МВС України
Харківський національний університет
внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

•

Матеріали
Міжнародної науково-практичної конференції

м. Харків, 12 листопада 2014 р.

Харків
Права людини
2014

УДК [351.74:343.85](063)
ББК 67.9(4УКР)611.31я43
А 43

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова – ректор Харківського національного університету внутрішніх справ ***Гусаров Сергій Миколайович***.

Співголова – радник ректора Харківського національного університету внутрішніх справ ***Бандурка Олександр Маркович***.

Заступник голови – перший проректор з навчально-методичної та наукової роботи Харківського національного університету внутрішніх справ ***Головко Олександр Миколайович***.

Секретар – доцент кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ ***Манжай Олександр Володимирович***.

Члени оргкомітету:

– начальник факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ***Марков В'ячеслав Валерійович***;

– начальник кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми ***Тулупов Володимир Володимирович***;

– президент Міжнародного жіночого правозахисного центру «Ла Страда – Україна» ***Левченко Катерина Борисівна***;

– начальник відділу організації наукової роботи ***Мірошниченко Оксана Станіславівна***;

– начальник відділу міжнародних зв'язків ***Осятинський Станіслав Олександрович***;

– начальник інформаційно-технічного відділу ***Полховський Олександр Миколайович***;

– начальник відділу організації служби ***Тарасенко Віталій Миколайович***;

– начальник відділу матеріального забезпечення ***Копаниця Олексій Вікторович***;

– директор загальної бібліотеки ***Процких Тамара Олексіївна***.

Друкується за рішенням оргкомітету відповідно до доручення
Харківського національного університету внутрішніх справ
від 16.10.2014 № 133.

**Матеріали видано за підтримки
Міжнародного жіночого правозахисного центру
«Ла Страда – Україна»**

ISBN 978-617-7266-01-2

ЗМІСТ

Розділ 3.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Розділ 5.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

РОЗДІЛ 1
ОКРЕМІ ПИТАННЯ ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343.1:65.012.8

Сергій Миколайович ГУСАРОВ,
ректор Харківського національного університету внутрішніх справ, доктор юридичних наук, член-кореспондент Національної академії правових наук України, заслужений юрист України

АКТУАЛЬНІ ПИТАННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Події останнього року в Україні засвідчили, наскільки важливим, а інколи критичним є належне забезпечення інформаційної безпеки держави. Не випадково однією із загроз національній безпеці в інформаційній сфері згідно зі ст. 7 Закону України «Про основи національної безпеки України» визначено комп'ютерну злочинність і комп'ютерний тероризм, а в Конституції України забезпечення інформаційної безпеки названо справою усього українського народу.

За останні роки вітчизняні правоохоронні органи значно підсилили напрям протидії кіберзлочинності. Було створено окреме Управління боротьби з кіберзлочинністю у структурі Міністерства внутрішніх справ України, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, структури із захисту інформації у складі міністерств та інших органів виконавчої влади. Також наприкінці червня 2014 року у складі Національної гвардії України було створено Управління інформаційної безпеки.

В останні місяці було активізовано зусилля із розбудови системи протидії кіберзлочинності на вищому державному рівні. Так, Указом Президента України від 24 вересня 2014 року № 744/2014 «Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності» було передбачено створення національного центру кіберзахисту і протидії кіберзагрозам.

А вже 14 жовтня 2014 року наказом Адміністрації Держспецзв'язку створено оперативну групу (координаційний центр) із питань реагування на комп'ютерні інциденти.

До складу оперативної групи входитимуть представники Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Міністерства внутрішніх справ України, Служби зовнішньої розвідки України, Міністерства оборони України та Генерального штабу Збройних Сил України, Генеральної прокуратури України, Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, представники двох десятків провідних операторів і провайдерів телекомунікацій, а також громадських організацій ІнАУ, «ТЕЛАС» та Київського відділення ISACA.

Незважаючи на значну кількість державних та недержавних суб'єктів, що спрямовують свої зусилля на подолання кіберзлочинності, левову частку цієї діяльності забезпечують підрозділи боротьби з кіберзлочинністю Міністерства внутрішніх справ України. Тільки протягом 2013 року було зареєстровано 4123 таких злочини, при цьому їх розкривання становить близько 50 %.

Головними завданнями, що постають перед органами, які беруть участь у протидії кіберзлочинності, сьогодні можна визначити:

– *внесення змін і доповнень до чинного законодавства.* Нормативно-правова база серед іншого потребує змін у частині захисту національного інформаційного простору від протиправного контенту, надання додаткових повноважень правоохоронним органам з оперативного припинення окремих видів кіберзлочинів тощо;

– *якісну підготовку та підвищення кваліфікації кадрів.* На сьогодні ці завдання виконує Харківський національний університет внутрішніх справ на підставі наказу Міністерства внутрішніх справ України «Про організацію підготовки кадрів у Харківському національному університеті внутрішніх справ» від 20.11.2012 № 1062. У серпні 2014 року університет було включено до Стратегії Ради Європи «Підготовка правоохоронних органів» у частині навчання фахівців із протидії кіберзлочинності в Україні;

– *розробку актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі* (визначення місцезнаходження особи за її мережними ідентифікаторами, перехоплення вмісту повідомлень або службової інформації цільового об'єкта, дослідження даних, у тому числі порівняння ідентифікованих та ідентифікуючих об'єктів, документування інтелектуальних слідів учинення злочину, активна дія на цільовий об'єкт);

– *удосконалення системи інформаційно-аналітичного забезпечення* (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю);

– *покращення рівня відповідної внутрішньої та зовнішньої взаємодії* (найбільш актуальним питанням є удосконалення механізму міжнародної взаємодії, адже більшість кіберзлочинів мають транснаціональний характер, а тому виникає багато проблем юрисдикційного характеру).

Харківський національний університет внутрішніх справ є активним учасником системи протидії кіберзлочинності. Зокрема на його базі було розроблено унікальну модель навчання курсантів, у рамках якої відбувається одночасне виконання курсантами завдань з охорони правопорядку, відпрацювання навичок правоохоронця на спеціальних навчально-тренувальних полігонах і розробка власного програмного забезпечення. Вказаний процес реалізується у безпосередній взаємодії з територіальними підрозділами органів внутрішніх справ на підставі укладених договорів.

Подібний проект реалізовано в університеті Пердью (штат Індіана, США), проте запропонована Харківським національним університетом внутрішніх справ модель вигідно відрізняється тим, що курсанти залучаються до роботи правоохоронних органів не лише під час проведення відповідних експертних досліджень, але й для виявлення, попередження, розкриття правопорушень та розшуку осіб.

Для реалізації моделі навчання в університеті було спроектовано навчально-тренувальний центр боротьби з кіберзлочинністю і моніторингу кіберпростору та спеціалізоване програмне забезпечення (автоматизований банк даних «Невід») для супроводження його діяльності.

Одержано 17.10.2014

УДК 343.98

Володимир Миколайович ЄВДОКИМОВ,
перший заступник Міністра внутрішніх справ України

НАУКОВІ ЗАСАДИ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Історія розвитку цивілізації повсякчас доводить свою багатогранність та, водночас, внутрішню суперечливість. Незмінним її супутником виявляється злочинність, що адаптивним феноменом пронизує все нові і нові сфери й форми соціодинаміки. Не є виключенням в цьому сенсі й кіберпростір, як віртуальний ресурсно-комунікаційний комплекс, інтеграція можливостей якого до життєдіяльності суспільства невідворотно тягне за собою й впровадження до останнього специфічних видів кримінальної активності. З'являються нові прояви злочинності – комп'ютерної, які отримують поширення при використанні нових методів, наприклад, технології Bluetooth, бездротових систем зв'язку Wi-Fi та WiMAX, піринговых мереж (P2P), спаму та інших. Крадіжки грошей з банківських карток, створення сайтів з дитячою порнографією, комп'ютерні віруси, пропаганда насильства та расової, релігійної, етнічної ненависті, інструкції з виготовлення саморобних вибухових пристроїв, кібератаки на комп'ютерні мережі державних установ – це лише мала частина злочинів, що вчиняються сьогодні у Інтернеті та яким намагаються запобігти правоохоронні органи різних країн [1]. Поширеність та суспільна небезпечність кіберзлочинів в останні роки набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави на інноваційні безпекові виклики.

Перш за все, варто зауважити на тому, що досвід протидії кіберзлочинності засвідчує неспроможність жодної окремої країни та жодного відомства автономно вирішити зазначену проблему. Успіх можуть гарантувати лише спільні дії, як державних, так і комерційних структур, в тому числі й у міжнародному контактному форматі.

Задля ефективної протидії будь-яким проявам кіберзлочинності та більш швидкого і повного розкриття злочинів у цій сфері правоохоронні органи повинні взаємодіяти із суб'єктами ринку телекомунікаційних послуг, зокрема операторами та провайдерами. Зазначена взаємодія повинна ґрунтуватися на зобов'язані відповідних працівників цих організацій в залежності від функціональних обов'язків або їх власників повідомляти про будь-які випадки незаконного використання мережі,

а також всіма доступними в межах закону засобами сприяти виявленню, припиненню, розслідуванню та іншим заходам протидії кіберзлочинам. На наш погляд, налагодження таких зв'язків можливе через законодавче врегулювання відповідальності зазначених осіб за відмову від співробітництва (ненадання інформації, непредставлення доступу до мережі тощо) обов'язково із позбавленням права зайняття такою діяльністю, а для самих організацій – припинення діяльності.

Необхідним напрямком діяльності правоохоронних органів є удосконалення заходів взаємодії з підприємствами, установами, організаціями, діяльністю яких є розробка комп'ютерної техніки та програмного забезпечення. Така взаємодія має декілька цілей: по-перше, відстежувати осіб, які мають певні знання у цій сфері (особливо тих, які звільнилися та офіційно не працевлаштувалися або стали займатися індивідуальною підприємницькою діяльністю), тобто можуть бути потенційними суб'єктами аналізованих злочинів; по-друге, покращення форм та методів діяльності на підставі отримання інформації відносно розвитку комп'ютерних технологій; по-третє, удосконалення програмного забезпечення власних систем через перейняття досвіду.

Також зауважимо, що доцільним заходом протидії кіберзлочинності є підтримання та розширення співробітництва відповідних правоохоронних органів з міжнародними організаціями, що спрямовують свою діяльність у зазначеній сфері. В цьому сенсі позитивним слід визнати досвід «відпрацювання» у 2011 р. Службою безпеки України разом з НАТО загальних механізмів боротьби з кіберзлочинністю, результатом чого стало розроблення експертних консультацій відносно кібернетичного захисту [2]. Переконані, що зазначений напрям взаємодій слід й надалі розвивати, інтенсифікувати.

Дотичним до цього аспектом взаємодії суб'єктів протидії кіберзлочинності є приєднання відповідних підрозділів правоохоронних органів до міжнародних програм, що створюються та організовуються різними державами на підставі договорів та угод. Так, наприклад, відповідно до Конвенції «Про кіберзлочинність», держави-учасники (в тому числі й Україна) повинні здійснити організаційні заходи щодо розробки необхідних умов (зокрема, організація контактних пунктів) на національному рівні, та приєднатися до мережі щоденного цілодобового доступу (міжнародне позначення «24/7 Network» або «доступ 24 години 7 діб на тиждень»), що спрямована на співпрацю та надання допомоги при розкритті та розслідуванні

кіберзлочинів [3, с. 29]. В Україні органом, на який покладаються повноваження щодо створення та 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, є Міністерство внутрішніх справ України. Але, на сучасному етапі, не зважаючи на обов'язковість, зазначені умови не були виконані у необхідному обсязі. Укладення вказаних угод та приєднання до подібних програм є необхідним кроком для здійснення та розроблення заходів розкриття та протидії аналізованим злочинам.

Крім того, необхідним кроком міжнародної взаємодії, в зазначеній сфері, є не лише організація та прийняття участі у вказаних мережах, а й укладання угод, з відповідними підрозділами правоохоронних органів інших країн, з метою обміну інформацією відносно вчинених кіберзлочинів (способів, методів, застосованих технічних або інших засобів тощо) та заходів, які застосовуються щодо їх запобігання та розкриття. Нині, наприклад, чинним є Меморандум «Про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом» [4]. Налагодження подібних зв'язків є необхідною умовою оперативного та повного обміну інформацією у вказаній сфері.

Необхідною умовою протидії кіберзлочинності, на наш погляд, є також взаємодія органів внутрішніх справ з вітчизняними та міжнародними неурядовими організаціями, окремими підприємствами, що створюються на добровільних началах і мають за мету захист інформаційної інфраструктури. Так, наприклад, ще на початку 1990-х років була створена організація FIRST – форум команд реагування на інциденти, яка об'єднує 80 бригад реагування, які складаються із працівників державних, комерційних, промислових та навчальних установ з 19 країн світу. Здійснення зазначених заходів дозволить, по-перше, слідкувати за процесами розвитку комп'ютерних технологій та програмного забезпечення, по-друге, обмінюватися досвідом у сфері протидії аналізованим злочинам, по-третє, слідкувати за існуванням підприємств, установ та організацій, що здійснюють діяльність або надають послуги у вказаній сфері.

Гадаємо, викладені міркування, які, безумовно, мають набути подальшого теоретичного розвитку та прикладного

застосування, повинні сприяти вдосконаленню системи протидії кіберзлочинності.

Список використаних джерел:

1. Борьба с киберпреступностью – задача международного уровня / SecurityLab.ru. – 01 июня 2009 г. [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/380617.php.

2. СБУ отрабатывает с НАТО механизмы борьбы с киберпреступностью [Електронний ресурс]. – Режим доступу: http://za.zubr.in.ua/2011/10/18/13536/.

3. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів / В. М. Бабакін // Форум права. – 2011. – № 4. – С. 27–30 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2011_4_6.pdf.

4. Меморандум про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом : від 09.09.2009 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/528_031.

Одержано 25.09.2014

УДК 343.98

Сергій Васильович ДЕМЕДЮК,
начальник Управління боротьби з кіберзлочинністю МВС України

ОКРЕМІ АСПЕКТИ КРИМІНОГЕННОЇ СИТУАЦІЇ У КІБЕРСФЕРІ В УКРАЇНІ

З часу, коли до Кримінального кодексу України внесли окремий розділ, що містить склади злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, пройшло більше 13 років. За цей час коло кіберзлочинів значно розширилось. Стало очевидним, що за допомогою комп'ютерної техніки можна вчинити практично будь-який злочин. Вказане зумовило створення окремого підрозділу для боротьби з цим злом – Управління боротьби з кіберзлочинністю у складі МВС України.

Діяльність цього підрозділу є досить динамічною та потребує значного інтелектуального потенціалу правоохоронців, що обумовлено високою швидкістю розвитку техніки, мобільністю кіберзлочинців їх нерідкою високоосвіченістю у технічній сфері.

На сьогоднішній день розкриття зареєстрованих кіберзлочинів складає близько 50 %. Крім того, постійно змінюється криміногенна ситуація у країні як загалом, так і щодо сфери кіберзлочинності. На підтвердження цього проаналізуємо окремі

дані, що характеризують часовий розвиток злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Варто відзначити, що починаючи із 2002 до 2012 року фіксувалася незначна кількість таких злочинів, що, на нашу думку, обумовлено їх високою латентністю (рис. 1). Втім із прийняттям нового Кримінального процесуального кодексу ситуація дещо змінилася, що підтверджується вивченням двох останніх дев'ятимісячних проміжків.

Так, за 9 місяців 2013 року зареєстровано 549 таких злочинів, за 9 місяців 2014–362 (-34,06 %). Зауважимо, що за 9 місяців 2013 року загальна кількість кримінальних правопорушень цієї категорії, за вчинення яких особам вручено повідомлення про підозру, становила 216 з 549 зареєстрованих (39,3 %), за аналогічний період 2014 року ці показники становлять 184, 362 та 50,8 % відповідно.

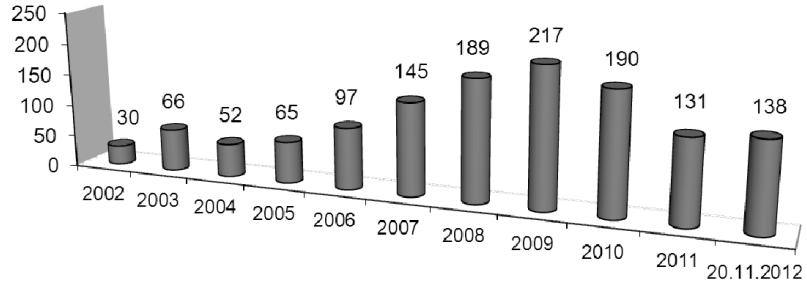

Рис. 1. Відомості про зареєстровані злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за 2002–2012 рр.

Аналіз структури досліджуваної категорії злочинів за ступенем тяжкості демонструє незмінність частки тяжких злочинів – 45,36 % у 2013 році та 46,13 % у 2014. Разом з тим частка злочинів середньої тяжкості знизилася з 46,81 % (2013 рік) до 43,65 % (2014 рік), а злочинів невеликої тяжкості збільшилась з 7,83 % до 10,22 % відповідно.

Частка злочинів, вчинених особами, які раніше вчиняли кримінальні правопорушення склала 8,00 % (2013) та 6,37 % (2014), групою осіб зросла з 5,5 % (2013) до 9,55 % (2014).

Вказане опосередковано підтверджує тенденцію до збільшення організованості національної кіберзлочинності. Це є характерним для усього світу. Якщо раніше кіберзлочини вчиняли

здебільшого одинаки-професіонали, не пов'язані із злочинним світом, то сьогодні таку діяльність беруть на озброєння організовані злочинні угруповання. Це стає дохідним бізнесом.

Також прогнозовано спостерігається сплеск кіберправопорушень на територіях України, де проводиться антитерористична операція. Уявна безкарність стимулює правопорушників з частини Донецької та Луганської областей до вчинення інтернет-шахрайств, розповсюдження дитячої порнографії, вчинення атак на державні та приватні інформаційні ресурси тощо.

Все це дає підстави до активізації зусиль із протидії кіберзлочинності в Україні, і не лише силами держави, але й відповідних приватних підприємств, установ та організацій, стимулює впровадження в Україні єдиної консолідованої системи боротьби з кіберзлочинністю, здатної адекватно реагувати на виклики XXI сторіччя.

Одержано 30.10.2014

УДК 343.98

Богдан Анатолійович БУРБЕЛО,
викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ

Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни. З розвитком і вдосконаленням глобальних комунікаційних мереж, комп'ютерного забезпечення відбувається і еволюція кримінального середовища як окремо взятої держави, так і всього світового співтовариства в цілому. Більш того, під впливом сучасних глобалізаційних процесів, зокрема глибокого проникнення Інтернету, інформаційна безпека набуває відносно самостійного наднаціонального характеру. Наднаціональна природа кіберзлочинності зумовлюється технологічними можливостями кіберпростору, що значною мірою розмивають державні адміністративно-територіальні кордони та ідентифікаційні характеристики суб'єктів. Така сутність кіберзлочинності висуває особливі вимоги до стратегії і тактики формування виваженої державної політики забезпечення інформаційної безпеки, яка повинна передбачати систему заходів державного та міжнародного характеру, належне місце в якому займатиме протидія кіберзлочинності.

Кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі Інтернет, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Це і дитяча порнографія, шахрайства, несанкціоноване втручання в роботу комп'ютерних і телекомунікаційних мереж, виготовлення та поширення шкідливих програм, викрадення ідентифікаційних даних осіб, електронне вимагання та інші.

Боротьба з кіберзлочинністю ускладнена наявними особливостями, а саме: латентністю кіберзлочинів; можливістю знищення або зміни комп'ютерної інформації, що є доказом вчинення злочину; виникненням проблеми огляду комп'ютерних систем, вилучення і дослідження слідів вчинення кіберзлочинів, які зберігаються в пам'яті технічних пристроїв, в електромагнітному полі, на машинних носіях комп'ютерної інформації; короткочасність зберігання інформації здатної виступити в якості доказів на серверах компаній – операторів телекомунікаційних мереж тощо.

Враховуючи суспільну небезпеку, виражену латентність, складність розслідування неправомірного доступу до комп'ютерної інформації, а так само наявний світовий досвід, особливу увагу, на наш погляд, необхідно приділяти питанням попередження та профілактики даних злочинів.

Результати наукових досліджень свідчать, що протидія злочинності в широкому розумінні включає у себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності. У такому розумінні система протидії злочинності корелюється з класичними гарантіями законності. Акцентуючи увагу на протидії кіберзлочинності, їх можна узагальнено представити у вигляді системи гарантій законності в інформаційній сфері, яка є правовою стороною системи діяльності по забезпеченню інформаційної безпеки. Для цього необхідний постійний активний процес розробки дієвих заходів, спрямованих на правове, організаційне, включаючи криміналістичне, технічне, забезпечення боротьби зі злочинами у сфері комп'ютерної інформації, а також вдосконалення методики їх розслідування та попередження.

На нашу думку, ефективними способами профілактики кіберзлочинності є вдосконалення науково-технічних засобів,

тактичних прийомів і методів розслідування неправомірного доступу до комп'ютерної інформації; своєчасне виявлення і припинення як розпочатих злочинів, так і неправомірного доступу до комп'ютерної інформації на стадії замаху або підготовки до нього; встановлення обставин, що сприяли вчиненню кожного злочину, розробка і вдосконалення методів і прийомів виявлення таких обставин.

У ході розслідування неправомірного доступу до комп'ютерної інформації слідчому необхідно максимально використовувати спеціальні знання експертів і фахівців, а також оперативну інформацію. Проведенню кожної слідчої дії повинна передувати ретельна підготовка, що включає в себе: вивчення та аналіз матеріалів кримінального провадження, вибір місця, часу проведення слідчої дії, визначення складу учасників та їх інструктаж, підбір технічних засобів фіксації результатів проведення слідчої дії, а при необхідності також підготовку комп'ютерно-технічних, програмних та інших засобів.

З метою зниження ризику несанкціонованого доступу до комп'ютерної інформації юридичних осіб необхідно: наявність посадової особи або підрозділу, що відповідає за безпеку комп'ютерної інформації; контролювання доступу співробітників до елементів управління засобів комп'ютерної техніки; використання складних паролів і їх своєчасна зміна; укладання договорів з працівниками на предмет нерозголошення охоронюваної комп'ютерної інформації; періодичне створення резервних копій комп'ютерної інформації, а також дотримання термінів їх зберігання тощо. Враховуючи всю складність і небезпеку кіберзлочинів, на шляху вироблення рішення проблеми боротьби з кіберзлочинністю, як інформаційної безпеки державного забезпечення виникає цілий комплекс технічних і юридичних проблем пов'язаних з відсутністю: 1) відповідних законодавчих актів; 2) спеціально підготовлених кадрів (оперативного та слідчого апарату, що спеціалізується на виявлення і розкриття злочинів у інформаційно-телекомунікаційній сфері); 3) необхідних технічних засобів.

Необхідною умовою підготовки фахівців належної кваліфікації для боротьби з кіберзлочинністю є тісний взаємозв'язок навчального процесу з науковими дослідженнями і практикою правоохоронної діяльності, розширення міжнародних зв'язків.

Одержано 17.10.2014

УДК 004.056.53

Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Віталій Миколайович КІЙКОВ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ DDOS-АТАК

Для сучасного світу характерним є збільшення політичної та економічної напруги у кіберпросторі, на теренах якого і відбувається інформаційна війна. Одним із поширених методів проведення кібератак є всім відомі DDoS-атаки.

В першу чергу під таки атаки підпадають державні установи та web-ресурси новин, які так чи інакше освітлюють події в окремих країнах та світі у цілому.

Розглянемо більш детально найбільш популярні у наш час DDoS-атаки і можливі тенденції їх розвитку у майбутньому.

Перше чим відрізняються DDoS-атаки 2013 и 2014 років від попередніх, є використання декілька векторів вразливості. Як відомо, для ураження цілі і нанесення гарантованого збитку достатньо одного вектора, у зв'язку з чим вірогідність успішності багатовекторної атаки збільшується. Крім того, така тактика збиває з пантелику IT-персонал атакованої організації.

Розглядаючи DDoS-атаки у цілому, в 2014 році продовжують домінувати атаки, націлені на веб-ресурси, як найбільш швидкодіючий вектор. Починаючи з 2013 року прослідкується чітке зростання DDoS-атак на програмні застосування як результат наявності розвернутих за останні роки в організаціях систем захисту від мережевих DDoS-атак. Крім того, мережевим атакам значно легше протидіяти та вони не відносяться до категорії атак, яким тяжко запобігти [1].

Сьогодні більшість засобів відбиття атак є достатньо розвинутими і організації можуть доволі довгий час протидіяти DDoS-атакам, націлених на мережу та програмні застосування без ущербу IT-інфраструктурі. Але зловмисники можуть використовувати багато векторів атаки в пошуку тих слабких місць, які не передбачені рішенням відбиття DDoS-атак, що

розвернуті в організації. Більше половини випадків – це DDoS-атаки з п'ятьма і більше векторами.

Часто атакуючі не планують використання усього спектру передбаченого арсеналу, даючи «жертві» можливість обробляти вектора атаки послідовно. У випадку блокування одного вектора атаки, атакуючими зловмисниками буде задіяний наступний. Це приводить к тому, що під час масованої DDoS-атаки буде хоча б один вектор, який не зможе бути відбитий і досягне кінцевої мети.

В більшості випадків результат DDoS-атаки – це непрацюючий, або повільно працюючий веб-сервер, але в останній час DDoS-атаки орієнтовані не тільки на веб-сервера. Основними цілями сучасних DDoS-атак все частіше стають інтернет-канал та між мережевий екран.

Ще однією особливістю сучасних DDoS-атак є значне скорочення циклів впровадження нових методів в обхід системи захисту [2]. Один із основних векторів, який приводить до такого результату – це атаки типа HTTP-флуд. Вони по починаються коли атакуючий направляє велику кількість HTTP GET/POST запитів, підриваючи ресурси сервера.

При цьому, хоча HTTP-атаки залишаються найбільш розповсюдженими, SSL-шифровані атаки залишаються небезпечними, оскільки їм важко протидіяти.

Шахрайство, хакерська активність, а також довгий список вимог приватності призвів до використання організаціями HTTPS-протоколу і шифрування комунікацій автоматично. Відповідно до дослідження ринку, більше 90 % організацій використовують HTTPS для любої публічно доступної взаємодії по WEB. Зазвичай HTTPS-повідомлення розшифровуються на дуже пізній стадії внутрішньої мережі організації.

Зловмисники використовують цю функцію зашифрованих повідомлень як засіб обходу рішень безпеки (анті-DoS/DDoS, брандмауера і IPS / IDS), які врешті не фіксують атаку.

Додатково цікавою особливістю на базі SSL DoS/DDoS-атак є асиметрична природа шифрування SSL, особливість якого у тому, що роз шифровка повідомлень займає майже в десять разів більше ресурсів ніж його шифрування.

Використовуючи цю асиметричну особливість, зловмисники можуть створити вельми руйнівну атаку з відносно низькими ресурсами. Використовуючи методи обходу систем захисту, атакуючим вдається доставити шкідливі повідомлення вглиб до мережі, де сервери і різні модулі більш вразливі до високого об'єму трафіку для спостереження підозрілих затримок чи повного відключення. SSL-шифровані атаки – новий тренд, який

буде збільшуватись з роками і за прогнозами у 2017 році більше половини DDoS-атак будуть SSL-шифрованими.

Таким чином, DDoS-атаки є і будуть в найближчі роки найбільш популярним засобом для нанесення економічних збитків від простою онлайн-сервісів, а також для підриву репутації політичних та медійних організацій шляхом відмови у обслуговуванні офіційних веб-сайтів. Такі атаки отримали особливий інкремент розвитку при збільшенні політичного та економічного протистояння у світі, що робить їх більш непередбачуваними. Усі вказані вище фактори змушують відповідні організації розглядати питання розробки та розвитку систем захисту від таких атак.

Список використаних джерел:

1. Ледовской В. Современные DDoS-атаки и защита от них с помощью Radware Attack Mitigation System [Електронний ресурс] / Валерий Ледовской ; Аналит. центр Anti-Malware.ru. – Режим доступу: http://www.antimalware.ru/analytics/DDoS_protection_Radware_Attack_Mitigation_System. – 27.03.2013.

2. Quarterly Global DDoS Attack Report: Q2 2013 / Akamai [Електронний ресурс]. – Режим доступу: http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q2.html. – July 17, 2013.

