативного працівника курсантам викладають додаткові спецдисципліни й спецкурси, знання яких необхідні для правоохоронців для виявлення, розкриття та розслідування кіберзлочинів, а саме: «Основи протидії кіберзлочинності», «Комп'ютерні мережі та засоби телекомунікацій», «Основи програмування», «Захист інформації в інформаційно-телекомунікаційних системах», «Комп'ютерна розвідка», «Аналітична робота в оперативно-розшуковій діяльності», «Попередження та розкриття кіберзлочинів», «Система електронних платежів», «Фінансовий аналіз», «Судова бухгалтерія», «Організація діяльності поліції (міліції) зарубіжних країн», спецкурс з іноземної мови тощо.

Науково-педагогічні працівники протягом 2013−2014 рр. підготували низку навчальних і наукових праць із цього напряму, зокрема посібники «Основи протидії кіберзлочинності», «Комп'ютерні мережі в діяльності ОВС», «Основи програмування», «Інтегрована інформаційно-пошукова система ОВС України», «Захист інформації в інформаційно-телекомунікаційних системах», підручник «Основи інформаційної безпеки», методичні рекомендації «Правові та організаційні засади використання комп'ютерного програмного забезпечення в ОВС», «Запобігання незаконному відтворенню та розповсюдженню комп'ютерних програм і баз даних», «Розслідування злочинів, пов'язаних із незаконним доступом до банківських рахунків» та ін.

Академія плідно співпрацює з профільним Управлінням, на базі якого створено кафедру боротьби з кіберзлочинністю на громадських засадах, до складу якої увійшли як представники практичних підрозділів, так і науково-педагогічні працівники академії. Підготовлено й узгоджено з УБК МВС України тематичний план підвищення кваліфікації працівників територіальних його підрозділів. Згідно з ним, слухачі мають набути знання й уміння щодо інформаційної безпеки, особливостей кваліфікації, попередження, виявлення, розкриття та розслідування злочинів у сфері високих технологій, проведення рольових ігор і тренінгів із практичним застосуванням розроблених нашими фахівцями методик протидії окремим видам злочинів, учинених із використанням комп'ютерних мереж. На сьогодні завершується спільне наукове опрацювання комплексу проблем протидії створенню «фінансових пірамід» у мережі Інтернет, а також психологічних аспектів функціонування «віртуальних» шахрайських схем. Фахівців навчального закладу залучено до робочої групи Міністерства щодо розроблення пропозицій до законодавства й інших нормативно-правових актів стосовно врегулювання процедури блокування протиправного інтернет-контенту.

Посилено й кадровий потенціал профільних кафедр і лабораторій за рахунок докторів наук та професорів зі споріднених навчальних закладів, наукових установ і відповідних практичних органів. Усвідомлюючи, що академія є спроможною забезпечити належну підготовку фахівців для підрозділів боротьби з кіберзлочинами, внесено пропозицію запровадити післядипломну підготовку фахівців із вищою юридичною освітою за спеціалізацією «Протидія кіберзлочинності» з числа осіб, які мають вищу технічну освіту в галузі знань «Інформатика та обчислювальна техніка» – випускників профільних вузів (Національного технічного університету України «Київський політехнічний інститут»,

Інституту захисту інформації Державного університету інформаційно-комунікаційних технологій, факультету захисту інформації Національного авіаційного університету тощо) або працівників ОВС із досвідом практичної роботи.

У науковому плані також проаналізовано правову регламентацію й практику протидії кіберзлочинності, узагальнено вітчизняний і зарубіжний досвід розкриття злочинів відповідного спрямування. Готуються дисертаційні дослідження щодо імплементації Україною міжнародно-правових зобов'язань стосовно відповідальності за кіберзлочини, проблем кримінологічного та криміналістичного характеру. На базі академії постійно проводяться важливі тренінги, семінари й конференції з обміну передовим досвідом щодо підготовки цієї категорії фахівців. Так, лише протягом 2012–2013 рр. викладачі, науковці та курсанти взяли участь у таких заходах міжнародного характеру: науково-практичному семінарі з питань протидії кіберзлочинності, проведеному за участі фахівців Секретної Служби США, American Express; тренінгах-семінарах англійських поліцейських щодо детального вивчення можливостей спеціалізованого програмного забезпечення для протидії кіберзлочинності («C4P» та «Netclean») та «Розслідування щодо непристойних зображень дітей он-лайн»; Міжнародній науково-практичній конференції «Вплив на кіберзлочинність на глобальному рівні технологічних досягнень: слідчі, правові й політичні аспекти приватної і державної співпраці», що відбулася за участі представників спецслужб США, Великобританії, Франції, Румунії та багатьох інших держав за підтримки Американської асоціації юристів «Ініціатива з верховенства права»; семінарі на тему «Боротьба з комп'ютерною злочинністю», який було проведено за участі заступника керівника Інспекції кримінальної міліції м. Аугсбург (Німеччина). За сприяння цієї асоціації нещодавно було проведено черговий міжнародний тренінг для оперативних