Одержано 13.10.2014

УДК 340.11

Євгеній Геннадійович ГОРДІЄНКО,
курсант факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ;

Олександр Вікторович КАРАЧЕВЧЕВ,
курсант факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ЗАПОБІГАННЯ ЗЛОЧИНАМ У СФЕРІ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Докорінні зміни політичного, соціального й економічного характеру в Україні, за два останні десятиліття, охопили всі сфери суспільного життя та вагомо вплинули на стан злочинності, її кількісні показники, а також структуру і характер. Так, у процесуальному розумінні значно розширилися та ускладнилися способи вчинення злочинів. Наприклад, злочинці розпочали активно використовувати для вчинення злочинів нові технічні засоби та знаряддя. Окрім того, підвищилася мобільність злочинців та їх технічна оснащеність. Наведене стосується також

й злочинів у сфері комп'ютерних технологій. Адже в процесі інформатизації відбувається й комп'ютеризація злочинності. Причому, злочини у сфері комп'ютерних технологій характеризуються підвищеним рівнем латентності, яка, в свою чергу, зумовлена технічною й соціальною специфікою.

Запобігання злочинам у сфері комп'ютерних технологій як діяльність, направлена на виявлення й усунення обставин, що сприяли вчиненню злочину, є складною і багатоаспектною проблемою. Під запобіганням злочинам необхідно розуміти діяльність, пов'язану з реалізацією системи заходів, направлених на виявлення і усунення обставин, що сприяють вчиненню злочинів та інших правопорушень. Означене дає підстави стверджувати, що запобігання злочинам охоплює виявлення обставин, які сприяли вчиненню злочину у межах конкретного діяння. З тих причин, сформовані та впроваджені висновки і пропозиції, одержані в результаті дослідження діяльності, спрямованої на запобігання злочинам у сфері комп'ютерних технологій є основою для дослідження обставин, що сприяють вчиненню злочину або ж його профілактики в майбутньому в сфері інформатизації суспільства.

Наведене дає підстави для висновків про те, що запобігання злочинам у сфері комп'ютерних технологій полягає у своєчасному встановленні та усунені обставин, що сприяли вчиненню злочину з дотриманням принципу всебічності, повноти та істинності. Лише таким чином буде забезпечено повне та якісне кримінальне провадження у сфері комп'ютерних технологій.

Запобігання злочинам у сфері комп'ютерних технологій полягає у розумінні негативного впливу, під час його вчинення, на комп'ютерну інформацію. Означений вплив може бути різного характеру: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, коректну за формою і змістом), ознайомлення з нею сторонніх осіб.

Варто виокремити також й ті обставини, які сприяли формуванню самої причини вчинення злочину у сфері комп'ютерних технологій. Доцільно погодитися з позицією науковці щодо розподілу обставин, що сприяли вчиненню комп'ютерних злочинів на три групи. До першої необхідно віднести обставини, в яких функціонує комп'ютерна техніка потерпілого. До другої виділено обставини щодо сучасного розвитку інноваційних технологій та технічного рівня знань особи, яка вчинила злочин у Сфері комп'ютерних технологій. До третьої групи – інші обставини про особу комп'ютерного правопорушника.

У запобіганні злочинам у сфері комп'ютерних технологій пріоритет повинен віддаватися соціальному аспекту. Профілактичні

дії безпосередньо щодо особи, яка може вчинити комп'ютерний злочин, є більш ефективними, ніж профілактичні заходи щодо вдосконалення систем захисту інформації. У першому випадку результатом профілактичного впливу є відмова особи від вчинення злочину, оскільки її морально-правова свідомість підвищується. У другому випадку результатом буде, як правило, вчинення незакінченого злочину (приготування або замах на злочин), який завжди спричиняє шкоду суспільним відносинам.

До перепон на шляху запобігання злочинам у сфері комп'ютерних технологій відносимо: 1) відсутність достатньої кількості відповідних засобів у системі органів досудового розслідування; 2) недосконалості знань, вмінь і навичок посадових осіб органів досудового розслідування у питаннях застосування означених засобів; 3) відсутності необхідних тактичних рекомендацій щодо їхнього застосування.

Запобігання злочинам у сфері комп'ютерних технологій, з залученням новітніх інформаційних технологій є можливим за умов наявності належно автоматизованого робочого місця працівників досудового розслідування, обладнаного комп'ютерною технікою, веб-камерою, системними програмами тощо. Застосування цих засобів є виправданим мінімальними витратами часу, фізичних та розумових зусиль, а також фінансових ресурсів.

Одержано 31.10.2014

УДК 343.1

Тетяна Іванівна ГУДЗЬ,
кандидат юридичних наук,
старший викладач кафедри конституційного та міжнародного права
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ПРАВОВІ ЗАСАДИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

В епоху інформаційного суспільства комп'ютери та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, що, у свою чергу, дає можливість для зловживань. Кількість злочинів, скоєних у кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж. За оцінками Інтерполу, темпи росту злочинності, наприклад, у глобальній мережі Інтернет, є найшвидшими на планеті. У XXI ст. світовим співтовариством все більше приділяється уваги злочинності,

пов'язаній з використанням комп'ютерів. Кіберзлочинність – за визначенням ООН – будь-який злочин, який може вчинятися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, скоєний в електронному середовищі.

Небезпеку кіберзлочинності визнають й українські правоохоронні органи, що підтверджує необхідність вивчення правових засад боротьби з кіберзлочинністю в Україні.

Правову основу діяльності органів та підрозділів по боротьбі з кіберзлочинністю в нашій державі становлять Конституція України, Конвенції Ради Європи «Про кіберзлочинність» 2001 р. та «Про захист осіб стосовно автономізованої обробки персональних даних» 1981 р., Кримінальний і Кримінальний процесуальний кодекси України, закони України «Про міліцію», «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про авторське право і суміжні права», й інші законодавчі акти України, нормативно-правові акти Міністерства внутрішніх справ України, чинні міжнародні договори.

Серед правових засад боротьби з кіберзлочинністю в Україні важливе місце посідає прийнята Радою Європи у 2001 р. «Конвенції про кіберзлочинність».

Конвенція складається з чотирьох розділів. Перший розділ присвячений визначенню термінів. Разом з тим, Конвенція не дає відповіді на питання «що таке кіберзлочинність», а увага авторів зосереджується на поняттях «комп'ютерна система», «комп'ютерні дані», «постачальник послуг».

У другому розділі визначаються види злочинів. Відповідно до Конвенції злочини у кіберпросторі поділені на чотири групи. Перша група включає правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем злочинів. Сюди увійшли такі правопорушення як незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в ст. 2–5 Конвенцій, але й комп'ютерні паролі, коди доступу та їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або до будь-якої її частини (з урахуванням злочинного наміру).

Друга група охоплює злочини, пов'язані з комп'ютером: підробка та шахрайство з використанням комп'ютерних технологій (ст. 7, 8 Конвенції). Третю групу складають злочини, пов'язані з контентом (змістом) даних, а саме правопорушення, пов'язані з дитячою порнографією (ст. 9 Конвенції). До четвертої групи правопорушень увійшли порушення авторського права і суміжних прав (ст. 10).

Третій розділ визначає загальні та конкретні принципи міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства, з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень. Приділено увагу питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі.

Прикінцеві положення знайшли закріплення у четвертому розділі.

Правовою основою боротьби з кіберзлочинністю на національному рівні є Кримінальний кодекс України, у якому окремі види комп'ютерних злочинів (кіберзлочинів) виділено в розділ VI Особливої частини – Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361, 363). Окремі види злочинів, у яких комп'ютерні продукти визначені як засіб злочину, розміщені також і в інших розділах Особливої частини. Наприклад, у розділі V Особливої частини зазначені окремі види злочинів, у яких комп'ютерні продукти визначені як засіб злочину (ст. 163, 176, 177) та Злочини у сфері господарської діяльності (ст. 200) в розділі VII.

В Україні з метою забезпечення реалізації державної політики у сфері боротьби з кіберзлочинністю, організації та здійснення відповідно до законодавства оперативно-розшукової діяльності, у складі кримінальної міліції МВС України було створено Управління боротьби з кіберзлочинністю.

Одним з основних завдань Управління є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку,

а також іншим кримінальним правопорушенням, учиненим з їх використанням. У тому числі: кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері; надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище кримінальних правопорушень).

Таким чином, виконання зазначених завдань має ґрунтуватись на міцній правовій базі. Правову основу діяльності органів та підрозділів по боротьбі з кіберзлочинністю в Україні відіграють як національні, так і міжнародні правові акти. Особливе місце в процесі боротьби з кіберзлочинністю відіграє прийнята у 2001 р. Радою Європи «Конвенція про кіберзлочинність», яка стала підґрунтям для уніфікації національного законодавства щодо регулювання правовідносини у сфері глобальної комп'ютерної мережі.

Одержано 14.10.2014

УДК 343.98

Ірина Олександрівна БАНДУРКА,
кандидат юридичних наук,
доцент кафедри кримінального права і кримінології
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА ПРАВА ТА СВОБОДИ ДИТИНИ

На сьогодні інформація виступає одним із найважливіших факторів системи суспільних відносин, а забезпечення інформаційної безпеки визнається одним із фундаментальних чинників його подальшого розвитку. Саме тому особливого значення набуває захист та протидія суспільно небезпечним явищам, що мають прояви в інформаційній сфері, зокрема,

протидія кіберзлочинності. Найбільш ураженими від негативного впливу інформації та кіберзлочинів є діти. А тому і питання захисту дітей від даних видів злочинів є одним із найактуальніших на сьогодні.

Вивченням даної тематики займалися такі вчені, як О. В. Швед, К. Б. Левченко, О. А. Удалова та І. П. Руденко, О. М. Бандурка, В. М. Куц, Б. В. Лизогуб, С. С. Мірошниченко, О. М. Подільчак, А. М. Толочко, В. В. Корольчук, Т. Л. Кальченко.

На даний час законодавством України термін «кіберзлочинність» безпосередньо не визначено. Європейська Конвенція про кіберзлочинність також не надає конкретизованого визначення, хоча і окреслює коло суспільно-небезпечних діянь, що повинні набути статусу кіберзлочинів на рівні національного законодавства. До них належать: незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання у дані, втручання у систему, зловживання пристроями, підробка та шахрайство пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав [1].

Проте, беручи до уваги напрацювання вчених і світову практику протидії даному явищу, можна виділити специфічні його ознаки, а саме: транснаціональний характер злочинності,оскільки для даного явища національні кордони не є перешкодою; висока латентність, адже постраждалі від даного виду злочинів не завжди заявляють про це правоохоронним органам, до того ж виявлення, фіксація і вилучення доказової інформації є складним процесом; «розповсюдженість» знарядь для вчинення таких злочинів в силу широкого використання комп'ютерної техніки в повсякденному житті; відсутність сталості явища кіберзлочинності, тому що комп'ютерні технології щоденно вдосконалюються [2].

Оскільки основним засобом вчинення кіберзлочинів є саме інформація, то важливо врахувати, що саме її розповсюдження через засоби масової інформації, Інтернет, друковані видання здійснюється шкідливий вплив на найменш захищений прошарок населення – дітей.

Сьогодні телебачення та Інтернет залишаються найбільш масовим і доступним засобом інформації. За даними соціологічних досліджень, телебачення та Інтернет займають одне з провідних місць за силою виховного впливу після сім'ї і школи, будучи каналом інтенсивної соціалізації. Особливістю сприйняття дитини є переважання емоційного ставлення до об'єктів дійсності за відсутності глибоких знань про них.

Отримання через засоби масової інформації негативної інформації досить часто стає причиною формування у дітей особистості злочинця, скоєння ними суспільно небезпечних діянь а також бути потерпілими від злочинів.

Найбільш розповсюдженим кіберзлочином є правопорушення пов'язані з дитячою порнографією. Порнографія стала багатомілліардним комерційним промислом і входить в число найбільш зростаючих компаній в Інтернеті. Діти є легкодоступними, а дитяча порнографія, у свою чергу є простою і недорогою у виробництві, а також тим більше в тих умовах, коли на неї є величезний споживчий ринок. Виготовлення такого роду продукції є надзвичайно вигідною справою, особливо коли практично немає ризику, набагато менше, ніж, наприклад, нелегальний бізнес зі зброєю, або розповсюдження наркотиків.

Запобігання даному виду злочину відображено не тільки на національному рівні, а й на міжнародному. Так, існують три міжнародно-правові акти, що стосуються протидії посиленню дитячої порнографії: Факультативний протокол до Конвенції про права дитини щодо торгівлі, дитячої проституції і дитячої порнографії, Конвенція про права дитини, та Конвенція Ради Європи про кіберзлочинність. Всі ці акти ратифіковані Україною, та їх виконання забезпечується на національному рівні.

Хоча Конвенція про права дитини є документом, що направлений на забезпечення широкого спектру прав та свобод дитини, у статті 34 чітко зазначено що держави-учасниці зобов'язані захищати дитину від усіх форм сексуальної експлуатації та сексуальних розбещень, вживати всіх необхідних заходів щодо запобігання використання дітей з метою експлуатації у порнографії та порнографічних матеріалах [3].

Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії в свою чергу є першим міжнародним документом, в якому даються визначення основних термінів. Так, у статті 2 Конвенції визначено чітко вказано, що порнографія – зображення будь-якими засобами дитини, яка здійснює реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головним чином в сексуальних цілях. У статті 3 міститься чітка вимога до держав-учасниць щодо притягнення до кримінальної відповідальності за дитячу порнографію, здійснених на національному та транснаціональному рівні, в індивідуальному чи організованому порядку. Також зазначено можливість притягнення до кримінальної відповідальності за просте володіння такими порноматеріалами,

навіть без наміру їх розповсюджувати. Ця стаття відображає поняття про те, що для боротьби з цією проблемою потрібен комплексний підхід. У статті 10 йдеться про необхідність міжнародного співробітництва, адже дитяча порнографія легко розповсюджується, тому багато злочинців можуть уникнути покарання [4].

Конвенція Ради Європи про кіберзлочинність містить рекомендацію що до встановлення як кримінального злочину виробництво дитячої порнографії з метою поширення через комп'ютерну систему, пропозицією або розповсюдження дитячої порнографії через комп'ютерну систему, придбання дитячої порнографії через комп'ютерну систему для себе або для іншої особи, володіння дитячою порнографією у комп'ютерній системі чи на інших інформаційно-зберігаючих пристроях [5].

На національному рівні вищезазначений злочин регулюється статтею 301 Кримінального кодексу України, що передбачає покарання за ввезення, виготовлення, збут і розповсюдження порнографічних предметів. Частина другої цієї статті передбачає покарання за ті самі дії, вчиненні щодо кіно – та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру. Разом з тим частина третя статті 301 Кримінального кодексу України встановлює відповідальність за ті самі дії вчиненні, щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію, або примушування неповнолітніх до участі у створенні творів, зображень або кіно – та відеопродукції, комп'ютерних програм порнографічного характеру [6].

Ефективні механізми боротьби з кіберзлочинами, а зокрема і з дитячою порнографією в комунікаційних мережах досі відсутні.

Більшість дослідників не заглиблювались до цього напряму, ігноруючи слідом за законодавцем неприродність поєднання в одній кримінально-правовій забороні питань створення та обігу порнографічної продукції з питаннями неправомірного впливу на людину для залучення її до цього процесу.

Автор цієї статті вбачає можливість розділення закріпленої в статті 301 Кримінального кодексу України кримінально-правової заборони на дві окремі. Внаслідок такого розділення першою охоплюватимуться дії щодо втягнення особи у створення порнографічних предметів, а другою – обіг предметів порнографічного характеру.

Простих змін у законодавстві не достатньо тому, звісно, на сучасному етапі розроблена низка програм щодо подолання даної проблеми, відбуваються постійні консультації, конференції, форуми та дебати як у всьому світі, так і в Україні, але необхідні конкретні заходи протидії цьому виду злочину, насамперед, в підготовці фахівців, які були б здатні розкривати та розслідувати кіберзлочини.

Потрібна також належно організована система комплексних превентивних заходів всіх суб'єктів протидії кіберзлочинності, організація міжнародного обміну досвідом боротьби зі злочинами у галузі високих технологій та кібертероризмом, проведення досліджень кримінально-правових та кримінологокриміналістичних проблем злочинності у сфері використання комп'ютерних технологій з метою надання науково-методичної допомоги законодавцям, вченим, правоохоронним органам, державним та комерційним організаціям, громадськості.

Список використаних джерел:

1. Про ратифікацію Конвенції про кіберзлочинність : закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

2. Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій : посібник / М. І. Камлик, Б. В. Романюк, В. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк ; за заг. ред. Я. Ю. Кондратьєва. – Київ : НАВСУ, 2000. – 64 с.

3. Конвенція про права дитини : ратиф. постановою Верховної Ради України від 27.02.1991 № 789-XII [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_021.

4. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії : від 03.04.2003 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_b09.

5. Конвенція [Ради Європи] про кіберзлочинність : від 23.11.2001 ; ратиф. Україною 07.09.2005 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

6. Кримінальний кодекс України. – Київ : Право, 2003. – 176 с.

Одержано 24.09.2014

УДК 343

Ганна Олександрівна ГОНЧАРОВА,
студент інституту підготовки кадрів для органів юстиції України Національного юридичного університету імені Ярослава Мудрого (м. Харків)

СВІТУ – ОФІЦІЙНЕ ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРЗЛОЧИННІСТЬ», АБО НЕДОЛІКИ ЗАКОНОДАВЧОЇ ОСНОВИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Поява та розвиток всесвітньої мережі Інтернет обумовила виникнення нового виду злочинності – кіберзлочинності, яка стає дедалі поширенішою та небезпечнішою. У зв'язку з цим постає питання забезпечення ефективної протидії зазначеному виду злочинності.

Законодавчою основою забезпечення протидії будь-якому прояву злочинності є національне законодавство та міжнародні договори, ратифіковані певною країною. Нажаль, ані законодавство зарубіжних країн, ані законодавство України не позбавлено недоліків у цій сфері, зокрема жоден нормативно-правовий акт не містить офіційного визначення «кіберзлочинність». Отож, постає питання розробки нових категорій та термінів і втілення їх в законодавство України та зарубіжних країн.

Цієї проблеми у своїх працях торкалися такі фахівці, як Ю. Батурін, В. Вехов, В. Голубев, М. Діхтяренко, Б. Романюк, О. Снегірьов та інші.

Це питання є важливим, оскільки прийнято вже декілька міжнародних документів, що стосуються кіберзлочинності, у країнах розроблені програми із запобігання та боротьби з кіберзлочинами, внесені зміни та доповнення до кримінальних кодексів, але досі не наведено жодного офіційного визначення кіберзлочинності.

Видатною подією у сфері боротьби із кіберзлочинністю стало підписання країнами Європи у 2001 р. Конвенції Ради Європи про кіберзлочинність, яку Україна ратифікувала у 2005 р.

Проте, навіть зазначена Конвенція не дає визначення кіберзлочинів, а також інших, пов'язаних з цим понять з префіксом «кібер», лише визначаючи перелік протиправних діянь, за які на національному рівні має встановлюватися кримінальна відповідальність або перелічуючи ознаки таких діянь.

Згідно з рекомендаціями експертів ООН, термін «кіберзлочинність» охоплює будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі, проти комп'ютерної системи

або мережі. Інакше кажучи, до кіберзлочинів відносяться такі суспільно небезпечні діяння, які здійснюються в кіберпросторі за допомогою або з використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Тобто, як у міжнародних правових актах, так і в національному законодавстві України та зарубіжних країн,офіційного визначення поняття «кіберзлочин» ще не дано. До того ж більшість з них на позначення цього явища використовує термін «комп'ютерні злочини».

Наприклад, в Іспанії правовою доктриною так визначено зміст категорії «комп'ютерний злочин»:

1) дії, які спрямовані на знищення або стирання програм чи їхніх складових, заміну, знищення накопиченої інформації, необґрунтоване використання комп'ютера (ЕОМ);

2) дії проти держави, національної безпеки, найближчого оточення, майна тощо.

В Італії один з важливих законодавчих актів, що стосуються комп'ютерних злочинів – це Закон № 547 від 23 грудня 1993 р. про «Зміни та внесення нових статей щодо комп'ютерних злочинів у Кримінальний кодекс».

Згідно з цим законом комп'ютерні злочини – це злочини, вчинені з використанням комп'ютерних технологій, від персонального комп'ютера до портативного телефонного апарата, забезпеченого мікрочипом.

У російськомовній літературі перевага також віддається поняттю «комп'ютерна злочинність». Ймовірно, це зумовлено тим, що єдина глава у Кримінальному кодексі РФ, яка передбачає відповідальність за злочини, об'єктом яких є інформація та інформаційні системи, має назву «Злочини у сфері комп'ютерної інформації».

Використовують поняття «комп'ютерні злочини» й вітчизняні науковці. Так, В. Б. Вєхов під останньою розуміє передбачені законом суспільно небезпечні дії, вчинені з використанням засобів електронно-обчислювальної техніки.

Тобто більшість розуміють терміни «кіберзлочинність» та «комп'ютерний злочин» як синоніми. На їх відмінності наголошують В. А. Номоконов та Т. Л. Тропіна, стверджуючи, що перше є ширшим та більш точно відображує сутність такого явища, як злочинність в інформаційному просторі. До того ж, Рада Європи у листопаді 2001 приймаючи Конвенцію про кіберзлочинність, застосувала саме термін «cybercrime», а не «computer crime».

Окрім цього, на сьогодні думки вчених з питань правової оцінки злочинів у сфері комп'ютерних технологій розходяться.

Одні під «комп'ютерними» злочинами розуміють протиправні діяння, де комп'ютер є або об'єктом, або знаряддям злочинного посягання. Інші вважають, що об'єктом посягання є інформація, яка обробляється в комп'ютерній системі, а комп'ютер слугує знаряддям посягання.

Підсумовуючи, можна сказати, що законодавче закріплення поняття «кіберзлочинність» є вкрай необхідним. До того ж краще буде, якщо таке закріплення відбудеться на міжнародному рівні. Це сприятиме одноманітному розумінню та застосуванню цього поняття, а відтак і розробці ефективних законодавчих та підзаконних нормативних актів, щодо протидії кіберзлочинності.

Одержано 02.10.2014

УДК 343.98

Ігор Володимирович КОБЗЕВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційної та економічної безпеки
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ;

Діана Олександрівна РУДЕНКО,
кандидат технічних наук, доцент,
доцент кафедри інформатики
Харківського національного університету радіоелектроніки

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ – ПРІОРИТЕТНИЙ НАПРЯМ РОБОТИ ПРАВООХОРОННИХ ОРГАНІВ КРАЇНИ

Глобальні світові процеси в поєднанні з інтенсивною інформатизацією сучасного суспільства зумовлюють ряд явищ, які визначають пріоритетність напрямів державної політики у сфері забезпечення як національної безпеки в цілому, так і кожній з її складових. На теперішній час інформаційна сфера складає одну з основ життєдіяльності суспільства, а забезпечення інформаційної безпеки держави визнається одним з основних чинників в його подальшому розвитку. За таких умов особливого значення набуває нейтралізація негативного впливу і подолання суспільно небезпечних фактів, які мають прояви в інформаційній сфері. Одним з таких явищ є кіберзлочинність.

На сьогодні можна виділити такі основні тенденції розвитку комп'ютерної злочинності в Україні: високі темпи росту;

корислива мотивація більшості вчинених комп'ютерних злочинів; вдосконалення способів скоєння комп'ютерних злочинів і поява нових видів протиправної діяльності у сфері інформаційних технологій; ріст професіоналізму комп'ютерних злочинців; омолоджування комп'ютерної злочинності і ріст числа осіб, які раніше не притягувалися до карної відповідальності; збільшення матеріальних збитків від комп'ютерних злочинів в загальній частці втрат від інших видів злочинів; перенесення центру тяжіння на скоєння комп'ютерних злочинів з використанням комп'ютерних мереж; переростання комп'ютерної злочинності в розряд транснаціональної злочинності; високий рівень латентності комп'ютерних злочинів.

Оскільки Internet взагалі нікому конкретно не належить, ніким конкретно не регулюється, то немає і адміністративної інстанції, яка відповідає за Інтернет. Положення ускладнюється ще і тим, що інформація може зберігатися на Web-сайтах в інших країнах або на інших континентах, де законодавство не передбачає відповідальність за зберігання і поширення забороненого контенту [1]. Проблема повинна вирішуватися на міжнародному рівні, можливо у рамках таких організацій, як ООН і ЮНЕСКО.

Результати аналізу характеристики комп'ютерної злочинності дозволяють прогнозувати подальше ускладнення боротьби з нею з огляду на те, що скоєння комп'ютерних злочинів з кожним роком набувають усе більш витонченого характеру. До вирішення цієї проблеми необхідно підходити комплексно.

Фахівці виділяють наступні елементи організації діяльності правоохоронних органів в глобальних інформаційних мережах: вивчення і оцінка обстановки в мережах; здійснення оптимальної розстановки сил і засобів, забезпечення взаємодії; управління, планування і контроль; координація дій суб'єктів правоохоронних органів.

Важливим елементом системи заходів боротьби з комп'ютерною злочинністю є заходи превентивного характеру, або заходи попередження. Більшість іноземних фахівців вказують на те, що попередити комп'ютерний злочин набагато легше і простіше, ніж розкрити і розслідувати його [2]. Зазвичай виділяють три основні групи заходів з попередження комп'ютерних злочинів, до яких можна віднести правові, організаційно-технічні і криміналістичні.

Усі інтереси в інформаційній сфері підрозділяються на інтереси особи, держави і суспільства. Проблема кіберзлочинності нині зачіпає, як цілі країни, так і окремі особи. Виходячи

з вищесказаного, можна зробити висновок, що протидія кіберзлочинності – це важлива частина державної політики в області захисту національних інтересів.

Кіберзлочинність вже стала великою проблемою для всього світу. Правоохоронні органи намагаються боротися з нею, законодавці ухвалюють нові закони, правоохоронні структури формують спеціальні підрозділи по боротьбі з кіберзлочинністю. Щоб успішно боротися з кіберзлочинністю, повинні притягуватися фахівці в області інформаційних технологій і ті активні члени суспільства, яких зачіпає злочинна діяльність, яка знайшла сприятливе середовище - віртуальний простір.

У рамках державної політики необхідно створити уніфіковану класифікацію і формальну модель кіберзлочинів. Це сприятиме протидії і розслідуванню злочинів такого роду. Організація забезпечення інформаційної безпеки повинна носити комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків. При цьому важливо не упустити ніяких істотних аспектів. Аналіз негативних наслідків передбачає обов'язкову ідентифікацію можливих джерел загроз, чинників, які сприяють їх прояви і, як наслідок, визначення актуальних загроз інформаційної безпеки.

Для ефективної протидії кіберзлочинності зусиль що робляться тільки на національному рівні явно недостатньо. Потрібна розробка, стандартизація і уніфікація законодавства і програмних засобів, що дозволить визначати місцезнаходження злочинців, які протиправно використовують комп'ютерні мережі і глобальні телекомунікаційні системи. Усе це і намагаються робити країни, які підписали Європейську конвенцію по боротьбі з кіберзлочинністю.

Список використаних джерел:

1. Цензура в Интернете, Россия и другие страны мира // Cheap domain.ru [Електронний ресурс]. – Режим доступу: http://www.cheap-domain.ru/censura-v-internete/. – 23 февр. 2013 г.

2. Вехов В. Б. Предупреждение компьютерных преступлений мира [Електронний ресурс] // Компьютерные преступления: способы совершения, методики расследования / В. Б. Вехов. – М., 1996. – Глава 4. – Режим доступу: http://www.pravo.vuzlib.org/book_z404_page_5.html.

Одержано 02.10.2014

УДК 65.012.8+004

Дмитро Юрійович КРОЛЕНКО,
студент факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

КІБЕРЗЛОЧИННІСТЬ: DOS-АТАКИ ЯК ЇЇ РІЗНОВИД

Кіберзлочинність – протизаконні дії, що здійснюються людьми, котрі використовують інформаційні технології для досягнення кримінальних цілей. Серед основних видів кіберзлочинності виділяють розповсюдження шкідливих програм, виламування паролів, викрадання номерів кредитних карток та інших банківських реквізитів, розповсюдження протиправної інформації через Інтернет та інформаційні атаки (DOS-атаки) на сайти крупних підприємств або державних установ.

Протягом року були неодноразово атаковані DOS-атаками сайти Адміністрації Президента, Кабінету Міністрів та особливо сайт Міністерства внутрішніх справ. У такі моменти зростає необхідність актуальної та правдивої інформації, саме через це питання безперебійного функціонування сайтів державних органів стає більш важливим.

Що ж таке DOS-атака? Ця абревіатура розшифровується як Denial of Service – відмова в обслуговуванні. Це атака на обчислювальну систему, котра виражається у створенні дуже великої кількості запитів, направлених на один конкретний сайт з ціллю його перевантаження. В DOS-атаці можуть брати участь як хакери, так і звичайні користувачі, що робить протистояння цьому типу атак більш тяжким. Тому зазвичай результатом таких операцій стає або повне відключення серверу певного сайту або організації, або дуже сильне уповільнення його роботи. Існує доволі багато різноманітних методів DOS-атак, кожний з котрих направлений на ти чи інші слабкі місця у комп'ютерних системах.

На даний момент заходи безпеки проти DOS-атак поділяються на активні та пасивні, а також на превентивні та реакційні. Можна зазначити основні методи:

– запобігання – дуже часто такі атаки викликані різними образами (в тому числі релігійними, політичними), тому потрібно своєчасно зреагувати на джерело образи;

– відповідні заходи – в наш час існує багато компаній котрі допомагають знайти навіть організаторів таких атак, а далі, використовуючи технічні і правові норми можна притягнути організаторів до відповідальності;

– програмне забезпечення – зазвичай підходить для невеликих та середніх компаній. Виражається у придбанні окремого серверу;

– фільтрація трафіку – блокування запитів, котрі йдуть від атакуючих ЕОМ. Основна проблема такого методу – неможливість відрізнити DOS-атаку від звичайних користувачів;

– зворотній DOS – перенаправлення трафіку, котрий використовується для атаки, на атакуючого – при достатній потужності можна вивести з ладу його сервер;

– виявлення та усунення вразливостей у сервері – доволі ефективний метод, окрім DOS-атак основаних на флуді (відправлення великої кількості повідомлень, потребуючих відповідей, та підміна IP-адреси атакуючого на IP-адрес жертви, котра таким чином і отримає усі відповіді) – при такій атаці мова йде про обмеженість ресурсів, а не про їх захищеність;

– розосередження – побудова розподілених та дубльованих систем, котрі продовжать обслуговування клієнтів незалежно від DOS-атаки на їх певну частину;

– ухилення – відведення безпосередньої цілі атаки подалі від ресурсів, котрі також підверглися DOS-атаці;

– придбання спеціального програмного або апаратного забезпечення.

Найбільш відомими DOS-атаками на території України є атаки першого лютого 2012 року на урядові сайти, пов'язані з припиненням функціонування файлообміннику ex.ua, та атаки тридцятого листопада 2013 року після зіткнень між опозицією та силами спецпідрозділу МВС «Беркут».

У наш час кібератаки стають все більш потужним та розповсюдженим засобом кіберзлочинців для атак на сайти органів влади та крупних компаній тому зростає необхідність тісної співпраці між інтернет-провайдерами та силовими структурами задля виявлення та запобігання таких атак. Також необхідно вдосконалити міжнародне законодавство з точки зору протидії кіберзлочинності та збільшити ступінь взаємодії на міждержавному рівні.

Одержано 28.10.2014

УДК 343.13(477)

Ірина Володимирівна ЛЄШУКОВА,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРЗЛОЧИННОСТІ

У XXI столітті ми не можемо заперечувати важливість інформаційних технологій, які заполонили майже всі сфери життєдіяльності. Нова історична фаза розвитку цивілізації – інформаційне суспільство – поступово набирає обертів, несучи з собою не тільки позитивні, а й свої негативні тенденції та явища. Як свідчить статистика, українці все більше користуються благами інформаційної ери та намагаються використовувати всі можливості електронної взаємодії, як то спілкування, торгівлю, сплату рахунків і отримання заробітної плати через електронні засоби або за допомогою Інтернету. Не зважаючи на зручність і швидкість сучасних засобів зв'язку, використання інформаційних технологій викликало новий вид злочинів, які загально можна окреслити як кіберзлочини.

На сьогодні мусимо констатувати, що законодавство України є недосконалим у сфері боротьби з кіберзлочинністю. Наразі у вітчизняному законодавстві не міститься навіть визначення поняття «кіберзлочинності», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерних систем та мереж електрозв'язку. Якщо ж говорити про нормативну базу, яка хоч якось торкається цього питання, то слід звернутися передусім до Закону «Про основи національної безпеки України» від 19.06.2003, у якому визначено, що на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві є в інформаційній сфері комп'ютерна злочинність та комп'ютерний тероризм [1]. Однак, що розуміється під терміном «комп'ютерний тероризм» законодавець у цьому Законі не визначає. На наш погляд, комп'ютерний тероризм є лише одним із видів злочинів у сфері інформаційних технологій і об'єднувати його з більш загальним поняттям як-то кіберзлочинність є некоректним як із теоретичної, так і з практичної точки зору.

У 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність і таким чином імплементувала положення міжнародного акта у вітчизняне законодавство. Зокрема, Конвенцією

пропонується розмежування кіберзлочинів залежно від об'єкта правовідносин. Так, до злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відносяться незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями; до злочинів, пов'язаних з комп'ютерами – підробка та шахрайство; до злочинів пов'язаних зі змістом – вироблення дитячої порнографії, пропонування або надання доступу до дитячої порнографії, розповсюдження, передача, здобуття дитячої порнографії за допомогою комп'ютерних і володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації; до злочинів щодо порушення авторських і суміжних прав – правопорушення, за які передбачено кримінальну відповідальність Паризьким актом від 24.07.1971 щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності, Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція) тощо. Проте, як відомо, українські правоохоронні органи майже не використовують у своїй практиці міжнародні правові норми, тому говорити про перенесення міжнародних стандартів на вітчизняну практику боротьби з кіберзлочинністю передчасно.

Чинний Кримінальний процесуальний кодекс не містить положення, які дають змогу використовувати докази в електронній формі. Таким чином, фактично відсутня можливість доказування наявності того чи іншого протиправного діяння, пов'язаного з рухом інформації в електронному вигляді в реальному масштабі часу. Саме рух інформації в цифровому вигляді є об'єктом протиправних діянь, які кваліфікуються як кіберзлочини. Наразі єдиним способом використання електронної інформації як доказів у суді є висновок експерта. Отже, доказами у кримінальній справі можуть бути використанні висновки комп'ютерно-технічної експертизи, виконаної відповідно до Закону України «Про судову експертизу». Позитивним в цьому аспекті є можливість здійснення експертизи не тільки в державних спеціалізованих установах, а й у незалежних експертів, які атестовані в порядку, визначеному законодавством України.

Слід зазначити, що в Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 р., а відповідні територіальні підрозділи почали створюватися лише на початку 2012 р. Специфіка роботи зазначеного підрозділу полягає не тільки у знанні правових аспектів і законодавчих норм, які є підставами для притягнення до відповідальності за кіберзлочини, а й глибоке знання технічної сторони

діяння, тобто співробітник правоохоронного органу має добре володіти інформаційними технологіями, бути обізнаними у принципах роботи мереж і пристроїв, які використовуються для вчинення правопорушень, а також бути в курсі останніх розробок у сфері ІТ-індустрії.

Таким чином, вважаємо, що вдосконалення нормативно-правового забезпечення у сфері попередження та протидії кіберзлочинності, можливе за наступними напрямами: 1) внесення змін до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій; 2) визнання електронних документів та інших даних у якості доказової бази при розслідуванні кіберзлочинів; 3) запровадження практики ідентифікації користувача Інтернет шляхом надання ідентифікаційного коду особи оператору зв'язку, при подачі письмової заяви про укладення договору на надання послуг; 4) обов'язку банків безкоштовно в обов'язковому порядку підключати послугу СМС інформування у частині здійснення будь-яких операцій за поточними картковими рахунками.

Список використаних джерел:

1. Про основи національної безпеки України : закон України від 19 черв. 2003 р. № 964-IV [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/964-15.

Одержано 20.10.2014

УДК 322.2

Борис Володимирович КУЗЬМЕНКО,
доктор технічних наук, професор,
професор кафедри комп'ютерно-інформаційних
інформаційних систем і технологій
Міжрегіональної академії управління персоналом (м. Київ);

Юрій Олександрович ЗАІКА,
доктор юридичних наук, професор,
завідувач кафедри цивільного права і процесу
Національної академії внутрішніх справ (м. Київ)

КІБЕРЗЛОЧИННІСТЬ ТА ВІРТУАЛЬНИЙ КРИМІНАЛІТЕТ, ПРОБЛЕМИ ВІТЧИЗНЯНОЇ НОРМАТИВНО-ПРАВОВОЇ БАЗИ

Для багатьох Інтернет, інформаційні технології, давно стали невід'ємною частиною життя всього українського суспільства, в тому числі і для криміналітету. Розрахунки в режимі онлайн українці здійснюють користуючись банківськими картками різних міжнародних систем. Достатньо великий обсяг коштів через віртуальний простір став мішенню для легкого

«заробітку» он-лайнових злодіїв. Разом з тим українська нормативно-правова база в сфері протидії злочинам в кіберпросторі не задовольняє потреб, і не охоплює всі ключові елементи для протидії всім наявним кіберзлочинам. Нині в Україні діють Закони України та нормативні документи, мета яких полягає в забезпеченні кібербезпеки держави. Це Закони України «Про державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України». Також діє два стратегічних документа: Стратегія національної безпеки України та Доктрина інформаційної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (статті 361–363). Проте в своїй більшості вітчизняне нормативно-правове поле у сфері інформаційної безпеки оперує дефініціями визначень яких фактично немає. Ряд законів не містять визначень вживаних термінів і понять, вільно використовуються не узгоджені між собою терміни (наприклад термін «комп'ютерна злочинність» у Законі України «Про основи національної безпеки України» та ін.). Велика кількість загроз, що пов'язана із використанням сучасних ІКТ, мають більш широкі та і комплексні наслідки. В зв'язку цим є потреба внесення суттєвих змін як до чинного законодавства, та діючого Кримінального кодексу України.

Іншою проблемою є координація діяльності правоохоронних структур та правового унормування зон відповідальності відомств, процедур взаємодії та засобів комплексного реагування на загрози кібербезпеці держави. Потребує визначення і поняття «критична інформаційна інфраструктура», узагальненим поняттям може бути: критична інформаційна інфраструктура держави – це сукупність інформаційно-телекомунікаційних систем держави та приватного сектору, які забезпечують функціонування та безпеку стратегічних інститутів держави і безпеку громадян.

Сучасне інформаційне законодавство України не має чіткої, ієрархічної побудови, єдності, комплексності, це викликає суперечливе тлумачення та застосування його норм на практиці, зокрема через те, що окремі цілісні проблеми вирішуються в різних нормативних актах фрагментарно і без узгодження між собою. При цьому не враховується специфіка традиційної

правової доктрини, за якою сформовано національну ментальність нашого населення, юридичної науки, інші особливості соціального та державного устрою. Законодавство України у сфері інформаційних відносин має ряд недоліків: по-перше, різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без належного узгодження понятійного апарату. Вони мають ряд термінів, що є недостатньо коректними, не викликають однозначної суспільної інформаційної рефлексії, або взагалі не мають чіткого визначення свого змісту. Термінологічні неточності та різне тлумачення близьких за формою і змістом понять та категорій призводить до їх неоднозначного розуміння і застосування на практиці, що викликає соціальну ентропію (невизначеність). Це породжує соціальні конфлікти в інформаційних правовідносинах та правовий хаос; у сфері боротьби зі злочинністю створено умови для можливого маніпулювання при визначенні ознак злочину, що, у свою чергу, дає змогу уникати правопорушникам відповідальності; по-друге, велика кількість законів та підзаконних нормативних актів у сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування, в першу чергу працівниками правоохоронних органів у боротьбі з комп'ютерною злочинністю, а особливо такою, що має ознаки організованої. Це призводить до зниження рівня виявлення, розкриття та доведення до суду кримінальних справ про такі злочини в Україні.

Для вирішення питань правового забезпечення боротьби з негативними проявами у сфері інформатизації України серед інших заходів, визначених у вітчизняному інформаційному законодавстві, необхідно: постійно проводити всебічний аналіз стану боротьби з право порушеннями в інформаційній сфері, особливо стосовно злочинів, здійснюваних в організованому порядку злочинними угрупуваннями; аналізувати стан правового регулювання та застосування законодавства, в тому числі і кримінального, про соціальні інформаційні відносини в умовах інформатизації України та становлення інституціонального інформаційного суспільства; науково-дослідні установи мають дослідити питання систематизації вітчизняного права у сфері соціальних інформаційних відносин та напрацювати фундаментальні методичні рекомендацій боротьби з комп'ютерною злочинністю.

Одержано 30.10.2014

УДК 343.98

Юрій Миколайович ОНИЩЕНКО,
*викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;*

Петро Євгенійович МИНКО,
*кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних технологій і систем управління
Харківського регіонального інституту Національної академії
державного управління при Президентові України*

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ЧАСТИНА ДЕРЖАВНОЇ СТРАТЕГІЇ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Кібербезпека все частіше розглядається, як стратегічна проблема державної важливості, що зачіпає усі шари суспільства. Державна політика кібербезпеки служить засобом посилення безпеки і надійності інформаційних систем держави. Щодо стратегії кібербезпеки застосовується високорівневий і низхідний підхід: висувається ряд державних цілей і пріоритетів, які необхідно досягти за певний проміжок часу. Фактично, стратегія є моделлю рішення задачі кібербезпеки усередині держави.

Перші стратегії кібербезпеки почали з'являтися на початку попереднього десятиліття. Однією з перших країн, яка стала сприймати кібербезпеку, як питання державної важливості були Сполучені Штати Америки. У 2003 році в США опублікована Національна стратегія безпеки в кіберпросторі [1]. У подальші роки по всій Європі почали поширюватися плани заходів і стратегії, покликані вирішити подібне завдання.

У 2005 році Германія приймає Державний план захисту інформаційної інфраструктури. Наступного року Швеція розробляє Стратегію посилення безпеки Інтернету в Швеції (Strategy to improve Internet security in Sweden). Услід за великою кібератакою в 2007 році Естонія стала однією з перших країн-членів Євросоюзу, що опублікувала в 2008 році широку державну стратегію кібербезпеки [2]. Відтоді в цій сфері на державному рівні була виконана велика робота, і в останні чотири роки десять країн – членів Євросоюзу опублікували свої державні стратегії кібербезпеки.

Як на європейському, так і на міжнародному рівні погодженого визначення кібербезпеки немає [3]. У кожній країні визначення кібербезпеки та інших ключових термінів може значно розрізнятися. Як наслідок, розрізняються і підходи до

складання стратегій кібербезпеки. Відсутність спільної «мови» і підходу ускладнює процес міжнародної співпраці, в той час як важливість співпраці визнається усіма країнами.

Як правило, в стратегії кібербезпеки зачіпаються наступні теми:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення відповідного механізму (в основному суспільно-державного партнерства), що дозволяє приватним і державним зацікавленим сторонам обговорювати і затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування і визначення необхідних політик і регулюючих механізмів, чітке позначення ролей, прав і відповідальності для приватного і державного сектора (наприклад, нова законодавча база для боротьби з кіберзлочинністю, обов'язкове інформування про інциденти безпеки, базові заходи забезпечення безпеки, нові норми матеріально-технічного забезпечення);

– визначення цілей і способів розвитку державних можливостей і необхідної законодавчої бази для вступу в міжнародну боротьбу з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі основних активів, сервісів і взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв і механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного і інтегрованого підходу до державного управління ризиками.

15 вересня 2014 року Адміністрація Держспецзв'язку подала до Кабінету Міністрів України проект Закону України «Про основні засади забезпечення кібербезпеки України». Цей законопроект визначає правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Для всебічного комплексного опрацювання питання забезпечення кібербезпеки в України було створено міжвідомчу робочу групу з питань розробки та узгодження законопроекту. Доопрацьований спільними зусиллями законопроект було погоджено зацікавленими державними органами. За результатами проведення його правової експертизи отримано позитивний висновок Мін'юсту, що дозволило подати його до Кабінету Міністрів України на розгляд [4]. Прийняття Верховною Радою України Закону України «Про основні засади забезпечення

кібербезпеки України» має стати вагомим кроком на шляху формування національної системи кібербезпеки.

Список використаних джерел:

1. National Strategy to Secure Cyberspace [Електронний ресурс]. – Режим доступу: http://www.dhs.gov/national-strategy-secure-cyberspace. – Official website of the Department of Homeland Security.

2. Cyber Security Strategy [Електронний ресурс] / Cyber Security Strategy Committee. – Tallinn : Ministry of Defence ESTONIA, 2008. – 36 p. – Режим доступу: http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

3. Ten National Cyber Security Strategies: a Comparison [Електронний ресурс]/ H. A. M. Luiijf, Kim Besseling, Maartje Spoelstra, Patrick De Graaf // Lecture Notes in Computer Science. – 2013. – Vol. 6983. Critical Information Infrastructure Security : 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8–9, 2011, Revised Selected Papers. – P 1–17. – Режим доступу: http://link.springer.com/chapter/10.1007/978-3-642-41476-3_1.

4. Держспецзв'язку внесла на розгляд Уряду України законопроект «Про основні засади забезпечення кібербезпеки України» / Пресслужба Держспецзв'язку [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=116076&cat_id=112509. – 17 верес. 2014 р.

Одержано 13.10.2014

УДК 347.734(477)

Ваган Саркісович СИМОВ'ЯН,
здобувач
Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ У БАНКІВСЬКІЙ СФЕРІ

Широке використання сучасних інформаційних систем у діяльності банківських установ та інших установ, як державної, так і приватної форми власності, піднімає проблему протидії кіберзлочинності. Останнє є одним із головних напрямків діяльності системи безпеки акціонерно-комерційного банку, яка направлена на захист законних інтересів від протиправних посягань. Внаслідок кібератак виникає серйозна загроза належній реалізації основних прав та свобод осіб (клієнтів, засновників банку тощо) у фінансовій сфері життєдіяльності суспільства. Так, виникає загроза несанкціонованого доступу до приватної, конфіденційної та іншої інформації, її знищення чи пошкодження. Інформатизація діяльності акціонерно-комерційного банку може стати серйозною загрозою для банківської таємниці та прав й свобод фізичних і юридичних осіб.

Питання протидії кіберзлочинності досліджувалось у працях багатьох вчених, а саме О. М. Бандурки, Є. В. Карманова, Н. Ф. Казакова, Ю. М. Онищенка, О. В. Орлова, В. С. Симов'яна, М. В. Старицького, А. О. Селіванова та інших. Однак, зважаючи на стрімкий розвиток інформаційних технологій, комп'ютеризації усіх сфер суспільного життя загалом та діяльності акціонерно-комерційного банку зокрема, глобалізаційних процесів в українському суспільстві, розвиток міжбанківських відносин та ряд інших факторів виникає необхідність подальшого більш детального дослідження проблеми протидії кіберзлочинності у банківській системі.

Нажаль, Україна у сфері протидії кіберзлочинності стала четвертою країною за кількістю вихідних кібератак. Передували нашій країні тільки Російська Федерація, Тайвань та Німеччина [1, с. 2]. Означене відбувається внаслідок недосконалої правової регламентації та реалізації адміністративної, кримінальної відповідальності за вчинення правопорушень означеної категорії, неефективної діяльності правоохоронних структур, органів державної влади, до повноважень яких входить протидія кіберзлочинам тощо.

Міжнародна спільнота приділяє значну увагу боротьбі із кібезлочинами [2–4]. Щорічні збитки від таких протиправних дій складають значні суми, а кількість кіберзлочинів демонструє динаміку до зростання. До того ж, кіберзлочинність, з огляду на її ознаки – відсутність кордонів, вчинення злочинів у віртуальному просторі, як правило, знаходження злочинця на великій відстані від місця вчинення злочину (навіть за межами країни або континенту) – ставить перед правоохоронними органами всього світу нові виклики та змушує об'єднувати зусилля [5].

Внаслідок означеного непоодинокими стали випадки кібернападів на інформаційні системи акціонерно-комерційних банків України. Зважаючи на останні тенденції вчинення правопорушень вказаної категорії їх можна класифікувати за такими критеріями:

– «класичні» правопорушення у банківській сфері, що здійснюються із використанням комп'ютерних технологій та персональної інформації, що надається потерпілою особою. У даній категорії правопорушення на будь-якій із стадій його вчинення залучається потерпіла особа. Так, наприклад, правопорушник, представляючись працівником банку, обманом дізнається необхідну для злочину інформацію. До даної категорії можна віднести й інші шахрайства, що вчиняються із використанням комп'ютерних технологій тощо;

– «новітні» правопорушення у діяльності банківських установ. Вказані кібератаки здійснюються без залучення потерпілої особи та стають можливими лише завдяки новітнім інформаційним технологіям. Так, наприклад, створення надсучасної вірусної програми для незаконного збору персональних даних клієнтів акціонерно-комерційного банку, отримання частково або повністю інформації, що містить банківську таємницю тощо.

Задля протидії кіберзлочинності та унеможливлення нанесення збитків інтересам банківської установи та інтересам осіб, яких вона представляє, акціонерно-комерційні банки вживають такі заходи протидії:

– здійснюють відповідний **підбір кадрового персоналу**. Так, наприклад, підвищують критерії відбору до кандидатів на посаду акціонерно-комерційного банку (особа обов'язково повинна мати відповідну освіту, особлива увага звертається на морально-вольові критерії особи);

– використовують **надсучасні інформаційні системи** захисту інформації;

– залучають **кваліфікованих спеціалістів** для роботи із комп'ютерним устаткуванням;

– працюють над **розробкою власних антихакерських програм**;

– створюють власні **бази даних осіб**, які були причетними до вчинення кіберзлочинів;

– створюють власні **бази даних, що містять відомості про способи** вчинення правопорушення та програми, які при цьому застосовувались;

– **співпрацюють із іншими банківським установами**, щодо обміну інформацією про осіб, способи вчинення кіберзлочинів тощо.

Оскільки Україна є одним із світових лідерів за рівнем кіберзлочинності, існує гостра необхідність удосконалення діяльності банківських структур щодо протидії означеним правопорушенням, покращення міжбанківської співпраці та взаємодії з правоохоронними органами. Стрімкий розвиток комп'ютерних злочинів у фінансовій сфері зумовлює і належний розвиток заходів протидії, з боку акціонерно-комерційних банків України.

Список використаних джерел:

1. Орлов О. В. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю [Електронний ресурс] / О. В. Орлов, Ю. М. Онищенко // Теорія та практика державного управління. – 2013. – Вип. 3 (42). – С. 1–6. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/tpdu/2013-3/doc/1/01.pdf.

2. Украина – один из лидеров по количеству кибератак в мире // Украинская правда [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/rus/news/2013/03/8/6985180. – 08.03.2013.

3. Йона О. О. Світові тенденції боротьби із кіберзлочинністю / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204). – Ч. 1. – С. 59–61.

4. Голубев В. А. Аналіз кіберзлочинності у сфері економічної безпеки / В. А. Голубев // Інформаційна технологія та безпека. – 2013. – № 1 (3). – С. 26–32.

5. Делегація МВС України взяла участь у конференції поліцій країн Дунайського регіону / УЗГ МВС України [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/printable_article/843584. – 08.05.2013.

Одержано 24.09.2014

УДК 343.346.8:004.056.53

Вікторія Євгенівна СТРУКОВА,
старший викладач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ;

Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ

ПРО ДЕЯКІ ЧИННИКИ ПОШИРЕННЯ КІБЕРЗЛОЧИННОСТІ

Тенденція останніх років щодо стрімкого переходу фінансово-економічних відношень із матеріальної сфери у віртуальну залишається незмінною і на теперішній час. Обсяги і форми електронних грошових операцій збільшуються, а разом з ними зростає і рівень кіберзлочинності.

Одним із чинників розповсюдження і поширення правопорушень у кіберсфері є ступінь доступності Інтернету. Цей фактор з одного боку сприймається в усьому світі як показник рівня розвитку демократії в державі, а з іншого боку, сучасні особливості побудови і функціонування всесвітньої мережі, зокрема, відкритість і анонімність, сприяють поширенню кіберзлочинності і ускладненню виявлення і документування кіберзлочинів. Доступність визначається техніко-технологічними, фінансово-економічними і нормативно-правовими чинниками [1].

Крім перелічених особливостей організації кіберпростору ускладнюють результативність розкриття кіберзлочинів також і адміністративно-організаційні особливості розслідування кіберзлочинів, на чому акцентував увагу фахівців представник правоохоронних органів США на міжнародній конференції по боротьбі з кіберзлочинністю, яка проходила в червні 2013 року в Донецькому юридичному інституті МВС України, коли доповідав про досвід роботи групи фахівців з розслідування кіберзлочинів в одному з штатів США. Специфіка кіберзлочину полягає в тому, що процесуальна реакція на нього повинна бути практично миттєвою. Інакше правопорушники дуже швидко знищують віртуальні сліди кіберзлочину і в подальшому зібрати достатню доказову базу стає дуже складно. Але діюча нормативна база визначає певний і доволі бюрократичний і тривалий порядок узгодження оперативно-розшукових і слідчих дій в результаті приводить до того, що коли співробітник правоохоронних органів отримує формальне право виконувати певні дії, віртуальні сліди кіберзлочину вже давно знищені правопорушниками. Це свідчить про те, що процесуальний порядок проведення оперативно-розшукових і слідчих дій при розслідуванні кіберзлочинів певного типу (зокрема крадіжки з банківських рахунків за допомогою засобів комп'ютерних мереж) повинен враховувати такі особливості. Крім того іншими повинні бути і форми взаємодії і координації співробітництва правоохоронців різних відомств саме в процесі розслідування кіберзлочинів з тим, щоб максимально зменшити в процесуальному плані час від скоєння кіберзлочину до початку дій з його розкриття.

Одними з основних ідентифікуючих ознак кіберзлочинів є IP-адреса і MAC-адреса. Однак техніко-технологічні особливості побудови сучасного кіберпростору такі, що ці ознаки є дуже нестабільними, що також негативно впливає на ефективність розкриття кіберзлочинів. Як IP-адреса, так і MAC-адреса може бути легко змінена користувачем або правопорушником як на самому комп'ютері, так і у будь-якій точці маршруту пакету повідомлення, що сприяє приховуванню джерела кібератаки. Причому стабільність цих вкрай важливих параметрів не підкріплена ані технічно ані нормативно.

Таким чином, станом на теперішній час ефективність розкриття кіберзлочинів стримується низкою чинників техніко-технологічного, фінансово-економічного, нормативно-правового та адміністративно-організаційного характеру. Розв'язання цієї проблеми в межах однієї установи і навіть держави не є можливим. Для цього потрібні скоординовані зусилля комплексної

групи фахівців, підтримані на державному і бажано міжнародному рівнях.

Список використаних джерел:

1. Струков В. М. До визначення напрямів протидії кіберзлочинності / В. М. Струков // Системи обробки інформації. – 2013. – Вип. 3 (110). – С. 203–207.

Одержано 29.10.2014

УДК 343.346.8

Володимир Володимирович ТОРЯНИК,
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних технологій та захисту інформації
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ;

Антон Юрійович ЧМИРЬ,
студент факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

АКТУАЛЬНІСТЬ ПРОБЛЕМИ АТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ

В сучасних умовах поширення інформаційних технологій нагальною є проблема нападів на комп'ютерні системи через використання спеціальних мережевих технологій для їх блокування – так звана DoS-атака. Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними до користувачів, для яких комп'ютерна система була призначена. Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (DDoS).

Типово DoS-атаки здійснюють за рахунок переповнення смуги пропускання. Зловмисники користуються флудом (англ. Flood – «повінь», «переповнення») – атакою через велику кількістю зазвичай безглуздих або сформованих в неправильному форматі запитів до комп'ютерної системи або мережевого обладнання, що має за мету призвести збій в роботі системи через вичерпання системних ресурсів – процесора, пам'яті або каналів зв'язку [1].

Технологічно це може реалізовуватись через програми з відкритим вихідним кодом для здійснення мережевих атак, наприклад, LOIC (акронім від Low Orbit Ion Cannon, написана на мові програмування C#), розробка компанії Praetox Technologies, але пізніше була опублікована як суспільне надбання. Програма

виконує розподілену атаку «відмова в обслуговуванні» (Denial of Service – DoS) шляхом постійних передач на потрібний сайт або сервер TCP-, UDP-пакетів або HTTP-запитів з метою появи збоїв в функціонуванні певного хоста. Існує також редакція програми LOIC Hive Mind, здатна автоматично отримувати завдання на атаку через IRC, RSS або Twitter, що дозволяє централізовано запускати DDoS-атаки (Distributed Denial of Service – DDoS) з використанням комп'ютерів добровольців [2]. Є два варіанти організації DDoS атак:

– ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера;

– флешмоб – домовленість великого числа користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера.

Широковідомі випадки успішних атак:

1. 2012 р. – в Україні після закриття міліцією популярного файлообмінника EX.ua було виведено з ладу сайт МВС. Деякий час був недієздатним сайт Президента України. За два дні невідомим хакерам вдалося вивести з ладу сайт адміністрації президента, МВС, СБУ та офіційний сайт Партії регіонів та Компартії України. З перебоями працювали сайти Кабінету Міністрів і Податкової адміністрації.