працівників ОВС України «Особливості застосування комп'ютерних технологій при розслідуванні кіберзлочинів», міжнародну науково-практичну конференцію «Боротьба з інтернет-злочинністю», що відбулася за підтримки Фонду Ганса Зайделя, міжнародну науково-практичну конференцію «Вплив на кіберзлочинність на глобальному рівні технологічних досягнень: слідчі, правові й політичні аспекти приватних і державної співпраці».

За сприяння ОБСЄ представники академії матимуть змогу в жовтні 2014 р. ознайомитися в складі делегації МВС України з роботою поліції та жандармерії Франції щодо протидії кіберзлочинам та організації навчання фахівців відповідного профілю. Безперечно, такі заходи сприяють набуттю цінного досвіду й досягненню позитивних результатів у цій нелегкій справі.

Курсанти мають змогу також на практиці закріпити отримані знання під час спілкування в межах тренінгів із працівниками зарубіжних правоохоронних органів. Так, у 2013 р. під час перебування з робочим візитом групи фахівців із боротьби з кіберзлочинністю Федерального Бюро Розслідувань США курсанти навчилися використовувати бази даних шкідливих програмних кодів «FREE». У межах договору про партнерство та співпрацю академія тісно співпрацює з Незалежною асоціацією банків. Згідно з цією угодою, представників Національної академії внутрішніх справ запрошують для проходження стажування в банківських установах – членах Асоціації, ознайомлення з існуючими в них програмно-технічними засобами протидії кіберзлочинності.

Таким чином, можна зробити висновок щодо особливої актуальності для більшості країн світу, у тому числі України, проблеми протидії поширенню кіберзлочинності, що вимагає невідкладного вирішення. Запровадження в Національній академії внутрішніх справ як провідному вищому

навчальному закладі системи МВС України нової спеціалізації «Протидія кіберзлочинності» слід уважати правильним і своєчасним заходом. Необхідною умовою підготовки фахівців належної кваліфікації для підрозділів боротьби з кіберзлочинністю є, насамперед, належний рівень матеріально-технічного забезпечення навчального процесу, розроблення та впровадження в навчальний процес нових спеціальних дисциплін, спецкурсів і тренінгів, старанне опанування курсантами навчального теоретичного матеріалу й новітніх інформаційних технологій правоохоронної діяльності, здійснення відповідного навчально-виховного процесу з курсантами, тісний взаємозв'язок навчального процесу з науковими дослідженнями та практикою правоохоронної діяльності, розширення міжнародних зв'язків. Водночас потреби практики в цілеспрямованій підготовці правоохоронців цієї спеціалізації та забезпечення повного циклу навчання зумовлюють необхідність створення в структурі Національної академії внутрішніх справ відповідного профільного факультету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про надання інформації щодо проблемних питань міжнародного співробітництва у сфері боротьби з кіберзлочинністю [Електронний ресурс] : довідка Управління боротьби з кіберзлочинністю МВС України від 15 січ. 2013 р. № 37/135. – Режим доступу :

http://mvs.gov.ua/mvs/control/main/uk/index.

2. Номоконов В. А. Интернет и преступность: криминологические и правовые аспекты взаимосвязи / В. А. Номоконов // Организованный терроризм и организованная преступность. − М., 2002. – 195 с.

3. Чернєй В. В. Кримінально-правові та кримінологічні засади запобігання злочинам у сфері діяльності небанківських

фінансових установ в Україні : [моногр.] / В. В. Чернєй. – К., 2014. – 456 с.

4. Джужа О. М. Актуальні питання підготовки майбутніх офіцерів міліції щодо протидії кіберзлочинності / О. М. Джужа // Підготовка працівників міліції (поліції): державні та міжнародні стандарти : матеріали міжнар. наук.-практ. конф. (Донецьк, 28 квіт. 2011 р.). – Донецьк : Донец. юрид. ін-т ЛДУВС ім. Е. О. Дідоренка, 2011. – С. 144–145.

5. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Вид. дім «Скіф», 2012. – 736 с.