2. Листопад - грудень 2013 р. – ЗМІ України заявляють про DDoS-атаки на їхні веб-сайти. Атак зазнали сайти: pravda.com.ua, zik.ua, zaxid.net, hromadske.tv, ukr.net, censor.net, zn.ua, lb.ua, 5.ua, tyzhden.ua [1].

3. Листопад 2014 р. – під час виборів до Верховної Ради України ЗМІ заявляють про DDoS-атаки на сервери ЦВК [4].

При підготовці та проведенні DoS атаки утворюються такі сліди технічного характеру:

1) наявність інструментарію атаки – програмних засобів (агентів), встановлених на комп'ютері зловмисника або, частіше, на чужих використовуваних для цієї мети комп'ютерах, а також засобів для управління агентами;

2) логи (переважно статистика трафіку) операторів зв'язку, через мережі яких проходила атака;

3) логи технічних засобів захисту – детекторів атак і аномалій трафіку, систем виявлення вторгнень, міжмережевих екранів, спеціалізованих антіфлудових фільтрів;

4) логи, зразки трафіку та інші дані, спеціально отримані технічними фахівцями операторів зв'язку в ході розслідування інциденту, вироблення контрзаходів, відбиття атаки. (Слід знати, що DoS атака вимагає негайної реакції, якщо власник

бажає врятувати свій ресурс або хоча б сусідні ресурси від атаки. В ході такої боротьби обидві сторони можуть застосовувати різні маневри і контрманевром, із за чого картина атаки ускладнюється.) [3, с. 60].

Очевидно, розглянуті атаки в мережі можуть бути істотним інструментом зловмисної протидії документуванню та розслідуванню кіберзлочинів. Цю обставину необхідно враховувати при розробці стратегії розслідування кіберзлочинів, принаймні, у двох аспектах. По-перше, у технічному аспекті, залучати експертів для фіксації атак та перешкоджанню використовування зловмисниками атак. По-друге, у законодавчому аспекті, проводити системну законодавчу роботу щодо створення адекватного правого механізму реагування.

Список використаних джерел:

1. DoS-атака [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/DoS-атака.

2. LOIC [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/LOIC

3. Федотов Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М. : Юрид. Мир, 2007. – 360 с.

4. ЦВК «бомбардують» DDoS-атаками / Інтерфакс-Україна // Українська правда [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2014/10/25/7041915. – 25 жовт. 2014 р.

Одержано 28.10.2014

УДК 32.019.5:316.485

Андрій Леонідович ЄРОХІН,
доктор технічних наук, професор,
помічник ректора, професор кафедри програмної інженерії
Харківського національного університету радіоелектроніки;

Олексій Петрович ТУРУТА,
кандидат технічних наук, доцент кафедри програмної інженерії
Харківського національного університету радіоелектроніки

ПИТАННЯ АДЕКВАТНОСТІ ПРОТИСТОЯННЯ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ

Існування сучасної держави пов'язано з інформаційною боротьбою (будь-якого типу), яка тісно переплетена з інформаційними операціями – маніпуляціями, інсинуаціями, дезінформацією, обманом і т. ін. Досить часто інформаційна боротьба здійснюється в наступних формах:

– інформаційна розвідка – пошук, збір, обробка та аналіз інформації про інформаційні ризики і загрози;

– планування інформаційних заходів тактичного (локального, внутрішньодержавного), оперативного (щодо країн-сусідів держави) і стратегічного (спільно з державами, які впливають на розвиток геополітики) рівнів;

– проведення заходів інформаційного характеру (інформаційних операцій, дій, акцій) в цілях реалізації завдань внутрішньої і зовнішньої політики держави;

– оцінки ефективності інформаційних заходів – визначення рівня досягнення успіху [1].

Інформаційні заходи стали невід'ємною частиною політики держави. У цьому сенсі Росія не тільки випередила розвинені європейські країни, а й почала конкурувати з США і Китаєм щодо питань інформаційного впливу. Про те, що російська пропаганда глибоко проникла в західне середовище і створила у себе контрпропагандистський щит, стали говорити вже наприкінці 2013 року. Інформаційна експансія російського закордонного мовлення («RT», «Голос Росії», ВГТРК) і система внутрішньої пропаганди («Газпром Медіа Холдинг», «Національна Медіа Група» і та ж ВГТРК) створили потужну інформаційну платформу російської системи інформаційної безпеки, що дозволяє проводити інформаційні атаки на інші держави. Сучасна РФ займається не просто дрібною дезінформацією, підробками інформаційного матеріалу, брехнею, витоками і кібернетичними диверсіями, які є звичайними засобами інформаційної війни, вона відображає «дійсність», створюючи масові галюцинації, які згодом перетворюються в політичні дії.

Аналіз досвіду США щодо роботи підрозділів психологічних операцій свідчить, що за 70 років участі у військових конфліктах американці виробили тактику психологічної війни для будь-якого регіону світу. У 2012 році після успіху «Арабської весни» збройні сили США замінили лякаючу назву PSYOPS новим терміном - «військові операції інформаційної підтримки» (Military Information Support and / to Operations - MISO). Як відомо, в даний час США мають намір переглянути загальну політику державної пропаганди. Очікується, що інновації торкнуться і військової сфери, однак на сьогодні в армії США тактика дій сил психологічних операцій залишилася майже без змін. Винятки становлять нові зразки техніки («LRAD», «Hyperspike PTZ», «LASER DAZZLER ™» та інші), які впливають на загальну схему психологічних операцій.

В Китаї класика психологічної війни поступово йде в площину інтернет-війн. В результаті проведення порівняльної характеристики питомої ваги Інтернет-сегмента інформаційно-

психологічних операцій виявилося, що в Росії він наближається до 15 %, в той час, як в Китаї сягає 50 %. Разом з тим, китайці не збираються залишати традиційні методи психологічної війни - друковану, усну, телевізійну і радіопропаганду. Отже, вони достатньо консервативні у дотриманні головного політичного вектора держави – так званої політики «м'якої сили» щодо інших країн [2].

Окремо необхідно звернути увагу на дослідження Девіда Янагізава-Дротта, який дослідив проблему вбивств тутсі в Руанді. Протягом 4 місяців було вбито півмільйона (за деякими даними мільйон) громадян. Заклики до протиправних дій розповсюджувались за допомогою радіотрансляцій. Місцевість в Руанді гірська, тому рівень сигналу в ряді селищ відрізняється. В результаті дослідження залежності кількості осіб, осуджених за геноцид, та рівня сигналу в селищі, було встановлено, що кількість засуджених за геноцид в селищах, де був добрий рівень сигналу, на 60–65 % більша за селища, де сигнал не досягав зовсім. Цей приклад доводить, що інформаційно-психологічні операції призводять до конкретних наслідків [3].

В українській армії за радянських часів існували військові структури які здійснювали інформаційно-психологічні операції, але в сучасних умовах вони не здатні протистояти ані масштабам, ані методам інформаційно-психологічних операцій противника через те, що внаслідок 23-річної політики в Україні домінувала теза, що «на нас ніхто не нападе, ворогів у нас немає і свою армію ми будемо тільки скорочувати». Існуюча інформаційно-бойова техніка за 23 роки морально застаріла. Бойові і технічні можливості центрів інформаційно-психологічних операцій навряд чи можна протиставити сучасним вимогам війни, наприклад, на Донбасі.

Гібридна війна на Донбасі жодного дня не обходиться без інформаційно-психологічних атак з боку терористів та російського керівництва, яке їх підтримує, а центри інформаційно-психологічних операцій – саме той військовий елемент, який повинен цьому протидіяти.

В березні 2014 року з'явилися рекомендації створити центр по боротьбі з інформаційною агресією проти України, антиукраїнською пропагандою і дезінформацією, однак, цього не було зроблено. Проте, такою діяльністю почали займатися приватні організації, представники українського громадянського суспільства, такі, наприклад, як Інформаційний опір, Inforesist, StopFake, що займаються аналізом кремлівської пропаганди і викриттям російської антиукраїнської інформації та дезінформації. Ці організації змогли ідентифікувати сотні

випадків інформаційних диверсій проти України і продемонструвати, як саме вони були організовані. Проте, в умовах глобальної інформаційної війни, ресурсів тільки приватної ініціативи стає явно недостатньо.

Очевидно, що різні держави проводять політику протидії інформаційним війнам. Сучасна проблема протидії інформаційним війнам виходить далеко за межі проблем функціонування комп'ютерних мереж і систем, проблем захисту інформації та протидії комп'ютерних злочинів. Важливою проблемою є протистояння різним видам інформаційно-психологічних нападів.

Для ефективного виконання інформаційно-психологічних операцій необхідно наступне:

– організувати підготовку фахівців з інформаційно-психологічних операцій для Служби безпеки України, Міністерства внутрішніх справ, Збройних сил України;

– забезпечити можливість вирішення наступних задач: створення та тиражування друкованих матеріалів; створення та трансляція телевізійних і радіопередач на визначений регіон; передачу необхідних повідомлень через телебачення; використання мережі Інтернет в інтересах операції;

– забезпечити можливість залучення державних та недержавних установ з метою створення і трансляції рекламних (агітаційних) роликів по телевізійним і радіоканалам в інтересах інформаційно-психологічних операцій; залучення операторів мобільного зв'язку для забезпечення передачі текстових, фотографічних, звукових та аудіовізуальних повідомлень пропагандистського характеру за допомогою мобільних телефонів; залучення Інтернет-провайдерів для забезпечення надання послуг доступу до мережі Інтернет для роботи фахівців інформаційно-психологічних операцій в мережі.

Список використаних джерел:

1. Pomerantsev P. Russia and the Menace of Unreality [Електронний ресурс] / P. Pomerantsev. – Режим доступу: http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

2. Гусаров В. Силы информационных операций России: каким должен быть ответ Украины? [Електронний ресурс] / В. Гусаров. – Режим доступу: http://sprotyv.info/ru/news/5931-sily-informacionnyh-operaciy-rossii-kakim-dolzhen-byt-otvet-ukrainy.

3. Yanagizawa-Drott, D. Propaganda and Conflict: Evidence from the Rwandan Genocide / D. Yanagizawa-Drott // The Quarterly Journal of Economics. – 2014. – Doi: 10.1093/qje/qju020.

Одержано 01.11.2014

УДК 343.55

Володимир Іванович СТРЕЛЯНИЙ,
кандидат юридичних наук,
провідний науковий співробітник науково-дослідної лабораторії
з проблем протидії злочинності
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

ПИТАННЯ ПРОТИДІЇ ВТРУЧАННЯМ У РОБОТУ СИСТЕМ ДИСТАНЦІЙНОГО БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ

Останнім часом активність кіберзлочинців значно зросла щодо втручання в онлайн-системи дистанційного банківського обслуговування (ДБО), зокрема системи «клієнт-банк». Причому спостерігається діяльність організованих груп злочинців. Ще нещодавно це були поодинокі випадки, то вже в 2012 р. кількість і обсяг злодійських трансакцій зросли в рази. Найбільша склала 32 млн грн. і була розбита на частини по 30 і 2 млн грн. Більшу трансакцію вдалося встановити тільки завдяки інструментам фінансового моніторингу НАБУ. Додатково банкіри занепокоєні тим, що у 2013 р. зафіксовані випадки масового застосування проти банків (одночасно проти десяти і більше банків) розподілених кібератак на зовнішні сервіси типу «відмова в обслуговуванні» (DDoS-атаки).

Але найчастіше банкіри перекладають відповідальність несанкціонований доступ до систем ДБО в більшості випадків на клієнтів. Методика несанкціонованого втручання та списання коштів з рахунків юридичних осіб проходить за усталеною схемою. Шахраї виводять досить великі суми з рахунків юридичних осіб, після чого переводять їх по ланцюжку з фіктивних юридичних або фізичних осіб і знімають готівкою. По рахунках фізосіб шахрайство в системах ДБО незначне. Більшість крадіжок відбуваються після 17.00 в п'ятницю, а власники рахунків дізнаються про це лише в понеділок, коли шахрайська операція давно завершена і гроші перекочували через десяток рахунків.

Експертами пропонуються зміни до законодавства України, які можуть сприяти зменшенню кількості випадків шахрайства зі спеціальними платіжними засобами, платіжними системами. Серед нагальних є встановлення юридичної відповідальності сторін у рамках розслідування інцидентів шахрайства із спеціальними платіжними засобами, платіжними системами. Посилення кримінальної відповідальності за кіберзлочини (ввести

чітке визначення кіберзлочину). Сспеціалісти пропонують розробити та затвердити єдині, обов'язкові для всіх учасників ринку стандарти, процедури і технології розрахунків за допомогою спеціальних платіжних засобів, систем (ДБО).

Крім цього, нагальним питанням є створення правової основи для арешту та конфіскації «електронних» доходів, а також запобігання відмивання грошей в мережі Інтернет, що потребує укладати угоди про співпрацю між правоохоронними органами та Інтернет-провайдерами.

Перед новим складом парламенту стоїть обов'язок законодавчого урегулювання питання щодо можливого арешту грошових коштів, отриманих шляхом шахрайства, які знаходяться на рахунку отримувача.

На сьогоднішній день низкою банків запроваджено локальні заходи щодо перевірки та виявлення фінансових операцій, які можуть бути пов'язані з кіберзлочинністю. Банками запроваджуються додаткові механізми захисту клієнтів:

– по клієнтській програмі клієнт-банк-OnLine – перед відправкою документів на проведення, клієнтом вводиться комбінація «картинок» або таємного коду, отриманого на свій мобільний телефон у вигляді sms-повідомлення;

– вводяться технологічні процедури запобіганню шахрайства при проведенні операцій з платіжними картками, а саме: 100-відсоткова авторизація всіх операцій в торгово-сервісній мережі;

– примусове введення на терміналі останніх 4 ембосованих цифр номера картки при формуванні запиту і зіставлення їх з даними на магнітній смузі. У разі якщо дані не співпали, операція не дозволяється;

– вводяться лімітування на максимальну суму покупки, на максимальну кількість операцій, максимальну суму операцій за однією карткою і т. д.;

– запроваджується підтвердження правомірності надходження платіжних документів клієнта, отриманих за допомогою системи «клієнт-банк», на значні суми, а також тих, що є нетиповими для клієнта, в телефонному режимі у відповідальних осіб;

– банк, за погодженням з клієнтом, здійснює контроль відповідності електронного цифрового ключа з IP-адресою робочої станції клієнта, на якій встановлено інтернет-банкінг та здійснюється відправка платежів (при наявності статичної IP-адреси);

– виявлення несанкціонованих клієнтами перерахунків коштів через систему «клієнт-банк» створена група розсилки

antifraud в яку входять співробітники підрозділів, що приймають участь в попередженні та розслідуванні таких випадків. На дану групу направляються повідомлення щодо підозр та фактів шахрайства, як безпосередньо від співробітників Банку, так і в автоматичному режимі при фіксуванні підключень з IP-адрес, комп'ютерів, з яких раніше фіксувались випадки та спроби шахрайства, та автоматичні повідомлення про формування платіжних документів на контрагентів, на яких вже були зафіксовані несанкціоновані платежі та їх спроби.

Всі ці заходи є дієвим інструментом для забезпечення нормального функціонування систем ДБО, але крім цього необхідно посилювати координацію подібних заходів між банками, шляхом обміну інформацією про випадки несанкціонованого втручання, а також відпрацювання методики взаємодії з правоохоронними органами щодо інформування та співпраці в протидії злочинним посяганням.

Одержано 03.11.2014

УДК 343.98

Ljuban PETROVIC,
Independent Police Inspector, Service for Combating Organized Crime – Cyber Crime Department

URGENT ISSUES OF LAW ENFORCEMENT AGENCIES ACTIVITY IN COMBATING CYBERCRIME

In the world of the cybercrime investigations and digital forensics, the year 2014 will be noted as a year of extreme new challenges that have been placed in front of all of us who are working in this field. Although none of the topics that will be mentioned here represent a new appearance in the cyber underground, their escalation has entirely changed the nature of their original impact on cyber security worldwide.

In order for us to give an overview of some the most critical spots (looking from the angle of various governmental organizations in charged with suppressing cybercrime) in digital world, we should differentiate two main problem areas. One part of the problem would be specific types of cyber crime offenses that are important either because of their frequency of because of their security impact.

Second part of the issues that LEA are facing is connected to the problems in gathering enough evidences necessary to discover cyber and cyber related crimes, locate and identify the offenders

and finally collect these digital evidences in a way that they can be used as an evidence in a criminal proceedings.

When it comes to the first area, we need to identify those urgent issues that have the biggest impact on overall security in IT area. Although, regrettably, computer technologies are facing a world full of security challenges, some of these problems are causing a lot of damage to a large group of users and therefore they need to be addressed with much more attention than it was the case until now. In regards to that, we should single out two forms of cyber crime that have experienced a strong increase both in the number of committed offences and both in the amount of damage they have inflicted on organizations and individuals throughout the world.

These two forms are not entirely new, but they keep appearing in new forms on a daily basis, which makes them a true challenge for all of us involved in cyber crime suppression. As most of the analysis show, distribution of mobile malware and a rise of ransomware (cryptolocker viruses) are the two distinct points around which cyber criminals are currently pivoting.

Same as in all other types of so called «classical crime» the main impulse for cyber criminals was and still is – money. We have witnessed various techniques aimed towards illegal acquisition of financial data, both from financial institution and from personal accounts of individuals all over the planet. The answer of all major players in this area on these challenges was going in two directions. First, they tried to make life more difficult for the criminals by introducing digital tokens and two-factor authentication methods. In the same time they increased the portfolio of digital e-banking services that they offered to their clients. With the huge rise in usage of mobile devices, it was inevitable that all of these services will migrate to mobile platforms. This trend was also followed by creating a brand new set of mobile pay service completely circumventing both traditional payment methods and «normal» e-banking[1]. Of course, it didn't take to long for the criminals to realize that they need to find their way into mobile device or else they will be loosing all their profit.

The answer they were looking for was already there. For decades we have been witnessing that our data has been compromised buy specific types of malware (i. e. Trojan's) who have been

[1] The latest example of such process is the one with Apple Company introducing its Apple-pay system [1].

made with a sole purpose of either gathering financial data or exploiting users resources for the financial benefit of the attacker (botnets). Obvious success that they had with this approach was the main reason why for several years in a row, malware developers have been massively switching to mobile malware platforms. It seems that cyber criminals could sense the market trends better then IT companies, since the latest statistics show that PC sales have dropped 9.8 % in 2013, with expected downfall of additional 6 % in 2014 [2]. In the same time, mobile devices usage is expected to rise for an additional 7.6 % comparing it to an already booming result in 2013. Especially important fact for us is the market share of Android powered devices, which is expected to reach over 1.1 billion users. If we know that most of the malware packets sold on the black market are aimed exclusively towards this OS, it should be clear why this particular criminal form needs to be dealt with outmost attention.

Flexibility of the Android OS, which allows users to install cracked and non-verified applications with a press of a button, has made this platform an ideal target for malware developers. But even if one could say that users who use legitimate applications downloaded only from official Google Play Store are protected from such attacks, in this case that's simply not true. In 2013 more than 42,000 apps in Google's store contained Trojan or similar malware solutions aimed towards data stealing – and that's only for the apps that Google managed to identify. In other words, the number of malicious applications distributed trough Google's official store has increased in incredible 388 % from 2011 to 2013 [3]. Another very important fact is the actual number of victims per country. Kaspersky Labs statistics show that the top five countries with the highest number of infected users are Russia (40 %), India (8%), Vietnam (4 %), Ukraine (4 %) and the UK (3 %) [4]. This means that Ukraine shares an infamous third place with Vietnam, containing 4 % of world's total infected victims. Considering the fact that Ukraine is also one of the worlds leading sources of cyber crime attacks, especially when it comes to malware dissemination (almost 5 % of total attacks in the world are coming from Ukraine) it should be obvious that this topics needs to be one of the top priorities for the local LEA [5].

It should also be noted that mobile malware hasn't expanded just in simple numbers. It has also evolved immensely in its technical capabilities and (based on their primary functions) we can now differentiate several different categories in mobile malware [6]:

Data Stealer – Steals information stored in the device and sends it to the attacker.

Premium Service Abuser – Subscribes the infected phone to premium services without user consent.

Click Fraudster – Mobile devices are abused via clicking online ads without users knowledge (pay-per-click).

Malicious Downloader – Downloads other malicious files and apps[2].

Spying Tools – Tracks user's location trough GPS data and sends it to the attacker

Rooter – Gains complete control of the phone, including their functions.

It is clear by looking at this list that two-factor authentication methods will have no use in protecting users that have been infected with one of these malicious solutions. Once they gain control over targeted device, they will simply intercept authentication SMS, verify their access in users on-line account, change all login parameters and the game will be over for the user. We should also never forget that two-factor authentication methods via SMS is a mandatory step not just only for e-banking services, but also for all major Internet content providers such as Gmail, Facebook or Microsoft. In a word, we are witnessing that the desire of large Internet companies to use mobile devices as a tool to protect users from unauthorized access has actually turned against them. They have given a powerful tool to all criminals, which can gain access in every aspect of users' on-line activity by simply hijacking their smartphones.

Unless our answer is fast and energetic we will be soon facing another offensive of cyber criminals that we will most likely once again loose. A possible good step in a right direction should actually come from Google it self by simply introducing much higher security standards for the applications released in an official Play Store. This can be done by following Apple's rigorous testing practice which has resulted in a completely malware free Apple Store.

This problem is also present in a second burning topic that we mentioned earlier – ransomware[3] malware. One of the worlds leading AV companies – McAfee, has analyzed almost nearly 250,000 unique samples of this type of malware just in first

[2] Mobile device is vulnerable to more infection, and often this is a first step towards installing a more sophisticated malware that will take complete control on infected device.

[3] Ransomware is a type of malware that restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed [7].

quarter of 2013, which has indicated more then a 100% rise in the use of this highly destructive software [8]. Again, same as we have already noted when speaking about the mobile malware, in 2014 a large number of these ransomware solutions has found its way to mobile devices. One of them, called Koler (Worm.Koler) is capable not only for encrypting Android smartphones but once you are infected, it will continue infecting other users by accessing your phonebook and sending SMS messages to all numbers in your contact list [9].

Although it is very hard to guess what is the total number of users who have been affected with ransomware viruses (regardless of the platform that they are using) since a lot of these offenses is never report to the police for various reasons, it is clear that the numbers are raising and it is also very clear that the damage they are causing is growing exponentially. However, these two facts are not the only reason why we should worry. Even bigger problem is the fact that LEA hasn't found an adequate answer to this challenge. Tracking these offenders is almost impossible since all payments are made using Bitcoins or similar digital currencies that provide complete anonymity for the parties included in the transaction. Second, not like in the case of botnets, police want have an opportunity to locate a command and control center somewhere and ultimately use it to track the criminals who set it up. A lot of these ransomware's won't even open an Internet connection. All they need is a ransom message on the screen and an email for receiving a proof of payment so that you are able to receive decryption instruction.

Finally, LEA hasn't even made a lot of success in helping users who refuse to pay to retrieve their data, and thus also retrieve additional evidences that might lead to the attacker. Only a few of the national LEA organizations have made some attempts in these directions, and this activity is usually reserved for those organizations that have the budget that can afford research in such problems. Although this is something that we can understand it is often a wrong practice. Some of these malicious programs are truly complicated but most of them use simple encryption methods that can easily be reversed without any sophisticated tools and with limited human resources. In a lot of cases, we will see that other researches have analyzed such or similar malware only and have offered both the tools for decrypting such infected machines and the instructions on how to do it. It is for these reasons why both the academia and private sector should join and try to do their best in keeping the level of education of LEA members on a

high level. Unless we increase the level of operational capabilities throughout the LEA community, then we can't expect that them to understand these treats stay informed about the possible solutions and finally apply them and investigate such crimes.

In the previous text we have covered some of the problems related to the specific types of cyber crime that without a doubt deserve to be addresses urgently. However, besides the problems that LEA have when investigating specific crime types, another as equally important problem is locating the criminals and securing enough evidence that can prove a certain offence. Although we are now talking about the digital world, this problem should be looked at the much wider scale since modern criminal investigation expects us to collect digital evidence for almost any type of crime. It has become almost impossible to investigate any criminal offence without encountering some form of digital evidence in that process. There for, LEA capabilities in collecting such data can often be crucial in the investigation. Considering the fact that Internet is becoming a predominant form of communication in the criminal underground, especially for the organized crime groups, we need to seriously evaluate the problems that LEA throughout the world are facing in this field.

First part of the problem, which is directly disabling police officers to conduct efficient evidence collection and suspect identification, is encryption and anonymity. More and more our colleagues are facing with the devices, which are properly seized but forensically completely useless. The reason for this is the fact the almost all OS's that are shipped with the new machines now support whole disk encryption. Further on, this type of data protection has also become a standard for the mobile devices. While some vendors (such as Google) use this as an option to be turned on by the user it self, some other major players (Apple) have recently announced that their OS's will automatically encrypt the entire device. Also, they have informed the representatives of LEA in Unites States that they will not be able to assist them in retrieving data from such devices even if they are presented with a court order to do so. According the available information's on the architecture of the new iOS devices, the reason for this lies in the actual topology of the entire encryption process, which has now been radically improved for security reasons. This procedure now includes automatic encryption of almost all files on the device starting from the moment when a user sets a passcode on its device. Any newly created file on the device is being encrypted from the very beginning. Apple now uses one of the strongest

encryption algorithms (AES 256) connected with specific keys generated for each device separately, and all new devices (starting from iPhone 5 and above) are now by default shipped with a new hardware encryption co-processor called the «Secure Enclave».

These challenges are something that neither LEA nor private sector has an answer to. In the recent INTERPOL-EUROPOL conference in Singapore, the representatives of one of the leading forensic companies, Cellebrite, have (reluctantly) stated that their engineers have no answer on this challenge. Realistically, unless something drastically changes, they probably never will. Considering these technical details, and having in mind the worldwide popularity of such devices, it is clear why this matter is of highest importance for all parties involved in criminal investigations. Also, we should be aware that this trend is likely only to be increased. Competition between some of the major players in the market (Apple, Google-Samsung) will just get us to the point where this type of data protection will soon be a default standard for all Android powered devices.

Second part of this problem is increased level of anonymity that has been offered to the users on the Internet. Although these trends are not new, the level of communication that has been passed from traditional means of communication to on-line service (e-mails, IM's and encrypted VoIP) has reached a point of no return. In the same time, most LEA have zero capacity in detecting and intercepting these forms of communications. Anonymity in communications is not the end of these problems. Additional problem posses the introduction of digital currencies and various payments system that enable anonymous transactions. Although we are all aware of the problems that have arisen with tracking Bitcoin on-line transactions, introduction of Bitcoin ATM's has made this problem only worse. Of course, this problem is not limited only to these open-source services. As we previously mentioned Apple has join the line of the companies offering e-payments systems. What is particularly important when we talk about this system is the fact that it also guaranties complete anonymity. In fact, as one if its prime features Apple explicitly states: «Apple doesn't save your transaction information. With Apple Pay, your payments are private. Apple Pay doesn't store the details of your transactions so they can't be tied back to you» [1].

Having all these previously mentioned issues in mind, it is clear that there are several fields which deserve urgent response, not just from the LEA but from all players involved in tackling crime in general. The issues mentioned in this paper will not be

limited just to cyber crime, and will not affect just those agencies involved in solving these types of offences. Consequences of these trends will without a doubt be felt in every aspect of every day policing. Regrettably, the level of awareness in the general LEA community on the potential dangers of these specific criminal trends, and the suggested investigative methodology for them, still stays very low.

List of references:

1. Apple-pay [Electronic sourse]. – Access mode: https://www.apple.com/apple-pay/.

2. Gralla P. Is the PC apocalypse upon us? Latest sales figures say it might be / Preston Gralla // Computerworld [Electronic sourse]. – Access mode: http://www.computerworld.com/article/2475990/windows-pcs/is-the-pc-apocalypse-upon-us--latest-sales-figures-say-it-might-be-.html. – Mar 6, 2014.

3. RiskIQ Reports Malicious Mobile Apps in Google Play Have Spiked Nearly 400 Percent : Press Release [Electronic sourse]. – Access mode: http://www.riskiq.com/company/press-releases/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400.

4. Mobile malware evolution: 3 infection attempts per user in 2013 / Kaspersky Lab [Electronic sourse]. – Access mode: http://www.kaspersky.com/about/news/virus/2014/Mobile-malware-evolution-3-infection-attempts-per-user-in-2013. – 24 Feb 2014.

5. Chebyshev V. IT threat evolution Q1 2014 / Victor Chebyshev, David Emm, Maria Garnaeva, Roman Unuchek // Securelist [Electronic sourse]. – Access mode: http://securelist.com/analysis/quarterly-malware-reports/59417/it-threat-evolution-q1-2014/. – April 17, 2014.

6. Celestino O. Mobile Apps: New Frontier for Cybercrime / Oscar Celestino Angelo Abendan II [Electronic sourse]. – Access mode: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/119/mobile-apps-new-frontier-for-cybercrime.

7. Ransomware [Electronic sourse]. – Access mode: http://en.wikipedia.org/wiki/Ransomware.

8. Samson T. Update: McAfee: Cyber criminals using Android malware and ransomware the most / Ted Samson // InfoWorld [Electronic sourse]. – Access mode: http://www.infoworld.com/article/2614854/security/update--mcafee--cyber-criminals-using-android-malware-and-ransomware-the-most.html.

9. Look out, this ransomware spreads via SMS / GMA News // GMA News Online [Electronic sourse]. – Access mode: http://www.gmanetwork.com/news/story/385933/scitech/technology/look-out-this-ransomware-spreads-via-sms. – October 30, 2014

Одержано 03.11.2014

РОЗДІЛ 2
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343.1

Олександр Миколайович ГОЛОВКО,
доктор юридичних наук, професор,
перший проректор з навчально-методичної та наукової роботи
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ ПИТАННЯ БЛОКУВАННЯ ТА ВИДАЛЕННЯ ПРОТИПРАВНОГО ІНТЕРНЕТ-КОНТЕНТУ

Протягом останніх років спостерігається активний розвиток України як інформаційного суспільства та законодавства в цій сфері. Багато питань у сфері доступу до інформації та обмежень, які стосуються змісту опублікованої інформації залишаються проблемними та досі не вирішеними у правовому полі України. Зокрема, це стосується розміщення протиправного контенту в мережі Інтернет (зокрема, пропаганда расової, національної чи релігійної нетерпимості, прояви сепаратизму, наклепи та образи, дитяча порнографія тощо) та протидії цьому явищу на національному рівні.

Нещодавно Харківським національним університетом внутрішніх справ на виконання доручення Міністерства внутрішніх справ України було підготовлено пропозиції щодо законодавчого врегулювання питання блокування та видалення протиправного інтернет-контенту.

Розглядаючи питання протидії цьому негативному явищу та попередження можливих наслідків розміщення такої інформації, слід вказати, що відповідно до ст. 15 Конституції України цензура заборонена, а ст. 34 Конституції передбачає право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. При цьому, кожному гарантується право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Вказані права можуть бути обмежені законодавством в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню

інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

З метою надання можливості реалізації вказаних положень доцільно у чинному законодавстві передбачити порядок та підстави блокування та видалення протиправного контенту. Здійснення цього можливо у розрізі заходів забезпечення кримінального провадження, передбачених чинним Кримінальним процесуальним кодексом України.

Враховуючи спрямованість вказаного заходу протидії доцільно розширити положення, що стосуються «тимчасового доступу до речей і документів» додатковим заходом забезпечення кримінального провадження – «блокування доступу до інформації», поширивши на нього порядок застосування тимчасового доступу до речей і документів.

Передбачається, що у разі виявлення протиправного контенту, суд (слідчий суддя) приймає рішення щодо тимчасового блокування інформації (з метою попередження зміни місця її перебування та поширення), у разі доведення правоохоронними органами наявності складу злочину та встановлення судом протиправного характеру заблокованої інформації, рішення про її видалення прийматиметься судом одночасно із винесенням вироку.

Одержано 17.10.2014

УДК 343.98

Сергій Володимирович БОНДАР,
здобувач кафедри криміналістики та судової медицини Національної академії внутрішніх справ (м. Київ)

СПОСОБИ ВЧИНЕННЯ ЗЛОЧИНІВ У СФЕРІ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Сучасне суспільство це суспільство інформаційних технологій, що базується на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя.

Банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи,

що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців.

Несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, втручання в роботу інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS-атаки на інтернет-ресурси, шахрайство в інформаційних мережах це не вичерпний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп'ютерних технологій. За оцінками експертів щорічні збитки від діяльності кіберзлочинців перевищують 100 млрд дол. США.

Підготовка та вчинення кіберзлочину здійснюється практично не відходячи від «робочого місця», тобто такі злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна вчинювати з будь-якої точки планети, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця.

Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу [1].

На сьогодні можливо виділити такі найпоширеніші інтернет-шахрайства, які вчинюють злочинці через мережу Інтернет:

1. Недотримання умов купівлі товарів через мережу Інтернет, зокрема при продажі товарів на інтернет-дошках оголошень та інтернет-аукціонах.

Найпоширенішими видами шахрайства є купівля товарів, розміщених на дошках оголошень, в інтернет-магазинах, на інтернет-аукціонах, так би мовити, по системі знижок чи у передсвяткові дні, за системою передоплати коштів за замовлений товар. Все це дає умови для шахраїв не дотриматись угоди покупки. Кількість таких випадків зростає з кожним днем. Попередженням даного виду шахрайства є проведення розрахунку тільки після того, як ви отримаєте товар і впевнитесь, що замовлений вами товар відповідає вашому бажанню й якості.

2. Дистанційне зняття коштів за допомогою послуги ПАТ «ПриватБанк» «Операція без картки».

Шахраї телефонують, представляються працівниками відділення того чи іншого банку та пропонують потерпілим підключити різного роду послуги, необхідні для безпеки їхнього власного відкритого карткового рахунку. Для цього пропонують повідомити алгоритм символів, які прийдуть в СМС-повідомленні для прийняття умов підключення послуги. Для здійснення своєї злочинної діяльності шахраям потрібно мати лише мобільний номер та картковий рахунок (16 символів).

3. Дистанційне зняття коштів за допомогою послуги «Приват24» ПАТ «ПриватБанк», шляхом входження в довіру й витребування інформації по картковому рахунку.

Зловмисники в мережі Інтернет підшуковують осіб, які розміщують оголошення про необхідність благодійної матеріальної допомоги та, під приводом надання матеріальної допомоги на розрахунковий рахунок, під час телефонної розмови входять у довіру і отримують необхідну інформацію щодо розрахункового рахунку, щоб у подальшому отримати над ним контроль.

4. Злочини в системі дистанційного банківського обслуговування втручання в систему «Клієнт-банк»

Сервіс «Інтернет Клієнт-Банк» дозволяє здійснювати дистанційне керування рахунком і платежами через Інтернет в режимі On-line. Особливістю даного виду злочину є те, що проходить зараження комп'ютера, до якого підключена послуга «Клієнт-Банк».

Зараження відбувається шляхом: розповсюдження шкідливої спам-розсилки; зараження вірусним програмним забезпеченням (через мережу Інтернет чи через магнітні носії), яке дозволяє здійснювати управління віддаленого доступу комп'ютером, на якому підключена послуга «Клієнт Банк»; фішинг вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних, посилаючи їм електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [2; 3, с. 70–71].

Отже, інтернет-простір став не тільки місцем вчинення злочину та одержання незаконного доходу, а й місцем легалізації такого доходу. При цьому різноманіття видів кіберзлочинів у сукупності з різноманіттям способів відмивання доходів, одержаних від вчинення даних видів злочинів, призводять до складності їх виявлення та розслідування. Виявлені схеми та механізми відмивання доходів, одержаних від кіберзлочинності, дозволяють стверджувати, що переміщення коштів можливе як традиційними способами переказу, так і з використанням сучасних систем термінових переказів, електронних платіжних систем та електронних грошей. При цьому, кошти використовуються в одних випадках для придбання передплачених карток, товарів або послуг в мережі Інтернет, а в інших переводяться в електронні гроші та перераховуються між електронними гаманцями, з подальшим переведенням у готівку.

Список використаних джерел:

1. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : наказ Держ. служби фінанс. моніторингу від 25 груд. 2013 р. № 157 [Електронний ресурс]. – Режим доступу: http://cct.com.ua/2014/25.12.2013_157.htm.

2. Найпоширеніші Інтернет-шахрайства та як не стати їх жертвою / Віньковец. РВ УМВС України в Хмельниц. обл. [Електронний ресурс]. – Режим доступу: http://vinmvs.at.ua/news/najposhirenishi_internet_shakhrajstva_ta_jak_ne_stati_jikh_zhertvoju/2014-05-20-96.

3. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.] ; за заг. ред В. В. Коваленка ; МОН України ; МВС України, НАВС ; РНБО України. – Київ : Скіф, 2012. – 722 с.

Одержано 29.10.2014

УДК 343.1:65.012.8+004

Андрій Вікторович ВІНАКОВ,
здобувач
Харківського національного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ВЗАЄМОДІЇ ПРОКУРАТУРИ ПІД ЧАС ЗДІЙСНЕННЯ ПРОКУРОРСЬКОГО НАГЛЯДУ ЗА ОПЕРАТИВНО-РОЗШУКОВОЮ ДІЯЛЬНІСТЮ ОРГАНІВ ВНУТРІШНІХ СПРАВ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Для того аби прокурорський нагляд логічно вписувався у правоохоронну систему держави та був орієнтований на швидкі та комплексні результати, потрібно налагодити ефективну систему взаємодії підрозділів прокуратури між собою та з іншими суб'єктами.

Головними суб'єктами внутрішньої взаємодії прокуратури під час здійснення прокурорського нагляду за здійсненням оперативно-розшукової діяльності з використанням інформаційно-телекомунікаційних систем є районні та регіональні підрозділи прокуратури, які проводять узгоджену діяльність із виявлення порушень у сфері здійснення окремих оперативно-технічних заходів, обмін інформацією, беруть участь у спільних заходах, організовують міжрегіональні заняття зі службової підготовки тощо.

Зовнішня взаємодія у досліджуваній сфері здійснюється з наступними суб'єктами:

– правоохоронні органи, у тому числі їх оперативні підрозділи та контролюючі суб'єкти (погодження інтрузивних оперативно-розшукових заходів із використанням інформаційно-

телекомунікаційних систем; участь у заслуховуваннях та нарадах по окремих напрямках боротьби з кіберзлочинністю та інших злочинах, з метою виявлення та попередження яких застосовуються інформаційно-телекомунікаційні системи; виявлення причин та умов та прогнозування порушень, які виникають під час застосування інформаційно-телекомунікаційних систем в оперативно-розшуковій діяльності; консультування оперативних працівників з досліджуваної сфери із моделюванням прикладних ситуацій; участь прокурора у проведенні занять зі службової підготовки із питань правомірного використання технологій в оперативно-розшуковій діяльності; взаємний обмін інформацією з питань виконання нормативних приписів щодо боротьби з високотехнологічною злочинністю; надання вказівок, а також підготовка і ухвалення спільних рішень з питань оперативно-розшукової діяльності з використанням інформаційно-телекомунікаційних систем; проведення спільних засідань колегій з питань застосування високих технологій в оперативно-службовій та слідчій діяльності);

– парламент (взаємодія через інститут тимчасових слідчих комісій; участь прокуратури у правотворчій діяльності, зокрема щодо законодавчого регулювання звітування правоохоронних органів про здійснені оперативно-технічні заходи в мережі Інтернет);

– засоби масової інформації (налагодження та підтримання контактів прокуратури та засобів масової інформації із особливою увагою до інтернет-видань; проведення медійних заходів; висвітлення інформації про результати прокурорського нагляду за здійсненням оперативно-розшукової діяльності з використанням інформаційно-телекомунікаційних систем у відомчих газетах та журналах, у тому числі тих, які мають обмежений доступ; сприяння засобам масової інформації в одержанні відкритих матеріалів, які стосуються резонансних подій, пов'язаних із неправомірним здійсненням оперативно-технічних заходів працівниками міліції тощо);

– населення та громадськість (повідомлення осіб про вжиті щодо них інтрузивні оперативно-розшукові заходи із застосуванням інформаційно-телекомунікаційних систем; потрібно по аналогії з МВС України створити при Генеральній прокуратурі дорадчо-консультативний орган (громадську раду) з числа представників найбільш авторитетних правозахисних організацій);

– суд (опротестування незаконної постанови суду про дозвіл або відмову на проведення окремих оперативно-технічних заходів);

– державні органи інших країн, міжнародні організації, закордонні приватні підприємства, установи, організації (обмін інформацією відкритого характеру та проведення заходів міжнародного співробітництва).

Одним з проблемних питань взаємодії під час здійснення прокурорського нагляду як у досліджуваній сфері, так і в цілому, є невирішений статус слідчого у питаннях здійснення оперативно-розшукової діяльності. Зважаючи на ці обставини пропонуємо виключити із наказу МВС України № 700 від 14.08.2012 норму щодо закріплення за оперативно-розшуковою справою слідчого як не властиву ані правозастосовній практиці, ані нормам чинного оперативно-розшукового законодавства.

Підсумовуючи відзначимо, що усі досліджені форми взаємодії на регіональному, державному та міжнародному рівнях потрібно здійснювати з урахуванням оперативних, тактичних та стратегічних цілей, що досягається не лише участю у конкретних спільних діях, але й своєчасним та якісним плануванням взаємодії прокуратури з іншими суб'єктами.

Одержано 14.10.2014

УДК 343.98.06(477)

Іван Андрійович ГРАБАЗІЙ,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ ЗЛОЧИНАМ, ПОВ'ЯЗАНИМ ІЗ СХИЛЯННЯМ ДО ВЖИВАННЯ НАРКОТИКІВ З ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ

Проблема організації дієвої протидії злочинам пов'язаним із схилянням до вживання наркотичних засобів, психотропних речовин або їх аналогів в мережі Інтернет є для діяльності правоохоронних органів України новою і тому представляє значний інтерес як для практичних працівників, так і для науковців.

Прогалина у даній сфері наукового знання негативно позначається на організації протидії і профілактики віртуального наркобізнесу, на законотворчій практиці, яка мала б регламентувати ці суспільні відносини. До недоліків наукового, законодавчого, правозастосовчого рівня додається ще і брак відповідних методик протидії даному виду злочинів, фахівців

і високотехнологічного програмно-пошукового забезпечення в мережі, висока латентність інтернет-наркобізнесу і т. ін.

Тому актуальність вивчення питання використання мережі Інтернет наркобізнесом для схиляння до вживання наркотиків є беззаперечною.

Слід відмітити, що протидія даному виду злочинів, саме із застосуванням мережі Інтернет значним чином ускладнюється тим, що:

1) При використанні невеликих ресурсів для їх здійснення може бути завдано величезної шкоди;

2) Злочин може бути вчинений в межах однієї юрисдикції (країни), а правопорушник може перебувати під іншою юрисдикцією (в іншій країні);

3) У багатьох національних законодавствах відсутнє чітке визначення (чи якесь визначення взагалі) таких правопорушень;

4) Небезпека, що загрожує правопорушникам, і ймовірність їх виявлення досить низькі.

Тому наркоторговці широко розповсюджують інформацію, що містить рекомендації щодо незаконного використання та виготовлення наркотиків, в мережі Інтернет з метою її популяризації, для розширення кола споживачів, реклами нових наркотичних засобів, у тому числі відкривають спеціальні інтернет-аптеки.

Підрозділам по боротьбі з незаконним обігом наркотиків слід враховувати високотехнологічні складові, які притаманні сучасній наркоіндустрії в інформаційному полі Інтернету. Типовими способами пов'язаним із схиляннням до вживання наркотичних засобів, психотропних речовин або їх аналогів в мережі Інтернет засобами електронно-цифрового технологічного походження є наступні:

1) пірингові мережі – наприклад: Overnet, Shareaza, Gnutella, принцип роботи яких передбачає встановлення програм по файлообміну, які знаходяться у вільному розповсюдженні в мережі Інтернету і дозволяють робити обмін файлами виключно в піринговій мережі;

2) електронна пошта – використовується переважно для розповсюдження каталогів наркопродукції, ознайомлення з умовами оплати, надсилання ключів для розшифровки інформації;

3) сервіси миттєвих текстів та передачі голосу і відеозображень які передбачають встановлення на комп'ютері спеціальних програм: Google Talk, Skype, ICQ, Messenger. Такі програми дозволяють користувачам передавати текст, аудіо-, відеозображення у форматі реального часу;

4) спеціальні веб-сайти, які є суто комерційними проектами та пропонують до продажу препарати, в тому числі сильнодіючі та нарковмістні.

Для підвищення ефективності протидії злочинам пов'язаним із схилянням до вживання наркотичних засобів, психотропних речовин або їх аналогів в мережі Інтернет необхідно дослідити слідову картину даного виду злочинів, яка носить матеріальний та нематеріальний характер.

До матеріальних слідів злочину, передбаченого ст. 315 КК України відносяться наступні предмети, відбитки та явища:

1. Наркотичні засоби.
2. Електронні носії інформації які містить рекомендації щодо незаконного використання та виготовлення наркотиків.
3. Засоби для виготовлення продукції які містить рекомендації щодо незаконного використання та виготовлення наркотиків: цифрова техніка (фотоапарати, відеокамери), комп'ютери, копіювальна та множильна техніка (сканери, ксерокси), друкуюча техніка (принтери), пишучі прилади, тощо.
4. Сліди людини на предметах, які збуджують в іншої особи бажання вжити наркотичні засоби. Такими є сліди рук, потожирові виділення, сліди запаху, волосся, відбитки взуття, тощо.
5. Облікові записи та нотатки у блокнотах, зошитах, супровідні надписи, цінники тощо.
6. Електронні протоколи передач файлів, які містяться на серверах.
7. Проксі-сервер, якій використовується як проміжний накопичувач для сторінок Інтернету.
8. Мобільні телефони, які можливо використати у якості доказів певних фактів злочину або окремих елементів події злочину, або епізодів, які причетні до злочинної діяльності і мають з нею кореляційній зв'язок.

Нематеріальними слідами є сліди пам'яті людини (свідків, самих злочинців, споживачів наркотичної продукції).

Таким чином усунення прогалин у даній сфері наукового знання шляхом дослідження типових способів схилянням до вживання наркотичних засобів, психотропних речовин або їх аналогів засобами електронно-цифрового технологічного походження а також їх слідової картини із подальшим впровадженням результатів дослідження в практичну діяльність ОВС України суттєво підвищить ефективність протидії даному виду злочинів.

Одержано 28.10.2014

УДК 343.98

Влада Олександрівна ГУСЄВА,
кандидат юридичних наук,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ;

Олена Вікторівна ОЛЕЙНІКОВА,
слухач магістратури
Харківського національного університету

ДЕЯКІ ОСОБЛИВОСТІ ВСТАНОВЛЕННЯ ХАРАКТЕРУ ТА РОЗМІРУ ШКОДИ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

В останні роки, в умовах соціально-економічних змін, відбувається значний розвиток інформаційних технологій в суспільстві, який набуває глобального характеру та стає підґрунтям для зростання злочинів у сфері використання комп'ютерних технологій. Головною особливістю зазначеної категорії злочинів, є інформація, яку суб'єкти інформаційної сфери створюють, зберігають, передають та розповсюджують, що може завдавати шкоду та створювати небезпечні наслідки. Тому, саме забезпечення матеріальних інтересів потерпілих від злочинів у сфері використання комп'ютерних технологій - одна з основних проблем як в науці, так і на практиці.

Згідно нового КПК України в процесі розслідування кримінального провадження слідчий або прокурор, який проводить досудове розслідування повинен встановити характер та розмір шкоди, що спричинив злочин. Тому виявлення та встановлення шкоди є однією з основних цілей досудового розслідування. Слідчий (прокурор) повинен доказати не тільки завдану шкоду, а й наявність безпосередньо самих потерпілих від злочину. Виявлення потерпілих включає в себе можливість особи реалізувати свої права в кримінальному провадженні, що як наслідок дає змогу в повній мірі встановити характер та розмір шкоди, спричинені злочином.

Слід зазначити, що злочини у сфері комп'ютерних технологій мають свої особливості, деякі питання доказування завданої шкоди були висвітлені в наукових працях В. Т. Нора, В. М. Савицького, В. А. Попелюшко, А. Г. Мазалова, М. І. Гошовського, Н. І. Газетдинова, С. А. Александрова, Н. Г. Власенко та інших учених. Проте окремі питання встановлення характеру та розміру шкоди заподіяної злочинами у сфері комп'ютерних технологій залишились поза увагою та потребують

подальшого розширення та деталізації, особливо зважаючи на прийняття нового КПК України.

Одним із способів спричинення шкоди є комп'ютерні віруси, які заповнюють увесь диск чи вільну пам'ять комп'ютера своїми копіями, чим блокують роботу комп'ютера, змінюють місцезнаходження файлів, форматують диски чи інші носії, виводять на екран негативне повідомлення, уповільнюють роботу комп'ютера, змінюють зміст програм і файлів, відкриту інформацію з обмеженим доступом (даний аспект закріплено в ст. 361-1 КК України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збуту», тому наприклад, для внесення даних до Єдиного державного реєстру досудового розслідування необхідно встановити саме факт створення з метою, безпосереднього розповсюдження чи збуту).

Встановлення потерпілого та шкоди, коли комп'ютерний вірус вразив комп'ютери закритої локальної сеті, можливо, але якщо вірус розповсюдився через вкладку електронної почти, чи через Web-сторінки, та за декілька годин вразив декілька тисяч комп'ютерів, то для правоохоронних органів виникнуть труднощі у розслідуванні даного кримінального провадження, а саме при встановленні потерпілих, характеру та розміру шкоди.

Так, Ю. В. Гаврилін стверджував, що при розслідуванні незаконного доступу до комп'ютерної інформації, перш за все треба встановити, чим були виражені шкідливі наслідки (викрадення грошових коштів або матеріальних цінностей, заволодіння комп'ютерними програмами, інформацією, шляхом вилучення її машинних носіїв, або копіювання, а також незаконна зміна, знищення, блокування або вивід з ладу комп'ютерного обладнання, введення в комп'ютерну систему завідомо неправдивої інформації чи комп'ютерного вірусу). Незаконне заволодіння комп'ютерними програмами як наслідок несанкціонованого доступу до системи, їх незаконне використання, виявляється скоріш за все, самими потерпілими, але бувають випадки, коли розмір завданої злочином шкоди встановити точно неможливо.

Розмір шкоди може бути встановлений шляхом проведення судових експертиз, таких як судово-бухгалтерська та судово-економічна експертизи в комплексі з інформаційно-технологічною та криміналістичною експертизою засобів комп'ютерної техніки і носіїв інформації.

Цікавою є статистика, згідно даних Української Антивірусної Лабораторії, яка провела дослідження по всій території України на початку 2014 року, де було виявлено, що найбільш

вразливими до вірусних загроз є користувачі трьох областей: Закарпатська область – рівень зараження ПК – 18,37 %, Рівненська область – 15,88 %, Кіровоградська область – 15,84 %, користувачі яких були атаковані вірусами, рекламними модулями та троянськими програмами (дані троянці, наприклад, створені для крадіжки конфіденційних даних користувачів, в тому числі паролів доступу до Інтернет ресурсів, номерів кредитних карт, іншої інформації, яку можна використати для крадіжки приватних фінансів користувача). Саме тому, специфіка розслідування комп'ютерних злочинів полягає в тому, що слідчий повинен бути не тільки добрим юристом, а й кваліфікованим програмістом, який є фахівцем у сфері інформаційних ресурсів.

Підсумовуючи викладене, слід відзначити, що зазначені в статті аспекти встановлення характеру та розміру шкоди при розслідуванні злочинів у сфері використання комп'ютерних технологій, дозволили визначити ряд теоретичних і прикладних питань, вирішення яких, на наш погляд, може сприяти вдосконаленню розслідування злочинів зазначеної категорії, але потребує більш детального та поглибленого теоретичного підходу до вирішення цих питань.

Одержано 28.10.2014

УДК 343.98

Олександр Валерійович ДІХТЯРУК,
заступник начальника – начальник відділу боротьби зі злочинами у сфері обігу протиправного контенту та господарської діяльності управління боротьби з кіберзлочинністю
ГУМС України в Одеській області

НЕЗАКОННЕ ВИКОРИСТАННЯ ЗНАКА ДЛЯ ТОВАРІВ І ПОСЛУГ, ФІРМОВОГО НАЙМЕНУВАННЯ, КВАЛІФІКОВАНОГО ЗАЗНАЧЕННЯ ПОХОДЖЕННЯ ТОВАРУ

Проблема боротьби з контрафактною та фальсифікованою продукцією – сьогодні одна з найгостріших у світі. Обороти від її нелегального виробництва і використання непорівнянні з оборотами від торгівлі наркотиками та зброї, а також доходами від видобутку нафти. Всесвітньовідома Коко Шанель говорила: «Підробки – це вищий ступінь визнання і захоплення». Але сьогодні з нею згодні далеко не всі дизайнери, бо майже 90 % одягу класу люкс, яка продається у всьому світі, – це підробка.

Парфуми і шампуні, ноутбуки та плейери, шоколад і мінеральна вода, годинники та автомобільні запчастини – сьогодні

навряд чи можна знайти хоч один товар, який не намагалися б підробити. Річний обсяг продажів контрафактної продукції у світі оцінюється в більше ніж 600 млрд. доларів.

Так нещодавно до УБК ГУМВС України в Одеській області надійшло звернення офіційного представника на території України всесвітньовідомої компанії по виробництву парфумів, в особі директора щодо незаконної реалізації в мережі Інтернет, а саме через інтернет-магазин здійснюється розповсюдження контрафактної, парфумерної продукції відомих торгівельних марок, а саме «Burberry», «Chanel», «Lacoste», «Nina Ricci», «Versace» тощо.

Матеріали звернення були направлені до СУ ГУМВС України в Одеській області та у подальшому за належністю де внесені до ЄРДР за ознаками правопорушення, передбаченого ч. 3 ст. 229 КК України.

В рамках доручення на проведення слідчих (розшукових) дій слідчого було встановлено Інтернет магазин реалізації, а також місця реалізації та зберігання контрафактної парфумерної продукції відомих торгівельних марок і за клопотанням слідчого отримані ухвали суду на проведення обшуків за чотирма адресами, де здійснюється зберігання та збут контрафактної продукції торгівельних марок.

В рамках виконання доручення на проведення слідчих (розшукових) дій для отримання доказів та фактичних даних про злочинну діяльність було здійснено контрольну закупку контрафактної продукції з використання сил УОТЗ.

У подальшому працівниками УБК ГУМВС спільно зі слідчими було проведено обшуки за вказаними адресами в результаті чого встановлені збут та зберігання контрафактної продукції торгівельних марок, з подальшим вилученням грошових коштів здобутих від збуту контрафактної продукції у сумі 70 000 гривень та 2 000 доларів США, а також контрафактної парфумерної продукції торгівельних марок: «Burberry», «Chanel», «Lacoste», «Nina Ricci», «Versace» та інших.

Загальна кількість товару вилученого при проведенні слідчих (розшукових) дій складає 107 062 одиниці.

Діяльність вищевказаних торгівельних об'єктів, де здійснювалося зберігання та збут контрафактної продукції торгівельних марок: «Burberry», «Chanel», «Lacoste», «Nina Ricci», «Versace» призупинена, тривають подальші перевірочні заходи.

В подальшому планується встановлення загальної суми збитків, які нанесено офіційному представнику компанії на території України в особі директора, направлення зразків вилученої парфумерної продукції, торгівельних марок: «Chanel»,

«Lacoste», «Nina Ricci», «Versace» до НДЕКЦ в Одеській області для проведення наукового дослідження з питань відповідності, а також встановлення офіційних представників інших вилучених торгівельних марок на території України з метою встановлення загальної суми збитків, які нанесено вказаним офіційним представникам від незаконного розповсюдження контрафактної продукції тощо.

З метою вилучення іншої контрафактної продукції, а також знарядь виробництва вже вилученої під часі слідчих дій контрафактної продукції, здійснити комплекс заходів, направлених на встановлення місць (виробництв) з незаконного виготовлення іншої контрафактної продукції торгівельних марок: «Burberry», «Chanel», «Lacoste», «Nina Ricci», «Versace» тощо.

Таким чином проблема підробок товарної продукції є актуальною на сьогодні, але потребує суттєвого аналізу та розробки. Лідируючі позиції з виробництва контрафакту займає Китай і, незважаючи на створення органів щодо регулювання даної проблематики, виникає необхідність проаналізувати її діяльність на предмет ефективності. Відомі бренди намагаються самостійно впоратися з цією проблемою, але дані демонструють негативні тенденції в цьому напрямку.

Одержано 30.10.2014

УДК 343.983

Сергій Олексійович ЗАХАРЧЕНКО,
старший викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

СПЕЦИФІКА ПРИЗНАЧЕННЯ ЕКСПЕРТИЗИ КОМП'ЮТЕРНОЇ ТЕХНІКИ І ПРОГРАМНИХ ПРОДУКТІВ

Ефективність розслідування будь-якого злочину безпосередньо пов'язана з використанням можливостей судових експертиз. Аналіз слідчої та судової практики дає підстави стверджувати, що майже в половині випадків очевидні помилки слідчих на етапах збирання матеріалів для експертних досліджень, призначення експертизи, використання її результатів у доказуванні.

Експертиза комп'ютерної техніки і програмних продуктів як самостійний вид експертиз виникла зовсім недавно і сьогодні зайняла своє неабияке місце серед інших експертних досліджень, які проводяться в рамках досудового розслідування і тому потребує специфічних моментів її підготовки та призначення.

Специфічним є криміналістичне дослідження документів, що виготовлені з використанням комп'ютерних і копіювальних технологій, що останнім часом стає об'єктом пильної уваги криміналістів. Основними завданнями експертизи комп'ютерної техніки і програмних продуктів є: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку [1].

Об'єктами експертизи комп'ютерної техніки і програмних продуктів є такі: системні блоки комп'ютерів та їх комплектуючі, ноутбуки; периферійні пристрої (принтери, сканери, дисководи, модеми, тощо), комунікаційні пристрої комп'ютерів і обчислювальних мереж; магнітні носії інформації (накопичувачі на жорстких та гнучких магнітних дисках, оптичні диски, флешкарти пам'яті); електронні записні книжки, мобільні телефони та інші електронні носії текстової або цифрової інформації.

Практикою напрацьовані певні вимоги до об'єктів, які направляються на експертизу комп'ютерної техніки і програмних продуктів: системні блоки комп'ютера та інші пристрої повинні бути упаковані й опечатані таким чином, щоб виключити будь-яку можливість їхнього пошкодження, вмикання в мережу та розбирання; у протоколі повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд предметів і документів, які направляються на експертизу; при вилученні комп'ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет і далі опечатувати вже сам пакет. Носії інформації також можна упакувати в картонну чи пластмасову коробку і потім її опечатати. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їхня кількість). Коробку з носіями та опис помістити до поліетиленового пакету, який потім заклеїти; під час перевезення комп'ютерних засобів необхідно вжити заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами.

Для дослідження інформації, яка міститься на комп'ютерних носіях, експертові надається сам комп'ютерний носій, а також комп'ютерний комплекс, до складу якого входить досліджуваний носій. У деяких випадках можна обмежитися наданням тільки комп'ютерного носія.

Перед призначенням експертизи комп'ютерної техніки і програмних продуктів слідчий, зазвичай, взаємодіє зі спеціалістом

у відповідній галузі, що може виражатися як у процесуальній, так і непроцесуальній формах. Даний процес є позитивним для слідчого оскільки він має можливість проконсультуватись з фахівцем з питань стосовно: 1) визначання виду експертизи (що залежить від функціонального призначення і природи об'єкта); 2) підбір експерта з необхідною сукупністю знань; 3) формування питань, які будуть винесені перед експертом; 4) підготовка об'єктів для проведення експертизи. О. В. Наріжний зазначає, що проведення непроцесуальних «оціночних» оглядів комп'ютерної техніки спеціалістом на місці події до порушення кримінальної справи є необхідним заходом [2, с. 138]. Та оскільки з прийняттям нового КПК України дана стадія кримінального провадження скасована, тому при розслідуванні комп'ютерних злочинів вважаємо за необхідне залучати спеціаліста для допомоги у проведенні першого ж огляду місця події з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань. Слідчий самостійно або через подання клопотання ініціює проведення експертизи. При призначенні експертизи комп'ютерної техніки і програмних продуктів необхідно максимально конкретно визначати коло питань, які мають бути роз'яснені судовим експертом та обсяг потрібних для експертного дослідження матеріалів, в той же час вони не можуть виходити за межі спеціальних знань експерта. Якщо об'єкти, що підлягають дослідженню, можуть містити чи містять державну таємницю, то в такому випадку експертизу комп'ютерної техніки і програмних продуктів треба проводити відповідно до положень ст. 518 КПК України.

При призначенні експертизи комп'ютерної техніки і програмних продуктів необхідно враховувати її технологічні та технічні особливості, а тому у багатьох випадках місцем її проведення, по можливості, треба обирати місце події або місцезнаходження об'єкта експертизи без його переміщення до експертної установи.

Список використаних джерел:

1. Інструкція про призначення та проведення судових експертиз та експертних досліджень : затв. наказом М-ва юстиції України від 08.10.1998 № 53/5 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0705-98. – Редакція від 22.01.2013.

2. Нарижный А. В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий : дис. … канд. юрид. наук : 12.00.09 / Нарижный Александр Викторович. – Краснодар, 2009. – 270 с.

Одержано 15.10.2014

УДК 343.3/.7

Оксана Олександрівна КНИЖЕНКО,
доктор юридичних наук, професор,
начальник відділу досліджень проблем протидії злочинності
Науково-дослідного інституту
Національної академії прокуратури України (м. Київ);

Дар'я Петрівна МАРЕНИЧ,
провідний науковий співробітник відділу досліджень проблем
протидії злочинності Науково-дослідного інституту
Національної академії прокуратури України (м. Київ)

ПРОБЛЕМИ КВАЛІФІКАЦІЇ НЕЗАКОННИХ ДІЙ З ДОКУМЕНТАМИ НА ПЕРЕКАЗ, ПЛАТІЖНИМИ КАРТКАМИ ТА ІНШИМИ ЗАСОБАМИ ДОСТУПУ ДО БАНКІВСЬКИХ РАХУНКІВ, ЕЛЕКТРОННИМИ ГРОШИМА, ОБЛАДНАННЯМ ДЛЯ ЇХ ВИГОТОВЛЕННЯ

Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення є одним із злочинів, які входять до групи «кіберзлочинів» та такими, що вчиняються у банківській сфері.

Слід відзначити, що під час проведення розрахункових операцій досить часто вчиняються й такі злочини як шахрайство (ст. 190 КК України) та крадіжки (ст. 185 КК України), які поєднані із несанкціонованим втручанням в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України). Тому, кваліфікація незаконних дій з документами на переказ та іншими засобами доступу до банківських рахунків потребує проведення відмежування від суміжних злочинів та оцінки діяння з урахуванням можливої сукупності злочинів.

Так, випадки таємного заволодіння готівкою шляхом механічного пошкодження банкоматів за допомогою газових різаків, кутових шліфувальних машин чи вибуху, шляхом віджимання задніх дверцят банкоматів тощо розцінюються у судовій практиці як крадіжки і не мають відношення до обговорюваної нами проблематики. Стосується це й крадіжки готівки з банкоматів шляхом використання спеціального пристрою, який встановлюється всередині «презентера» банкомату через «шаттер», що відкривається для видачі коштів під час отримання клієнтом готівки. Під час таких дій злочинець, використовуючи справжню карту, маніпулює пристроєм у вигляді вилки, який використовується злочинцями для фіксації

шторки та виймання готівки з банкомату. Зловмисник ініціює операцію на невелику суму з метою установки в диспенсер (вітвір для видачі готівки) такої «вилки». Далі замовляє велику суму та одночасно, притримуючи шторку диспенсера, симулює ситуацію «помилки запиту в умовах відсутності доступу до грошей». Одночасно «софт» банкомата направляє «solicited status», який каже про те, що «при видачі відбувся збій обладнання, клієнт до набраної суми доступу не мав». Злочинець робить відміну раніше списаної суми та баланс його карти не змінюється. Між тим, «вилка» з грошима виймається з банкомата з можливим одночасним пошкодженням «шаттера» (шторки). Кількість повторів в одному банкоматі залежить від працездатності АТМ та лінії поведінки шахрая. У такий спосіб вчиняється викрадення коштів з банкомату під назвою «ліванська петля» [1, с. 72–73].

При цьому слід звернути увагу, що фізичне проникнення до банкомату з метою викрадення коштів, що там знаходяться, зокрема за допомогою технічних пристроїв, слід кваліфікувати за ч. 3 ст. 185 КК України (як крадіжка, поєднана з проникненням в інше сховище).

Зважаючи на те, що диспозиція ст. 200 КК України передбачає декілька форм злочинного прояву, окремо слід зупинитися на кожному з них та висвітлити їхні специфічні ознаки. Це в свою чергу, насамперед обумовлює визначитися з такими поняттями як: 1) документи на переказ грошових коштів; 2) платіжні картки; 3) інші засоби доступу до банківських рахунків; 4) електронні гроші. Слід зазначити, що назва ст. 200 КК України вказує ще й на обладнання для виготовлення платіжних карток, документів на переказ, інших засобів доступу до банківських рахунків, однак таке обладнання не може бути визнане предметом аналізованого складу злочину, оскільки про нього не йдеться у диспозиції зазначеної норми. В літературі зазначається, що обладнання для виготовлення засобів доступу до банківських рахунків – це комплексна категорія, яка має відображати виготовлення документів на переказ (як в паперовому, так й електронному виді), платіжних карток та інших засобів доступу до банківських рахунків. Є дві групи ознак такого обладнання: 1) наявність апаратних та 2) наявність програмних засобів. Під апаратними засобами розуміються технічні, які використовуються для обробки і пересилання даних: механічне, електричне й електронне обладнання, що застосовується з метою обробки і пересилання даних. До апаратних засобів належать: АЕОМ (у тому числі сервер, персональний комп'ютер), периферійне обладнання, фізичні носії

машинної інформації, до яких відносять програмне забезпечення (системні, прикладні, інструментальні програми) та машинну інформацію. Під програмними засобами розуміються об'єктивні форми даних і команд, призначених для функціонування комп'ютерів і комп'ютерних пристроїв з метою одержання визначеного результату, а також підготовлені і зафіксовані на фізичному носієві матеріали і аудіовізуальні відображення, отримані під час їх розробок [2]. Програмні засоби можна розглядати і як частину комп'ютерної системи, і як самостійний предмет, для якого комп'ютер є оточуючим (периферійним) середовищем.

У літературі неодноразово порушувалося питання про те, які ж саме дії з обладнанням для виготовлення засобів доступу до банківських рахунків законодавець розуміє як незаконні. Дехто із вчених пропонує виходити з тієї позиції, що придбання, зберігання, перевезення, пересилання, використання зазначеного обладнання для виготовлення таких засобів, згідно зі ст. 14 КК, можна розглядати як підготовку до злочину. На нашу думку, така кваліфікація є вимушеною через недосконалість диспозиції норми, що аналізується, й у майбутньому в диспозиції цієї норми доцільно передбачити таке діяння як відповідало повною мірою назві статті, що значно спростить притягнення до відповідальності осіб, які виготовляють таке обладнання.

Як різновид фальсифікації платіжних карток слід визнавати злочини під час вчинення яких у законних держателів викрадаються платіжні засоби та в їхні реквізити (номер, ім'я та прізвище, підпис, цифровий код на магнітній стрічці) вносяться інші дані. Крадіжка таких даних здійснюється у різних місцях, наприклад, у звичайних магазинах, де номер картки залишається у касира на сліпі. Тобто інформація про реквізити справжніх платіжних карток викрадається особами, які мають доступ до інформаційних баз даних про здійснені трансакції з використанням платіжних карток. Це переважно працівники банків, процесингових установ, торгівельних закладів.

Список використаних джерел:

1. Система и меры предупреждения преступлений в банках при проведении расчетно-кредитных операций : монография / А. В. Давыдова, Д. Н. Иконников, А. Я. Казаков, В. Д. Ларичев. – М. : Юрлитинформ, 2013. – 392 с.

2. Берзін П. Проблеми кваліфікації банківських комп'ютерних злочинів [Електронний ресурс] / Павло Берзін. – Режим доступу: http://www.crime-research.ru/library/berzin2.html.

Одержано 20.10.2014

УДК 343.98.06(477)

Олександр Олександрович КОЗЛЕНКО,
здобувач
Харківського національного університету внутрішніх справ

СТРУКТУРА ПРАВОВИХ ВІДНОСИН ОПЕРАТОРІВ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ТА ПРАВООХОРОННИХ ОРГАНІВ У ПРОТИДІЇ ЗЛОЧИНАМ

Під телекомунікацією слід розуміти електрозв'язок, тобто передавання, випромінювання та приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, дротових, оптичних або інших електромагнітних системах, зокрема бездротового доступу. Операторами телекомунікацій слід вважати суб'єктів господарювання, які мають право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж. Крім операторів, телекомунікаційні послуги мають право надавати провайдери, тобто суб'єкти господарювання, які мають право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку. Телекомунікаційна мережа – це комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, дротових, оптичних чи інших електромагнітних системах. Телекомунікаційна послуга це продукт діяльності оператора або провайдера телекомунікацій, спрямована на задоволення потреб споживачів у сфері телекомунікацій, зокрема: фіксованого телефонного зв'язку (тобто дротового) та рухомого (тобто мобільного) телефонного зв'язку, доступу до мережі Інтернету.

«В умовах динамічного розвитку науково-технічного прогресу відбувається вдосконалення форм і методів злочинної діяльності, головними рисами якої є маскування протиправних дій, використання сучасних технічних засобів які полегшують процес скоєння злочинів та їх приховування. Ці чинники помітно ускладнюють виконання завдань слідчих та оперативних підрозділів щодо протидії злочинам, а також діяльність щодо нейтралізації злочинних угрупувань. Вказані обставини обґрунтовують і потребують використання в слідчій та оперативно-розшуковій діяльності сучасних інноваційних технологій, застосування нових методів щодо протидії злочинам.

Слід зазначити, що у співробітників оперативних підрозділів та слідчих ОВС України разом з технічним розвитком з'являються нові технічні можливості, які можуть посприяти протидії злочинам, встановленню місця знаходження осіб, які становлять оперативний інтерес, з'ясування особистих зв'язків особи та документування її діяльності. Ці можливості пов'язані з мережею мобільного зв'язку України та мережею всесвітньої інформаційної системи загального доступу – Інтернет.

Структура правових відносин передбачає наявність у одного суб'єкта – права, а у іншого суб'єкта – зобов'язання. Правовідносини у яких не буде правоуповноваженої або правозобов'язаної особи є алогічними і можуть породжувати юридичні спори та фактичні протистояння. Безумовно, що право (законний інтерес) державного органу або посадової особи засновується на повноваженнях, передбачених правовими нормами, але і зобов'язання правовиконавців теж повинні бути визначені правом. Для конструктивних правовідносин завжди слід знаходити наявність правової норми щодо прав одного суб'єкта та відповідних їм обов'язків іншого суб'єкта. Це обумовлено положеннями ст. 19 Конституції України у якій зазначено, що правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством. Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Цей нормативний припис носить імперативний характер.

Працівникам практичних підрозділів ОВС слід враховувати, що відповідно до ст. 68 Конституції України кожний, хто перебуває на території України, зобов'язаний неухильно додержуватися законів України. Ця конституційна норма є основною та фундаментальною підставою для подальшого апелювання щодо правил побудови відносин між правоохоронними органами України та іншими суб'єктами правових стосунків, зокрема і з операторами телекомунікаційних послуг.

Для правильної організації правових відносин з операторами телекомунікаційних послуг, зазначену вище конституційну норму (тобто ст. 68 Конституції України), слід застосовувати у сукупності з тими правовими нормами законів України, які носять загальний імперативний та зобов'язуючий характер. У таких нормах повинно бути зазначено про обов'язок щодо сприяння правоохоронним органам України у діяльності по боротьбі зі злочинністю та обов'язок щодо вчинення певних дій. Такими правовими нормами є:

1) стаття 6 Закону України «Про міліцію» у якій зазначено, що державні органи, громадські об'єднання, службові особи, трудові колективи, громадяни зобов'язані сприяти міліції в охороні громадського порядку і боротьбі із злочинністю;

2) стаття 11 Закону України «Про оперативно-розшукову діяльність», у якій вказано, що органи державної влади, підприємства, установи, організації незалежно від форми власності зобов'язані сприяти оперативним підрозділам у вирішенні завдань оперативно-розшукової діяльності.

Таким чином, кожна особа зобов'язана сприяти міліції у діяльності по боротьбі із злочинністю та у вирішенні завдань оперативно-розшукової діяльності, оскільки цей обов'язок передбачено Законами України, а як зазначено у ст. 68 Конституції України, кожний зобов'язаний неухильно додержуватися законів України.

Одержано 28.10.2014

УДК 343.98

Марина Олександрівна КРАВЦОВА,
ад'юнкт
Харківського національного університету внутрішніх справ

МОТИВАЦІЯ КІБЕРЗЛОЧИНІВ: ДАНІ ЕМПІРИЧНОГО ДОСЛІДЖЕННЯ

Кримінологічна суть злочину, відповідно й особистість того, хто його вчиняє, найбільш повно виявляється в змісті мотивації злочинної діяльності, оскільки саме у мотивах виражається не будь-яка окрема риса особистості, а у певному сенсі вся людина, всі характерні для неї властивості й особливості. Мотив цементує думку й волю, свідомість і дію й служить тією основною пружиною, що направляє вольовий процес, надаючи йому певний зміст. Отже мотив це одне з найбільш суттєвих психологічних понять, за допомогою якого розкривається внутрішня природа людських вчинків, їх суть. Він виступає найважливішим компонентом психологічної структури будь-якої людської діяльності, її рушійною силою, позначає внутрішню (психологічну) причину вчинків конкретної особи.

Під мотивом, як правило, розуміють внутрішнє спонукання, яким керується особа, вчиняючи суспільно небезпечне діяння. Це суб'єктивний стимул людських учинків, у якому знаходять вираження рушійні сили особистості, пов'язані із задоволенням її потреб [1, с. 7].

В цілому більшість дослідників виокремлюють наступні групи мотивів, типових для вчинення кіберзлочинів: 1) корисливий мотив, 2) хуліганські мотиви, 3) помста, 4) політичні мотиви [2].

При цьому, як вказують вітчизняні дослідники, за суттєвих змін у технологіях, внутрішня сторона цього виду злочинів не зазнала докорінних змін. Корисливі ж мотиви переслідуються злочинцями в більшості комп'ютерних злочинів. З корисливим мотивом вчиняються переважно діяння, пов'язані з розповсюдженням шкідливих програм.

Проведений нами аналіз матеріалів кримінальних справ також показав, що характерними для кіберзлочинців є наступні мотиви: користь (86 %), помста (6 %), потреба у самоствердженні (3 %), хуліганські мотиви (2 %), кар'єризм (1 %), інша особиста нематеріальна зацікавленість (2 %).

Отже слід погодитися з фахівцями в тому, що мотиви кіберзлочинів є стандартними і принципово не відрізняються від інших видів злочинів. Однак, нажаль, не відрізняються вони від інших злочинів й у наступному.

У більшості випадків тільки обвинувальний акт та вирок суду містять вказівку на мотив, який в ході кваліфікації відповідного діяння встановив орган досудового розслідування або суд, спираючись на суб'єктивне ставлення винної особи до вчиненого нею діяння, виходячи з її ж пояснення. Глибокого аналізу мотивації вчиненого діяння ані під час досудового розслідування, ані судом фактично не проводиться. Це призводить до того, що мотиви вчинення значної частини досліджуваних злочинних діянь пояснюються користю чи хуліганськими спонуканнями.

Дослідники ж часто для позначення мотиву вчинення кіберзлочинів оперують такими дефініціями як «дослідницький інтерес», «допитливість» тощо, вносячи в дане питання ще більше непорозуміння. Наприклад, Л. В. Борисова вказує, що значне місце в списку мотивів комп'ютерних злочинів займає «унікальний за своєю суттю мотив – інтелектуальна боротьба між людиною і комп'ютерною системою» [3].

Ще далі пішли деякі вчені, вказуючи на існування окремого типу комп'ютерних злочинців «психічно хворих осіб, які страждають новим видом психічних захворювань – інформаційними хворобами або комп'ютерними фобіями». В. В. Крилов, з огляду на мотиви вчинення злочину, рівень професійної підготовки і соціального стану, виокремлює такі групи комп'ютерних злочинців: 1) «хакери» – особи, які розглядають захист комп'ютерних систем як особистий виклик і зламують їх

для одержання повного доступу до системи і задоволення власних амбіцій; 2) «шпигуни» – особи, що зламують комп'ютери для одержання конфіденційної інформації, яку можна використовувати в політичних, військових та економічних цілях; 3) «терористи» – особи, що розглядають злом інформаційних систем як створення ефекту небезпеки з метою політичного впливу; 4) «корисливі злочинці» – особи, які проникають в інформаційні системи для одержання особистої майнової або немайнової вигоди; 5) «вандали» – особи, які зламують інформаційні системи для подальшого руйнування; 6) психічно хворі особи, які страждають від нового психічного захворювання – інформаційна хвороба або комп'ютерна фобія [4, с. 148].

Зважаючи на те, що будь-яка фобія це психічна аномалія, а не хвороба, отже не виключає осудності, а що таке «інформаційна» хвороба залишається лише здогадуватися, хотілось б зазначити наступне.

Як відзначають фахівці, юристи та кримінологи досить рідко зверталися до неусвідомлюваного. Характеризуючи мотиви вчинення як злочинів в цілому, так й окремих їх видів, дослідники зазвичай оперують лише категорією усвідомлюваних мотивів, звертаючись для встановлення дійсних мотивів злочинної поведінки до сфери неусвідомлюваного дуже рідко, або взагалі ігноруючи її через складність та глибину проблеми.

На наш погляд, у всіх наведених випадках доцільно вести мову не про якісь особливі мотиви вчинення кіберзлочинів, а саме про мотиви, що лежать у сфері неусвідомлюваного, перш за все, про мотиви ствердження і самоствердження та так звані ігрові мотиви.

Отже, досліджуючи мотивацію кіберзлочинів, не треба шукати якихось специфічних мотивів (або вигадувати їх), а необхідно оперувати усталеними поняттями та категоріями. Специфіка кіберзлочинності полягає не стільки в мотивах вчинення злочинів даного виду, скільки в особливостях їх реалізації, обумовлених специфікою середовища та засобів їх вчинення.

Розглядаючи мотиви вчинення кіберзлочинів слід враховувати те, що, як слушно вказує А. В. Савченко, різноманітні мотиви не тільки не виключають один одного, але й доповнюють, підсилюють один одного [5, с. 25]. Враховуючи специфіку кіберзлочинів, при їх вчиненні можливі різні варіанти поєднання та змішування мотивів (залежно від особливостей суб'єкта злочину, специфіки їх виникнення та формування).

Як відомо, мотив є найважливішою обставиною, що характеризує ступінь суспільної небезпеки самого злочинного діяння,

а також характер і ступінь суспільної небезпеки особи, яка його вчинила. Отже правильне встановлення мотиву вчинення кіберзлочину дозволить не лише уникнути помилок при кваліфікації, а й досягнути успішної реалізації принців справедливості та невідворотності покарання.

З практичної точки зору встановлення мотиву та мети вчинення кіберзлочину дозволяє, зрозуміти внутрішню суть злочинної поведінки винного та виявити наявність чи відсутність сукупності злочинів.

Так, наприклад, фахівці вказують, що корисливий мотив при вчиненні «Несанкціонованого доступу до комп'ютерної інформації», може свідчити про те, що цей злочин був вчинений у сукупності з такими злочинами, як: «Порушення авторського права та суміжних прав» (ст. 176 КК України), «Вимагання» (ст. 189 КК України), «Розголошення комерційної таємниці» (ст. 232 КК України) тощо. Встановлення ж мети – передачі інформації іноземній державі, іноземній організації або її представникам при вчиненні громадянином України злочину «Несанкціонований доступ до комп'ютерної інформації» свідчить про сукупність вчинення даного злочину із злочином, передбаченим ст. 111 КК України «Державна зрада», встановлення мети – порушення роботи автоматизованої системи, що забезпечує функціонування атомної електростанції, може вказувати на сукупність вчинення досліджуваного злочину із злочином «Диверсія» (ст. 113 КК України).

Отже, встановлення мотивів кіберзлочинів грає значну, а у деяких випадках визначальну роль для привільної кваліфікації вчиненого діяння (особливо враховуючи корисливу спрямованість кіберзлочинів та поширеність вчинення їх у сукупності з іншими злочинами), а також сприяє виявленню причин (перш за все, суб'єктивних) та умов їх вчинення.

Список використаних джерел:

1. Антонян Ю. М. Личность преступника / Ю. М. Антонян, В. Н. Кудрявцев, В. Е. Эминов. – СПб. : Юрид. центр Пресс, 2004. – 364 с.

2. Косенков А. Н. Общая характеристика психологии киберпреступника / А. Н. Косенков, Г. А. Черный // Криминологический журнал БГУЭП. – 2012. – № 3. – С. 87–94.

3. Борисова Л. В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти / Л. В. Борисова // Актуальні проблеми держави і права. – Вип. 44. – 2008. – С. 76–80.

4. Крылов В. В. Расследование преступлений в сфере компьютерной информации / В. В. Крылов. – М. : Городец, 1998. – 264 с.

5. Савченко А. В. Мотив і мотивація злочину : монографія / А. В. Савченко. – Київ : Атіка, 2002. – 144 с.

Одержано 17.10.2014

УДК 343.98

Максим Юрійович ЛІТВІНОВ,
кандидат юридичних наук,
доцент кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ЩОДО УПОРЯДКУВАННЯ ЧАСТИНИ СУСПІЛЬНИХ ВІДНОСИН У СФЕРІ КІБЕРБЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ, ПОВ'ЯЗАНИХ ІЗ ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ

Нові технології створюють безпрецедентні зміни можливостей (віртуалізація, криптографія, відсутність кордонів у мережах, транснаціональні соцмережі), які, якщо мають цінність для суспільства, порівнянну з наявними аналогами поза мережею, повинні і захищатися з аналогічним ступенем інтенсивності. Але багато нових сфер можливостей, що надаються новими технологіями, в національному законодавстві взагалі відсутні.

Залишивши все як є зараз, суспільство ризикує бути маніпульованим ззовні (троллізм, псевдоновини, фейкові думки псевдо експертів), продовжувати морально розкладатися за рахунок порнографії (чим далі-тим більше збочень), не поважати інтелектуальну працю, провокувати прояв низинних мотивів поведінки (брехня, лестощі, агресія, інші стадні рефлекси і скотинячі інстинкти).

Водночас знаходження балансу між ефективним захистом суспільних відносин у сфері кібербезпеки та недопущенням цензури потребує суспільного договору, який відповідно визначається адекватним розумінням проблеми не лише фахівців, але й переважної більшості дієздатних громадян України.

Наразі пропонуємо власне бачення механізму боротьби з протиправним контентом в мережі Інтернет.

1. Будь-який суб'єкт інформаційної діяльності (людина, представник громадськості, державний чиновник, правоохоронець) звертається на гарячу лінію волонтерської організації, представник якої має електронний цифровий підпис (ЕЦП), і, уособлюючи собою перший «суспільний» фільтр повідомлень, подає офіційну заяву про наявність ознак правопорушення (тобто про те, що факт трансляції контенту за конкретним URL-посиланням має ознаки кримінального правопорушення (КП), позначеного в Кримінальному кодексі (КК).

2. Згідно з Кримінальним процесуальним кодексом (КПК), заяву має розглядати прокурор або слідчий, який є другим фільт-

ром, має повноваження оцінити ознаки злочину і внести до єдиного реєстру досудових розслідувань (ЄРДР) вказану в заяві подію.

3. Безпосередньо після внесення події до ЄРДР, слідчий, прокурор отримують право застосувати «Захід забезпечення кримінального провадження» (якого зараз не існує!). Наприклад «Тимчасове обмеження доступу до ресурсу з протиправним контентом» (робоча назва), отримуючи санкцію суду у відповідь на клопотання (за аналогією з іншими заходами забезпечення КП в розділі 2 КПК), а в окремих випадках – дозвіл прокурора на термінове обмеження доступу до винесення такого рішення суду з його подальшим отриманням протягом 24 годин).

4. У відповідному розділі сайту ЄРДР (якого зараз не існує) вноситься URL (можливо за певних обставин – IP, домен), і формалізований ідентифікатор контенту (кеш файлу, частина тексту, сигнатура програми тощо).

5. Таблиця, яка формується в ЄРДР щодо внесених ресурсів з протиправним контентом надається провайдерам і використовується ними для обмеження доступу абонентів.

6. Звернення власника заблокованого ресурсу з клопотанням до слідчого, прокурора (на етапі термінового обмеження до рішення суду) або до судді (після прийняття рішення про тимчасове обмеження доступу) – тягне за собою прийняття відповідного рішення.

7. При знаходженні ресурсу в юрисдикції України – обмеження триває до винесення вироку або закриття справи, а також до прийняття суддею окремої ухвали за умови обґрунтованого клопотання володільця (власника) ресурсу, до якого обмежено доступ.

8. При знаходженні ресурсу поза юрисдикцією України і за відсутності складу злочину – КП підлягає закриттю, проте особа, яка приймає рішення про закриття КП має вирішити питання про продовження обмеження доступу на невизначений термін або до появи клопотання володільця (власника) ресурсу. (Пояснення: наприклад, продаж наркотиків або розповсюдження порнографії у деяких країнах не є кримінально караним, тому складу злочину в діях іноземця, який розміщує такий контент – не буде, але подія триваючого злочину у вигляді трансляції порнографії або реклами наркотиків на територію України – буде.)

Підсумовуючи, зазначимо, що на теперішній час стан технікної анонімності, в якому знаходяться наші користувачі, призводить до безкарності порушників, бо відновити порушені права, особливо несуттєво порушені, стає незрівнянно дорого / складно у порівнянні з розміром збитку або ступенем завданої шкоди.

Одержано 23.10.2014

УДК 343.98

Тетяна Петрівна МАТЮШКОВА,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ТИПОВІ СЛІДЧІ СИТУАЦІЇ, ТАКТИЧНІ ЗАВДАННЯ ТА АЛГОРИТМ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Стрімке розповсюдження засобів обчислювальної техніки й сучасних комп'ютерних технологій у різних галузях та у побуті, зневажливе ставлення користувачів мережі Інтернет та інших осіб до безпеки інформаційних даних призводить до значного збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (далі – ЕОМ), систем та комп'ютерних мереж і мереж електрозв'язку. Якщо у 2012 році цих видів злочинів виявлено 138, то у 2013 році – 581, при чому 412 із них – це несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем (далі – АС), комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України). Та лише у 116 випадках їх вчинення особам вручені повідомлення про підозру, у 298 кримінальних провадженнях на кінець 2013 року рішення не прийнято. Аналіз наукової літератури та матеріалів слідчої і судової практики дозволяє визначити типові слідчі ситуації, тактичні завдання і засоби їх розв'язання при розслідуванні комп'ютерних злочинів.

В більшості випадків інформація про досліджувані злочини виявляються: 1) службами з питань інформаційної безпеки організацій, внаслідок регулярних перевірок надійності системи доступу до інформації; 2) випадково користувачами інформаційних систем при їх використанні; 3) посадовими особами контролюючих органів під час проведення бухгалтерських ревізій, аудиту; 4) оперативним шляхом правоохоронними органами; 5) слідчими в ході проведення досудового розслідування у інших кримінальних провадженнях.

Типові слідчі ситуації початкового етапу розслідування комп'ютерних злочинів обумовлені проміжком часу між вчиненням злочину до його виявлення, наявністю на місці події та характером слідів злочину, обсягом інформації про злочинця, використані ним спосіб і засоби незаконного втручання.

Перша ситуація – комп'ютерний злочин виявлений власником ЕОМ чи АС в момент його вчинення, зафіксовані сліди, підозрюваний затриманий «на гарячому», використаний спосіб та засоби незаконного втручання відомі. Тактичне завдання слідства – фіксація доказів вчинення злочину конкретною особою. Алгоритм розслідування: огляд місця події з вилученням відповідних документів, комп'ютерного обладнання, слідів злочину; затримання, особистий обшук та допит підозрюваного; допит потерпілого, свідків; обшуки у місці проживання, роботи підозрюваного, в інших місцях; призначення відповідних експертиз.

Друга ситуація – комп'ютерний злочин виявлений власником ЕОМ чи АС невдовзі після його вчинення, зафіксовані сліди, що прямо вказують на злочинця, але він не затриманий, є інформація про вид способу та засоби незаконного втручання. Тактичне завдання слідства у цій ситуації полягає в зборі й фіксації доказів вчинення злочину конкретною особою, встановлення місця знаходження та затримання підозрюваного. Алгоритм розслідування: огляд місця події; допит заявника, свідків, потерпілого; витребування документів; призначення судових експертиз; доручення в порядку ст. 40 КПК України з метою встановлення місця знаходження винного, місця, звідки відбувалось вторгнення в АС, інших обставин; обшуки з метою виявлення слідів підготовки й реалізації злочинних дій підозрюваного, використаних ним програмних і технічних засобів.

Третя ситуація – комп'ютерний злочин виявлений під час проведення бухгалтерської ревізії (аудиту) за певний час після його вчинення, відомі особи, які за своїм службовим становищем несуть за це відповідальність, але характер їхньої особистої провини та інші обставини не встановлені. Тактичне завдання слідства у цій ситуації полягає у зборі й фіксації слідів злочину, встановленні мотивів його вчинення, особи злочинця та його можливих співучасників. Алгоритм розслідування: допит заявника, потерпілого; огляд місця події; витребування та огляд відповідної технічної документації, а також записів камер відео спостереження (якщо приміщення ними обладнане); призначення відповідних судових експертиз; допит свідків; доручення в порядку ст. 40 КПК України щодо проведення негласних слідчих (розшукових) дій з метою вивчення особистостей, способу життя, інших даних про осіб, запідозрених у вчиненні злочину, встановлення мотивів їхніх дій тощо.

Четверта ситуація – комп'ютерний злочин виявлений за тривалий час після його вчинення слідчим при розслідуванні у межах іншого кримінального провадження, є певні відомості

про особу (осіб), що його вчинили, сліди відсутні. Тактичне завдання слідства у цій ситуації полягає у виявленні, дослідженні слідів злочину та зборі доказів його вчинення конкретною особою (особами), а також встановленні жертви (жертв) злочину. Алгоритм розслідування полягає у комплексі наступних слідчих (розшукових) дій: доручення в порядку ст. 40 КПК України щодо встановлення потерпілих, вивчення осіб, причетних до вчинення злочину, виявлення слідів та знарядь злочину, встановлення очевидців тощо; допит потерпілого і свідків; огляд місця події; огляд вилучених документів, матеріалів та призначення відповідних судових експертиз. Послідовність проведення зазначених дій залежить від джерела інформації про злочин та конкретних обставин його вчинення.

Врахування слідчими інформації про типові слідчі ситуації, тактичні завдання і засоби їх розв'язання сприятиме підвищенню ефективності розслідування комп'ютерних злочинів.

Одержано 31.10.2014

УДК 343.98

Юрій Юрійович НІЗОВЦЕВ,
здобувач
Національної академії Служби безпеки України (м. Київ)

ЩОДО ВИЯВЛЕННЯ ТА ДОСЛІДЖЕННЯ ОЗНАК ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

В сучасних умовах забезпечення інформаційної безпеки держави – одна з найважливіших складових у комплексі заходів із захисту національних інтересів. Одним з напрямків інформаційної безпеки є технічний захист інформації в інформаційно-телекомунікаційних системах, важливу роль у якому відіграє розслідування випадків несанкціонованого втручання в роботу зазначених систем.

У нашій публікації ми розглянемо один з випадків втручання в роботу інформаційно-телекомунікаційних систем з точки зору можливостей експертно-криміналістичного забезпечення розслідування зазначеного випадку.

Отже, ввечері 25 травня 2014 року на російських телеканалах було анонсовано новину про начебто перемогу на виборах Президента України одного з кандидатів, а саме – Дмитра Яроша. На підтвердження цієї інформації російські ЗМІ продемонстрували зображення нібито сайту Центрвиборчкому України з офіційними результатами виборів.

Попереднє «розслідування» даної ситуації здійснювали спеціалісти CERT-UA (скор. – Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) – спеціалізованого структурного підрозділу Державного центру захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). Саме аналіз їх матеріалів і покладено в основу цієї статті [1–3]. Заздалегідь зауважимо, що усі часові мітки в статті зазначені для часового поясу GMT+03:00.

У якості досліджуваного об'єкту співробітникам CERT-UA була надана побітова копія накопичувача інформації «внутрішнього» веб-сервера cvk.gov.ua. Також досліджувались інші комп'ютери, що входять до мережі ЦВК.

У цілому схема роботи веб-серверів ЦВК виглядала наступним чином. Безпосередньо зміст веб-сторінки (контент) формує «внутрішній» веб-сервер. Крім нього на ресурсах різних провайдерів розміщені так звані «дзеркала», тобто, сервера-копії «внутрішнього» сервера. Відмінністю «дзеркал» від «внутрішнього» сервера є те, що на «дзеркалах» відображається лише статична інформація, яка через певні проміжки часу (15–20 хвилин) отримується від основного («внутрішнього») сервера.

Доступ до «внутрішнього» веб-сервера з мережі Інтернет по доменному імені «cvk.gov.ua» був неможливий, оскільки відповідні записи були заздалегідь видалені з DNS-серверів. Звернутися до зовнішнього інтерфейсу «внутрішнього» веб-серверу можливо було лише вказавши в адресному рядку Інтернет-браузера IP-адресу, яку, до того ж, потрібно було знати (зрозуміло, що при зверненні до доменного імені ця адреса не «видавалася»).

Провівши аналіз журналів веб-сервера, фахівці CERT-UA дійшли наступних висновків.

Починаючи з ранку 22 травня зловмисники здійснюють спроби виявлення вразливих параметрів на веб-сайті «cvk.gov.ua». Сканування на вразливості продовжується й продовж наступних днів до 25 травня включно. 23 травня відбувається «злам» веб-сайту і на нього було завантажено веб-шел (тобто PHP-скрипт, який надає можливість віддаленого прихованого управління веб-сервером). Пізніше на сервер завантажується графічний файл «result.jpg», який містить зображення тієї самої «картинки Яроша».

Увечері 25 травня, а саме о 20:16, фіксується перше звернення до веб-сайту ЦВК виключно за IP-адресою внутрішнього веб-сервера із зазначенням у GET-запиті повного шляху до

картинки «result.jpg» з IP-адреси 195.230.85.129. Зазначена IP-адреса, відповідно до бази даних RIPE, відноситься до діапазону IP-адрес телеканалу «ОРТ».

О 20:17, з різницею в 5 секунд, на «картинку Яроша» з IP-адреси 80.247.35.7 заходять подивитися й співробітники (або особи, які мають доступ до мережі) «Всероссийской государственной телевизионной и радиовещательной компании» (ВГТРК).

Взагалі звернення до «картинки Яроша» мали місце 25 травня 2014 року з 20:16:56 до 20:33:46, після чого «внутрішній» веб-сервер був вимкнений співробітниками ЦВК. За цей час було здійснено 60 звернень з вказаної вище IP-адреси телеканалу «ОРТ».

Слід додатково наголосити, що 25 травня 2014 року побачити «картинку Яроша» можливо було лише зайшовши на «внутрішній» сервер ЦВК за його IP-адресою, а також вказавши повний шлях до файлу «result.jpg». Але ця адреса не була доступна у вільному доступі, а повний шлях до «картинки» взагалі знали лише ті зловмисники, які її помістили на сайт. Побачити ж «картинку Яроша», зайшовши на сайт ЦВК за його офіційним доменним іменем «cvk.gov.ua», було неможливо, оскільки за цим іменем відбувалася адресація на «дзеркала», а не на «внутрішній» веб-сервер ЦВК. У свою чергу, на «дзеркала» «картинка Яроша» ніяким чином не могла потрапити, оскільки вона разом зі своїм скриптом знаходилася не в тій папці «внутрішнього» веб-сервера, з якої відбувалася реплікація.

Під час дослідження змісту накопичувачів інформації комп'ютерів мережі ЦВК особливу увагу спеціалістів CERT-UA привернули три з них, а саме:

– веб-сайт «study.cec.net», який, по словам представників ЦВК, функціонував як навчальний проект ОБСЄ;

– веб-сайт «cvk.gov.ua», доступ до якого повинен був бути і був з мережі Інтернет;

– комп'ютер головного адміністратора мережі ЦВК.

Увагу звернув на себе той факт, що на цих комп'ютерах в однакових папках під однаковими назвами містилися одні й ті ж виконувані файли (правда, створені у різний час), а саме:

– «xpssvcs.exe»;

– «vcdcs.exe»;

– «winexesvc.exe».

Два з приведених вище файлів являють собою різні версії доволі відомої програми «Зргоху», яка є маленьким багато платформенним набором проксі-серверів. До цього набору окрім інших входить також й SOCKS-проксі-сервер, тобто функціонал

мережевого протоколу, що дозволяє клієнт-серверним додаткам прозоро використовувати сервіси за міжмережевими екранами (фаєрволами, брандмауерами).

Третій файл – «winexesvc.exe» – програма Winexe (Remote Windows-command executor), призначена для віддаленого виконання команд, що запускаються з систем GNU/Linux, на ЕОМ з операційними системами Windows.

Щоб більш повно зрозуміти суть проблеми, слід описати місце кожного з зазначених вище комп'ютерів у мережі ЦВК.

Доступ до сервера «study.cec.net» через протокол ssh (з привілеями root) мали представники компанії-розробника рішень для електронного голосування SOESoftware (рішення цієї компанії забезпечують прозорість виборів у 34 штатах США). Щодо цього сервера, то звертають на себе увагу перш за все такі два моменти. По-перше, значення рівня безпеки (security level) для сегменту мережі, в якому знаходився цей сервер, був вищим за рівень безпеки для зон, в яких знаходилися сервер корпоративної електронної пошти та веб-сервер ЦВК. Теоретично, враховуючи відсутність політик фільтрації на відповідному інтерфейсі, з сервера «study.cec.net» були доступні поштовий сервер та веб-сервер ЦВК. А по-друге, на цьому сервері було помічено працюючий процес Зproxy.

На сервері «cvk.gov.ua», як вже зазначалося вище, було виявлено веб-шел. Крім того, на цьому сервері також було знайдено все той же Зproxy, а також файли winexesvc.exe та lsass.exe (усі вони були створені 24.04.2014).

Вкрай небезпечною є схема підключення веб-сервера до мережі: з одного боку – він підключений до міжмережевого екрану Cisco ASA (так і повинно бути), але, з іншої сторони, також є його підключення і до локальної мережі ЦВК. По суті виходить, що веб-сервер не ізольований в DMZ-зоні, а як раз навпаки – виступає сполучною ланкою між мережею Інтернет та внутрішньою мережею ЦВК.

Комп'ютер головного адміністратора мережі ЦВК відповідно до існуючих в ЦВК політик контролю доступу (ACL) міг мати доступ до серверу адміністрування (звідки були доступні вже всі пристрої), а також до деякого серверного, активного мережевого обладнання та пристроїв захисту. На цьому комп'ютері також було виявлено виконуваний файл «xpssvcs.exe» (створений 28.04.2014), а також файл «winexesvc.exe» (створений ще 31 березня 2014 року).

Підсумовуючи викладене можна зробити висновок, що як мінімум починаючи з 24 квітня до 25 травня 2014 року (тобто за 32 дні) зловмисники мали несанкціонований доступ до

відомчої мережі ЦВК, використовуючи «внутрішній» вебсервер ЦВК як «точку входу». Якщо ж брати за точку відліку час створення файлу «winexesvc.exe» на комп'ютері головного адміністратора мережі ЦВК (31 березня 2014 року), тривалість несанкціонованого доступу виходить ще довшою.

Аналізуючи результати дослідження спеціалістами CERT-UA втручання в роботу інформаційної системи ЦВК, можна зробити наступні висновки.

Одним з основних методів, який застосовується для виявлення та дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем, є дослідження журнальних файлів (log-файлів) фіксації подій у системі. Таким чином дуже важливим є правильне налаштування журналювання. Фіксуватися повинні всі важливі для системи події, особливо ті, що стосуються безпеки. Повнота фіксації повинна бути з одного боку достатня для розуміння подій у системі, а з іншого – не переобтяжена зайвими деталями, оскільки це потребує більшого дискового простору, а також ускладнює процес дослідження.

Крім того, якщо зловмисник отримає повний контроль над атакованою системою (а в деяких випадках достатньо і часткового), він зможе знищити певні журнальні файли (але це відразу буде помічено досвідченим системним адміністратором і буде чіткою ознакою втручання) або відредагувати їх таким чином, щоб приховати сліди втручання або направити розслідування хибним шляхом. Звичайно, такі можливості залежать від операційної системи сервера та встановленого програмного забезпечення, але журнальні файли у будь-якому разі слід відповідним чином захистити. Це може бути обмеження прав доступу до них у самій системі, або взагалі виділення окремого серверу, на який інші будуть записувати свої журнальні файли, або дублювання журнальних файлів у самій системі та на окремому сервері тощо. Слід зазначити, що на даному етапі не існує єдиного універсального підходу до системи захисту журнальних фалів, вибір конкретної схеми здійснюється у кожному випадку в залежності від наявних можливостей та досвідченості системного адміністратора.

Другим методом, який також часто застосовується для виявлення і дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем, є пошук та наступне дослідження шкідливого програмного забезпечення, встановленого на ЕОМ, що піддавалася втручанню. Разом з тим слід пам'ятати, що при втручанні шкідливе програмне забезпечення на атаковану систему може і не встановлюватися. Крім того, під

час дослідження може бути виявлене шкідливе програмне забезпечення, яке не було задіяне під час втручання або навіть взагалі відноситься до інших зловмисників.

Також під час пошуку шкідливого програмного забезпечення слід враховувати наявність на досліджуваній ПЕОМ антивірусного програмного забезпечення та особливості його функціонування. Антивірус може знищити виявлене шкідливе програмне забезпечення чи його частину і в такому разі подальший пошук цього шкідливого програмного забезпечення та слідів його втручання буде вкрай ускладненим або зовсім неможливий. Кращим для подальшого дослідження є таке налаштування антивірусу, при якому він при виявленні не знищує шкідливе програмне забезпечення, а переносить його у карантин.

Ще одним важливим моментом, на який слід звернути увагу, є людський фактор, який полягає як у професійному рівні співробітників, які забезпечують адміністрування та захист системи, так і в рівні обізнаності та підготовки зловмисників.

Що стосується зловмисника, то, судячи з усього, у наведеному випадку він був недостатньо обізнаним щодо схеми функціонування серверів ЦВК: помістив «картинку Яроша» у невірну папку на сервері. Внаслідок цього дана «картинка» не була реплікована на «дзеркала» і тому не відображалася при заході на сайт ЦВК через його доменне ім'я «cvk.gov.ua».

Якщо говорити про співробітників, які відповідали за налаштування та безпеку серверної інфраструктури ЦВК, то тут також виникають питання. Зазначені вище порушення елементарних правил інформаційної безпеки могло бути або наслідком низького професійного рівня цих співробітників, або халатністю, або навіть свідомим створенням умов для вдалого втручання у роботу інформаційної системи ЦВК. Звичайно, що обвинувачення у скоєнні злочинів не є метою даної публікації, це завдання компетентних органів. Але на думку автора, досліджуючи ознаки втручання в роботу інформаційно-телекомунікаційної системи експерт повинен дослідити у тому числі і такі фактори, які могли сприяти вчиненню злочину, з метою кваліфікованого інформування про це ініціатора проведення експертизи.

Підсумовуючи викладене слід зазначити наступне. Експертиза шкідливого програмного забезпечення є досить складним видом досліджень, що часто вимагає від експерта високої кваліфікації за кількома напрямками досліджень: дослідження комп'ютерної техніки і програмних продуктів, а також

дослідження телекомунікаційних систем і засобів. Крім того, для результативності експертного дослідження заздалегідь відповідним чином повинні бути налаштовані журналювання подій у системі та антивірусне програмне забезпечення. Якщо зазначені налаштування виконані без урахування потреб вірогідного проведення експертизи у майбутньому, проведення цієї експертизи буде значно ускладнено, а у деяких випадках може взагалі не дати бажаних результатів.

Список використаних джерел:

1. «Картинка Ярошa». Часть 1 [Електронний ресурс]. – Режим доступу: http://cert-ua.org/?p=1070.

2. «Картинка Ярошa». Часть 2 [Електронний ресурс]. – Режим доступу: http://cert-ua.org/?p=1097.

3. Взлом ЦИК. Часть 1 [Електронний ресурс]. – Режим доступу: http://cert-ua.org/?p=1162.

Одержано 30.10.2014

УДК 343.98

Оксана Василівна ПЧЕЛІНА,
кандидат юридичних наук,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ СЛУЖБОВОЇ ДІЯЛЬНОСТІ

Сьогодення характеризується суцільними процесами інформатизації та комп'ютеризації в усіх галузях суспільного життя. Причому такі процеси не тільки вдосконалюють діяльність окремих інститутів соціального буття, будучи прогресивними факторами. Ці досягнення науки використовуються й особами під час реалізації їх злочинних намірів. Зокрема, під час вчинення злочинів у сфері службової діяльності.

Таким чином, злочини у сфері службової діяльності тісно пов'язані зі злочинами у сфері комп'ютерних технологій. На це вказує той факт, що 97 % комп'ютерних злочинців були службовцями державних установ і організацій, які використовували комп'ютерні системи та інформаційні технології у своїх виробничих процесах [1, с. 384]. Тобто особа злочинця є внутрішнім користувачем, оскільки перебуває в трудових відносинах із підприємством, організацією, установою, фірмою або компанією, на якому вчинений злочин [2, с. 149].

Вищезазначене підтверджує той факт, що комп'ютерна інформація виступає в якості доказової інформації й обумовлює слідову картину злочинів у сфері службової діяльності. Тому вважаємо за необхідне вказати основні напрямки дослідження комп'ютерної інформації під час розслідування окресленої категорії злочинів.

Так, багато державних органів, органів місцевого самоврядування, підприємств, установ й організацій всіх форм власності у своїй діяльності користуються електронним документообігом (обігом електронних документів). Під останнім прийнято розуміти сукупність процесів створення, обробления, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [3].

Беззаперечно електронний документ, створений за допомогою засобів автоматизації документообігу, підписаний електронним цифровим підписом і збережений в системі у вигляді файлу відповідного формату, значно спрощує роботу з великими об'ємами інформації. І, природно, що електронний вигляд документів накладає на документообіг певні вимоги. Зокрема, кожен виконавець, залучений у документообіг повинен мати електронний підпис [4]. Відповідно під час кримінального провадження необхідно переконатися у автентичності електронного цифрового підпису. Для цього потрібно: по-перше, отримати тимчасовий доступ до відомчої документації, що визначає порядок присвоєння таких підписів за особою, порядок видачі необхідних ключів; по-друге, допитати операторів і адміністраторів у якості свідків, попередньо отримавши консультацію у фахівця, можливо навіть із залученням останнього до цих слідчих (розшукових) дій; і, по-третє, призначити комп'ютерно-технічну експертизу.

Тож під час розслідування злочинів у сфері службової діяльності значну увагу слід приділити виявленню, огляду та вилученню електронних документів, що можуть містити важливу для кримінального провадження інформацію. Ось чому, розпочинаючи досудове розслідування, слідчий повинен ознайомитися з установчими документами, щоб з'ясувати організаційно-правову форму установи, завдання її діяльності та способи їх досягнення. З'ясовуючи зазначені питання, паралельно слід установити порядок ведення діловодства й відповідно звузити коло документів, що підлягають вилученню та подальшому дослідженню.

Під час проведення гласних і негласних слідчих (розшукових) дій, спрямованих на виявлення, фіксацію, вилучення та подальше дослідження комп'ютерної інформації, обов'язково потрібно залучати спеціалістів у галузі знань комп'ютерних технологій та інформаційної безпеки. Це пояснюється тим, що для здійснення безпечних для комп'ютерної інформації (щоб остання не була пошкодженню чи-то знищеною) маніпуляцій потрібні спеціальні знання. Окрім того, для дослідження та фіксації всіх атрибутів електронного документу також потрібно мати відповідні навики та знання.

Досить часто може виникати необхідність під час огляду комп'ютерної техніки, на якій містяться важливі для провадження відомості, зупиняти дію програмного забезпечення, спрямованого на знищення окремих файлів. Також може виникнути необхідність у поновленні знищеного чи пошкодженого електронного документу, з'ясуванні часу та змісту внесення останніх змін у файлову систему. Окрім того, для зняття інформації з електронних інформаційних систем застосовуються спеціальні програми для перехоплення кореспонденції, для чого також потрібні спеціальні знання у відповідній галузі знань.

Отже, дослідження комп'ютерної інформації є невід'ємною та необхідною умовою ефективного розслідування злочинів у сфері службової діяльності.

Список використаних джерел:

1. Біленчук П. Д. Криміналістика. Кредитно-модульний курс : [підручник] / П. Д. Біленчук, Г. С. Семаков ; за ред. П. Д. Біленчука. – 4-те вид., змін., допов. і доопр. – Київ : Дакор, 2014. – 520 с.

2. Алєксєєв О. О. Розслідування окремих видів злочинів : навч. посіб. / О. О. Алєксєєв, В. К. Весельський, В. В. Пясковський. – Київ : Центр учб. літ., 2013. – 278 с.

3. Про електронні документи та електронний документообіг : закон України від 22.05.2003 № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

4. Електронний документ – єдиний механізм по роботі з документами [Електронний ресурс]. – Режим доступу: http://www.ca.upg.kiev.ua/info/ecp/workflow/index.php.

Одержано 23.10.2014

УДК 343.985

Тетяна Іванівна САВЧУК,
кандидат юридичних наук,
старший викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ПЛАНУВАННЯ ДОПИТУ ПІДОЗРЮВАНИХ У ВЧИНЕННІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Соціологічні опитування у різних, насамперед, високорозвинених країнах показують, що серед питань, які турбують людей найбільше, кіберзлочинність посідає одне з чільних місць. Незважаючи на зусилля багатьох держав, спрямовані на боротьбу з кіберзлочинами, їх кількість у світі не зменшується, а навпаки, постійно зростає. Ця проблема вже давно перетнула кордони і стала проблемою міжнародного масштабу. Зокрема це зумовлене технологічним розвитком у сфері комп'ютеризації та розширенням сфери застосування комп'ютерної техніки, яка впроваджується в різноманітні галузі людської діяльності та виконує найважливіші функції сучасного суспільства.

Зважаючи на специфічність комп'ютерних злочинів, та наявність у злочинця професійних знань і навичок, з метою якісного проведення допиту необхідно досить серйозно поставитись до його планування. Так в загальному слідчий повинен для себе з'ясувати наступні аспекти: специфіку справи, особливо питання, що стосуються технічних аспектів підготовки та реалізації злочинних намірів; визначити обставини, які потребують з'ясування або уточнення; підготувати доказові або інші матеріали для пред'явлення в процесі допиту; визначитись із часом та місцем проведення допиту, а також способом виклику допитуваного.

Подальше планування допиту залежить в першу чергу від процесуального статусу допитуваної особи. Так для успішного проведення допиту підозрюваного крім ретельного вивчення матеріалів провадження, необхідно також отримати інформацію про особистість підозрюваного, способи вчинення злочину, докази, які вказують на винність конкретної особи, і т.п.

Крім того перед початком проведення допиту слідчому необхідно:

– отримати кваліфіковані консультації відповідних спеціалістів з даного напряму;

– в окремих випадках доцільно запросити спеціаліста для участі у слідчій дії, який може роз'яснити слідчому показання, що містять відомості технічного характеру;

– ознайомитися зі спеціальною літературою, що стосується предмета допиту;

– приділити увагу пізнанням у сфері електронного документообігу, режиму конфіденційної інформації, засобів і методів її захисту та безпечної обробки;

– детально ознайомитися з результатами проведених слідчих (розшукових) дій (документами, предметами, протоколами тощо);

– визначитись із колом питань, що будуть ставитись допитуваному (питання доцільно розділити на блоки, наприклад, питання що стосуються підготовки до злочину, безпосереднього вчинення злочину та приховання його слідів);

– підготувати додаткові засоби фіксації допиту (диктофони, відеокамери, так як предмет допиту зазвичай складний і насичений великою кількістю технічних термінів).

Необхідно зазначити, що особливість проведення допиту підозрюваного полягає в тому, що на першому допиті підозрюваний може спробувати пояснити факт порушення роботи ЕОМ, її системи або комп'ютерної мережі некримінальними причинами (випадковістю, збігом певних обставин, стороннім впливом і т. п.). Може розповісти і про вчинення таких дій при відсутності злочинного наміру. Для викриття таких осіб добрі результати дає правильна реалізація інформації про злочинну діяльність цієї особи, отриману при проведенні оперативно-розшукових заходів, а так само пред'явлення предметів і документів, що належать підозрюваному і використовувалися при вчиненні комп'ютерного злочину. Уміле використання вказаних відомостей може певним чином вплинути на підозрюваного та отримати правдиві показання на першому допиті.

Зважаючи на специфічність комп'ютерних злочинів доцільно складати письмовий план допиту, він повинен включати:

– відомості про подію злочину та механізм його вчинення (дата, місце, прізвища учасників, технологію злочинної події тощо);

– відомості про особистість допитуваного;

– обставини, що підлягають встановленню;

– перелік питань, що необхідно поставити допитуваному, в правильній послідовності;

– перелік тактичних прийомів, що можуть бути використані для досягнення мети допиту;

– перелік речових і письмових доказів, які необхідно пред'явити допитуваному.

Враховуючи викладене можна підсумувати, що допит підозрюваних у вчиненні кіберзлочинів є особливо складною

слідчою (розшуковою) дією, проведення якої повинно ретельно плануватись за участю спеціалістів у сфері комп'ютерних технологій. Особливості планування допиту залежать від процесуального статусу допитуваного, а також конкретного злочину вчиненого ним.

Одержано 18.10.2014

УДК 343.985:004

Юрій Вікторович СТЕПАНОВ,
кандидат юридичних наук,
доцент кафедри державно-правових
та кримінально правових дисциплін
Донецького університету економіки та права

ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ ПРИ ВИЯВЛЕННІ І РОЗКРИТТІ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Оцінюючи науково-технічну ситуацію, що склалася в світі, можна стверджувати, що людство вступило в епоху інформаційного суспільства. Останніми роками інформація, стаючи одним з визначальних чинників розвитку сучасного суспільства, набуває все більшого значення.

Основним інструментом управління цифровою інформацією і її обробки є комп'ютерна техніка. Сьогодні комп'ютер стає необхідністю не тільки крупних підприємств і організацій, але і окремих людей.

Закономірно, що при розширенні сфери використання інформаційних технологій і різних технологічних процесів зростає і кількість правопорушень, пов'язаних з комп'ютерними технологіями. Використання досягнень науки і техніки при вчиненні злочинів завжди створювало немало проблем правоохоронним органам в розкритті злочинів.

Однією з головних умов успішного розкриття комп'ютерних злочинів є оперативність і невідкладність дій. Проте залучення фахівців до проведення цих заходів не завжди є можливим. У зв'язку з цим особливої значущості набувають знання оперативних працівників в області комп'ютерних технологій. А відсутність у правоохоронця таких знань вабить зволікання в зборі доказової інформації, і як результат – у багатьох випадках правопорушники залишаються безкарними.

Існуюча статистика виявлених комп'ютерних злочинів підтверджує, що отримання і оцінка доказів у справах про злочини у сфері комп'ютерної інформації (комп'ютерних злочинів) –

одне з важко вирішуваних на практиці завдань. Основним видом таких доказів є так звані «електронні докази».

«Електронні докази» – сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв і в електронних пристроях.

При проведенні оперативних заходів не варто забувати про те, що кожна людина, що працює з інформацією в електронному вигляді, прагне її захистити від неправомірних дій з боку інших суб'єктів. Можна привести лише основні напрями подолання перешкод, які створюють правопорушники для захисту інформації.

По-перше, після входу в приміщення, в якому знаходиться об'єкт, необхідно зафіксувати положення всіх осіб, що знаходяться в ньому, не допускаючи при цьому ніяких дій з їх боку по відношенню до будь-яких технічних пристроїв, що є поблизу.

По-друге, якщо комп'ютер, що підлягає огляду, вимкнений, то в міру можливостей потрібно зберегти його стан до прибуття фахівця. Необхідно пам'ятати, що при включенні комп'ютера можуть активуватися певні програми, які можуть проводити дії з інформацією по заздалегідь встановленому алгоритму.

По-третє, необхідно пам'ятати, що разом з програмними засобами модифікації і знищення інформації існують також апаратні способи. Для руйнування магнітних носіїв може використовуватися метод дії на них сильного магнітного поля, яке створюється за допомогою спеціальних пристроїв (генераторів магнітних полів і ін.).

Перш ніж приступити до огляду персонального комп'ютера оперативники повинні знати і дотримуватись загальних правил поводження з обчислювальною технікою і носіями інформації.

Наведемо для прикладу деякі з них:

1. Всі включення (виключення) комп'ютерів і інших технічних засобів проводяться тільки фахівцем або під його керівництвом;

2. Виключення попадання дрібних частинок і порошків на робочі частини комп'ютерів;

3. При роботі з магнітними носіями інформації забороняється торкатися руками до робочої поверхні дисків, піддавати їх електромагнітній дії, згинати диски, зберігати без спеціальних конвертів (пакетів, коробок);

4. Зі всіма незрозумілими питаннями, що зачіпають термінологію, пристрої та функціонування обчислювальної техніки необхідно звертатися тільки до фахівця.

При провадженні слідчих або інших дій, в процесі яких вилучаються об'єкти для виробництва експертних досліджень, необхідно прийняти всі можливі заходи для виключення можливого псування або знищення інформації, що зберігається в комп'ютерах. Включати і вимикати комп'ютери, проводити з ними які-небудь маніпуляції може тільки фахівець в області обчислювальної техніки, що бере участь у виробництві даної слідчої дії.

Оскільки результати експертних досліджень, що проводяться, особливо експертизи програмного забезпечення, безпосередньо залежать від збереження інформації на внутрішніх і зовнішніх магнітних носіях, необхідно вилучити всі створюючи її пристрої, незалежно від їх приналежності (особиста власність, власність даної установи, та ін.).

Якщо вилучення всього пристрою неможливе або недоцільно, слід вилучити встановлений в нім носій (носії) інформації.

Транспортування і зберігання комп'ютерної техніки і інформації повинні здійснюватися в умовах, що виключають її пошкодження.

Враховуючи нестандартність обстановки, в якій може оглядатися місце злочину, про можливість вилучення комп'ютерної техніки і інформації, спосіб упаковки, транспортування і зберіганні вилучених об'єктів вирішується слідчим в кожному конкретно випадку спільно з фахівцем. Процесуальний порядок вилучення об'єктів визначається загальними вимогами Карно-процесуального кодексу України. Як понятих при провадженні слідчих дій рекомендується залучати осіб, що володіють спеціальними пізнаннями у сфері комп'ютерної техніки та інформатики.

Одержано 29.10.2014

УДК 343.98

Галина Константиновна АВДЕЕВА,
кандидат юридических наук,
старший научный сотрудник, ведущий научный сотрудник
НИИ изучения проблем преступности НАПрН Украины

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Глобальная компьютеризация общества, развитие современных информационных технологий и телекоммуникационных систем приводят к появлению новых средств и методов

преступной деятельности. Это, в свою очередь, требует использования адекватных средств противодействия преступлениям, интенсивного внедрения инноваций в работу правоохранительных органов для своевременного выявления, квалифицированного расследования и профилактики преступлений в сфере использования компьютерных технологий.

Следы преступлений в сфере использования информационных технологий образуются в результате воздействия на компьютерную информацию путем внешнего доступа к ней и представляют собой любые её изменения, связанные с событием преступления. Такими изменениями могут быть следы уничтожения, модификации, копирования информации, блокирования информационной системы. Часто преступниками осуществляются модификации баз данных, программ, текстовых файлов, находящихся на стационарных и сменных носителях информации, предназначенных для многократной её перезаписи. Информация может сохранить следы ее частичного уничтожения или модификации (удаления из каталогов имен файлов, удаления или добавления отдельных записей, физического разрушения или размагничивания носителей). Информационными следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть обнаружены при экспертном исследовании компьютерного оборудования, протоколов работы операционных систем, приложений, антивирусных программ, программного кода и др.

Следы неправомерного доступа к информации можно обнаружить в сети Интернет, а затем, исходя из их признаков – установить исходное подключение и техническое средство, с которого совершалось данное правонарушение.

Сегодня для решения проблем борьбы с компьютерными преступлениями необходимо исследование технического характера их осуществления. Однако в настоящее время в ряде государственных судебно-экспертных учреждений некоторые виды исследований не проводятся из-за отсутствия специального оборудования и соответствующих специалистов.

Методики судебно-экспертного исследования компьютерной техники, программных продуктов и телекоммуникационных сетей требуют постоянного обновления и доработки в святи с тем, что через каждые 2–3 года изменяются форматы представления данных, операционные и файловые системы, протоколы и среда переноса данных, технические средства, обеспечивающие процесс передачи информации. Усовершенствование таких методик возможно лишь при использовании

труда ученых в области телекоммуникационных сетей и квалифицированных IT-специалистов, которые не являются сотрудниками государственных экспертных учреждений.

Не способствуют развитию данных видов экспертиз и отдельные нормы проекта закона «О судебно-экспертной деятельности в Украине», разработанного Министерством юстиции Украины. Например, в п. 3 статьи 17 Проекта монопольное право на проведение криминалистических экспертиз (в т. ч. – экспертиз видео- и звукозаписи, цифровых документов и др.) принадлежит государственным судебно-экспертным учреждениям.

В соответствии с Проектом монопольное право на обучение и аттестацию судебного эксперта, выдачу Свидетельства на право проведения судебных экспертиз, а также право на приостановление действия или аннулирование данного Свидетельства принадлежит экспертно-квалификационным комиссиям государственных органов, к сфере управления которых относятся государственные специализированные экспертные учреждения Украины.

Сегодня экспертно-квалификационные комиссии МЮ Украины не имеют возможности аттестовать экспертов и выдавать им Свидетельства на право проведения компьютерно-технической и телекоммуникационной экспертиз из-за отсутствия в их составе соответствующих специалистов. Однако правоохранительные органы Украины по-прежнему надеются на получение результатов полного, всестороннего экспертного исследования объектов телекоммуникационной и компьютерно-технической экспертиз. Возникает ряд вопросов: 1) где опытному IT-специалисту можно получить Свидетельство на право проведения таких экспертиз (согласно Проекту без Свидетельства осуществлять судебно-экспертную деятельность нельзя); 2) у кого будет стажироваться опытный IT-специалист, заплатив за это немалые деньги; 3) к кому может обратиться следователь для проведения особо сложных судебных телекоммуникационных экспертиз? К сожалению, ответа на данные вопросы пока нет.

Компьютерная информация является новым объектом криминалистического исследования, а компьютерная техника (технико-криминалистическое средство для работы с компьютерной информацией) придает этой информации значение источника доказательства. Наиболее полно доказательную базу можно сформировать, привлекая специалистов в области информационных технологий, использующих постоянно обновляющиеся программные средства.

Эффективность расследования преступлений, совершаемых с использованием компьютерных технологий, напрямую зависит от качества проведения компьютерно-технических и телекоммуникационных судебных экспертиз. Отмена монополии государственных судебно-экспертных учреждений на проведение таких экспертиз и подготовку экспертных кадров, а также – при условии развития института негосударственной судебной экспертизы в Украине.

Одержано 01.11.2014

УДК 343.451

Андрій Петрович КОСМИНЯ,
оперуповноважений відділу боротьби з незаконним обігом наркотиків Дніпровського РУ ГУМВС України в місті Києві

ОКРЕМІ ПИТАННЯ РОЗКРИТТЯ НАРКОЗЛОЧИНІВ, ЯКІ ВЧИНЯЮТЬСЯ ЗА ДОПОМОГОЮ МЕРЕЖІ ІНТЕРНЕТ

Незаконний обіг наркотиків в Україні з кожним роком набирає все більші масштаби, постійно видозмінюється і набуває нові форми підлаштовуючись під сучасні реалії. Важливо відмітити, що все частіше для поширення наркотичних засобів, психотропних речовин або їх аналогів використовується глобальна мережа Інтернет. Особливою популярністю користуються спеціально створені сайти та популярні в молодіжному середовищі соціальні мережі. У результаті розвитку систем безготівкової оплати Інтернет-ринок наркотиків став стійким, контролювати його досить складно.

У мережі поширюється інформація про місця збуту наркотичних засобів, надаються рекомендації по вирощуванню коноплі в закритих умовах, рекламуються послуги по доставці посівного матеріалу. Незаконний обіг наркотиків в мережі Інтернет включає не тільки продаж заборонених препаратів, а також і незаконну торгівлю лікарськими засобами, що містять у собі наркотичні засоби та психотропні речовини.

Дуже велику небезпеку складає той факт, що широкі можливості анонімного придбання психотропних засобів з використанням телекомунікаційних пристроїв в мережі Інтернет отримують також діти і підлітки. Підвищений інтерес наркозлочинців до мережі Інтернет проявляється у можливості збереження анонімності комунікації постачальників (збувачів).

Використання злочинцями ресурсів мережі Інтернет, електронних платіжних систем, засобів мобільного зв'язку, значно знижує для них ризик бути затриманими в момент передачі

наркотичних засобів. Як наслідок, найбільш організовані злочинні групи наркодилерів в основному переходять на так звані «безконтактні» способи збуту наркотиків. Це істотно ускладнює застосування оперативними працівниками класичних методів здійснення оперативної закупівлі, що залишається основним заходом виявлення та документування злочинів, пов'язаних з незаконним обігом наркотиків.

Безконтактний збут наркотиків організовується, як правило, в такий спосіб. На створеному злочинцями ресурсі в мережі Інтернет розміщується реклама пропонованих для реалізації наркотичних засобів (форма подачі матеріалу при цьому може бути завуальована). Тут же вказуються способи оплати «товару». Споживачеві пропонується відправити замовлення з зазначенням виду та кількості наркотику, який він бажає придбати з використанням SMS-повідомлень, ICQ, Viber, WhatsApp, електронної пошти або через ресурси соціальних мереж. При отриманні замовлення один з учасників злочинної групи, що виконує роль диспетчера Call-центру, дає відповідь покупцеві із зазначенням суми і способу оплати, яка може бути проведена через електронні платіжні системи (WebMoney, Яндекс.Деньги, QIWI.), або шляхом пересилання кодів карт оплати послуг мобільного зв'язку. Після здійснення платіжної транзакції покупцеві надсилається повідомлення з зазначенням місця знаходження тайника з наркотиками (місця закладки). В окремих випадках після оплати злочинці відправляють споживачу посилку з наркотиком звичайною поштою або кур'єрськими службами на адресу, вказану у заявці. Як вже зазначалося, відсутність безпосереднього контакту злочинців із споживачем при передачі наркотику в подібних випадках виключає застосування оперативними співробітниками добре відпрацьованих на практиці тактичних оперативно-розшукових алгоритмів встановлення учасників злочинних груп. Ускладнюють цю роботу і особливості організації та функціонування таких груп. Як правило, для них характерний чіткий розподіл ролей, серед яких можуть бути виділені:

– організатор (координатор) – здійснює загальне керівництво діями членів групи, виробництвом, придбанням, фасуванням наркотиків, розподілом заробітку, організацією функціонування мережевого інформаційного та платіжного ресурсів;

– диспетчер – отримує замовлення від покупців, контролює процес оплати, передає інформацію закладчикові і отримує від них відомості про місця схованок, повідомляє про них покупцям;

– закладчик – здійснює закладку наркотиків в тайники і повідомляє диспетчеру про їх місцезнаходження;

– касир – отримує грошові кошти, що надійшли через платіжні термінали, банківські рахунки, з карт оплати послуг мобільного зв'язку, переводить їх у готівку і розподіляє їх між рештою учасників організованої злочинної групи;

– експедитор (кур'єр) – передає раніше отримані наркотики закладчикові.

Після виявлення ресурсів, через які організовано обіг наркотичних засобів, важливо забезпечити встановлення контакту з продавцями (диспетчером), з'ясування способів зв'язку з ними і даних контактів, у тому числі номерів мобільних телефонів, електронних гаманців, банківських рахунків тощо. Важливо вжити заходів до визначення фізичного місцезнаходження пристроїв, за допомогою яких злочинцями здійснюється вихід в мережу Інтернет, а також їх MAC-адреси.

Подальші дії пов'язані із застосуванням усього комплексу оперативно-розшукових сил, засобів і методів, які підтвердили свою ефективність у протидії наркозлочинності. Одночасно з встановленням всіх учасників організованої злочинної групи повинні проводитися оперативно-розшукові заходи, які дозволять з'ясувати роль кожного з фігурантів у збуті наркотиків, а також визначити місця закладок наркотичних засобів, канали поставок, способи перетворення безготівкових коштів у готівкові, а також інші обставини, що свідчать про їх злочинну діяльність.

Тому, перш за все, для боротьби з вказаною категорією злочинів оперативні працівники повинні розумітися і володіти певними навиками в сфері інформаційних технологій з метою всебічного документування та розкриття даних кримінальних правопорушень.

Одержано 01.11.2014

УДК 00.007.5

Олександр Вікторович МІНЧЕНКО,
викладач Сумського училища професійної підготовки, підпорядкованого УМВС України в Сумській області

АКТУАЛЬНІ ПРОБЛЕМИ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ

На теперішній час у своїй злочинній діяльності кримінальні структури використовують найсучасніші досягнення науки і техніки, комп'ютерні системи та нові інформаційні технології. Тобто, відбувається процес інтенсивної інтелектуалізації

організованої злочинності. Великою проблемою на сьогоднішній день є взаємодія правоохоронних органів з суб'єктами підприємницької діяльності у протидії шахрайствам з використанням комп'ютерних технологій.

Інформаційні технології викликали появу нових умов, які використовуються криміналітетом для скоєння злочинів на національному, міжнародному і транснаціональному рівнях. Злочинні об'єднання, окремі «фахівці» кримінального бізнесу повною мірою використовують новітні технології для «відмивання» грошей, здобутих злочинним шляхом, несанкціонованого доступу до інформаційних систем.

Специфіка даного виду злочинності полягає у:

– відносній комфортності, тобто готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця»;

– доступності – у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку;

– географії скоєння злочинів, яка є досить широкою, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає «левова частка» злочинності;

– віддаленості об'єкту злочинних посягань – він може знаходитись за тисячі кілометрів від місця скоєння злочину;

– складності виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її в якості речового доказу.

Офіційна статистика не дає можливості одержати достовірні дані щодо кримінологічної характеристики злочинів, що вчинюються у сфері використання інформаційних технологій, динаміки й структури таких злочинів.

Це зумовлене рядом об'єктивних та суб'єктивних причин, до першорядних з яких відносяться:

– швидкоплинність і прихованість вчинення транскордонних злочинів з використанням інформаційних технологій;

– високий рівень оснащеності злочинців, а також залучення ними до незаконних операцій висококваліфікованих спеціалістів;

– неузгодженість процедур обміну інформацією між правоохоронними органами різних країн;

– недовіра до правоохоронних органів з боку потерпілих структур пов'язана зі страхом отримати широкий розголос фактів вдалих атак на власні комп'ютерні системи, що може призвести до втрати прибутків через зниження рівню ділової репутації;

– відсутність профільних вузів (факультетів) для підготовки спеціалістів в цій дуже специфічній галузі (фахівець з кіберзлочинності, окрім юридичної освіти та чималого досвіду організації протидії кіберзлочинам, повинен володіти спеціальними знаннями системотехніки та програмування), як результат – вкрай низький рівень підготовки правоохоронних структур по відношенню до значно вищої кваліфікації правопорушників;

– відсутність соціальної привабливості та належного фінансування праці для залучення обдарованої молоді;

– прояви нездорової конкуренції між спецпідрозділами різних відомств (нерідко СБУ передає до спецпідрозділів МВС оперативні матеріали за підвідомчістю за фактом виявлених тільки тих кіберзлочинів, які вважаються безнадійними для розкриття).

Тому, виходячи з вищевикладеного, нам потрібно прийняти певні рішення для вирішення даних проблем, а саме:

– розробити проекти постанов щодо вжиття першочергових заходів, спрямованих на зниження рівня хуліганської і кримінальної активності в Інтернет, що регламентуватиме роботу постачальників Інтернет-послуг та їх клієнтів, провайдерів і операторів IP-телефонії. А саме: запровадити практику ідентифікації користувача Інтернет шляхом надання ідентифікаційного коду особи оператору зв'язку, при подачі письмової заяви про укладення договору на надання послуг;

– розробки та введення в дію системи з попередження шахрайств в Інтернет з метою проведення інвентаризації та сертифікації сайтів компаній і фірм, основною сферою діяльності яких є торгівля та надання послуг (у тому числі сайтів з азартних ігор, лотерей, аукціонів), які проводять розрахунки між продавцем та покупцем за допомогою засобів електронного зв'язку;

– всебічно сприяти створенню у вітчизняному сегменті Інтернет-сайтів, які висвітлюють діяльність правоохоронних органів у сфері протидії кіберзлочинності;

– встановити чітку взаємодію правоохоронних органів з суб'єктами підприємницької діяльності у протидії шахрайствам з використанням комп'ютерних технологій;

– розробити інформаційну базу, щодо міжнародного співробітництва правоохоронних органів щодо протидії кіберзлочинності.

Одержано 01.11.2014

Актуальні питання діяльності правоохоронних органів
у сфері протидії кіберзлочинності. Харків, 2014

УДК 343.985.3

Сергей Владимирович ШОШИН,
кандидат юридических наук, доцент,
доцент кафедры уголовного, экологического права и криминологии
юридического факультета Саратовского государственного
университета имени Н. Г. Чернышевского

ИННОВАЦИИ В КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ В ПЕРИОД ГЛОБАЛИЗАЦИИ

Выбор конкретного поставщика и определения характеристики закупаемого в РФ оборудования, используемого для проведения оперативно-розыскных мероприятий и следственной деятельности, сегодня осуществляется без учета требований антимонопольного законодательства. Результатом подобной ситуации становится весьма значительное отличие техники и технологий, применяемых в РФ, от лучших мировых образцов, при значительном объеме финансирования данных закупок. [1, с. 310]. Не является исключением здесь и процесс расследования (и оперативного сопровождения) уголовных дел о киберпреступности.

Похожая ситуация складывается и при использовании в процессе доказывания по уголовному делу информации, полученной при контроле телефонных и иных переговоров. Особую актуальность сейчас представляют переговоры правонарушителей (и иных лиц), производимые с использованием технологий компьютерной видеосвязи «Скайп» (и аналогичных ей). Организовать производство судебной экспертизы по делам о киберпреступлениях (с положительным результатом), используя потенциал местных экспертных подразделений территориальных органов МВД РФ, не всегда оказывается возможным. Связано это, порой, с дефицитом соответствующих специалистов, компетентных в проведении соответствующих видов экспертных исследований. Практика российской действительности сегодня требует от кандидатов (в исполнители) на проведение таких исследований наличия ранее выданных им специальных допусков на право производства таких экспертных исследований.

Интересным может оказаться опыт Республики Болгария, накопленный в вопросе организации судебных экспертиз. Эксперт в Республике Болгария назначается органом, который назначил проведение экспертизы, по принципу случайного отбора из соответствующего списка специалистов, утвержденных в качестве экспертов. В ст. 397 Закона «О судебной власти»

Республики Болгария (в ред. от 7 августа 2007 г. с посл. изм. и доп.) предусматривается возможность назначения в качестве эксперта и специалиста, не включенного в соответствующий список. За каждым судебным районом окружной и административный суды (в Республике Болгария) составляют, как предписывается ст. 398 Закона Республики Болгария «О судебной власти», списки специалистов, утвержденных экспертами. Верховный кассационный суд, Верховный административный суд, Верховная кассационная прокуратура, Верховная административная прокуратура и Национальная следственная служба (в Республике Болгария) при необходимости утверждают отдельные списки для нужд своей деятельности. Когда возникает необходимость, соответствующий орган судебной власти в Республике Болгария может назначить проведение экспертизы со списков специалистов других районов. Списки экспертов в Республике Болгария являются публичными [2, с. 228].

Важно рекомендовать рассмотреть возможность сертифицировать услуги по проведению судебных экспертиз в соответствии с ИСО 9001:2000 с учетом требований международного рынка услуг.

Важно законодательно закрепить обязательность проведения страхования ответственности лиц, производящих судебную экспертизу. При определении конкретных исполнителей государственных услуг в сфере подобного страхования, востребованной должна оказаться конкуренция.

Конкуренция необходима также в деятельности по: 1) изменению внешности и перемена места жительства (в рамках процесса защиты свидетелей и т. п. лиц); 2) определению конкретного переводчика иностранного языка. Это в полной мере справедливо и для перевода языка глухонемых; 3) определению конкретного исполнителя ревизии или аудиторской проверки; 4) обеспечению безопасности тайны следствия (технические мероприятия по обеспечению информационной безопасности, как то: установка средств физической защиты информации, надлежащего программного обеспечения, надлежащей компьютерной техники и средств связи и т. д.).

Экономическое господство одних хозяйствующих субъектов над другими возможно (в цивилизованном рыночном хозяйстве) лишь на основе открытой и максимально возможной конкурентной борьбы. К участию в процессе такой борьбы надлежит допускать субъектов предпринимательской деятельности из разных стран мира. Процесс глобализации способен дать импульс для продвижения вперед и (российскому) национальному законодательству, и (российской) правоприменительной практике.

Список использованных источников:

1. Шошин С. В. Инновации и дактилоскопия / С. В. Шошин // Роль кафедры криминалистики юридического факультета МГУ имени М. В. Ломоносова в развитии криминалистической науки и практики : материалы конф. (Москва, 18–19 окт. 2010 г.) / МГУ им. М. В. Ломоносова. – Т. 1. – М. : МАКС-Пресс, 2010. – С. 310–312.

2. Репешко П. И. Судебная экспертиза в уголовном процессе Республики Болгария [Электронный ресурс] / П. И. Репешко // Теорія та практика судової експертизи і криміналістики. – Вип. 10. – 2010. – С. 223–231. – Режим доступа: http://www.hniise.gov.ua/user_files/File/sbornik/2010/Repeshko.pdf.

Одержано 01.11.2014

УДК 347.78(477)

Олександр Олександрович ЗАГУМЕННИЙ,
слухач магістратури
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ОСІБ, ЯКІ ВЧИНЯЮТЬ КІБЕРЗЛОЧИНИ

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютерізації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Осіб, які вчиняють комп'ютерні злочини (кіберзлочини), у криміналістичній літературі поділяють на декілька категорій. Так, М. С. Полєвой та В. В. Крилов виокремлюють такі типи:

– порушники правил користування ЕОМ (несанкціоноване використання комп'ютерів, поширення вірусів і т. п.);

– «білокомірцеві» злочинці;

– «комп'ютерні шпигуни» – підготовлені професіонали, метою яких є отримання важливих стратегічних даних про супротивника в економічній, політичній, технічній та інших сферах;

– «хакери» («одержимі програмісти») –технічно підготовлені особи, які, вчиняючи злочини, часто не переслідують при цьому прямих матеріальних вигод (для них має значення самоствердження, помста за образу, бажання пожартувати тощо) [1, с. 234, 239].

В. Б. Вєхов виділяє такі три групи комп'ютерних злочинців:

– особи, особливістю яких є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості;

– особи, які страждають на новий вид психічних захворювань – інформаційні хвороби (комп'ютерні фобії);

– професійні комп'ютерні злочинці з яскраво вираженою корисливою метою [2, с. 38–39].

В. Є. Козлов у цій класифікації уточнює назву другої групи правопорушників, пропонуючи іменувати їх особами, які страждають на новий різновид психічної неповноцінності – інформаційні хвороби чи комп'ютерні фобії [3, с. 162; 4 с. 54–55].

За наявності подібних фактів у процесі розслідування призначають судово-психіатричну експертизу на предмет установлення осудності злочинця на час учинення ним злочинних дій.

Сучасний рівень технологій сприяє тому, що хакери спеціалізувалися у окремих напрямах. Така спеціалізація дає можливість виділити в загальній масі хакерів «групи за інтересами», наприклад «крекеров» (cracker) – спеціалістів по обминанню механізмів безпеки; «кранчеров» (cruncher) – спеціалістів по знаттю з програмного забезпечення захисту від копіювання; «крешеров» (cruncher) – любителі активно експериментувати з комп'ютерною системою з метою дослідження можливостей управління нею.

В залежності від предмету діяльності, хакерів можна поділити на три групи:

Software hackers, чи софтверні хакери, займаються тим, що «зламують» програмне забезпечення. Це навіть сам багато численна група хакерів, і шкода від діяльності цих людей вимірюється мільйонами доларів.

Phreks, по визначенню фрікер – це особа, що надає перевагу «альтернативним» способам оплати теле- та інших комунікаційних послуг (наприклад, заставить заплати за телефон сусіда замість себе, якщо на телефоні стоїть блокіратор). В останній час серед фрікерів з'явився новий прошарок – carders. Кардери – це особи, які перепраграмовують телефонні картки таким чином, що на карті відкривається практично безмежний кредит на телефонні розмови. Це, мабуть, найбільш небезпечна частина фрікерів. Вони мають глибокі знання у галузі радіоелектроніки та програмування мікросхем. Оскільки кардери потенційно можуть принести велику шкоду, за їх діями уважно слідкують спеціальні служби.

Net hacers –ця група осіб відділилася від фрікерів, коли почали активно розвиватися технології у мережах. Мережевий хакер повинен дуже добре розбиратися у мережах зв'язку та способах їх захисту. Мережеві хакери зламують захист серверів Інтернет, атакують державні та корпоративні інформаційні системи. Мета атак може бути різною, навіть до промислового шпіонажу за замовленням конкуруючих кампаній.

Найбільш численна категорія це зломщики програмного забезпечення. Основними видами діяльності яких є: зняття захисту з комерційних версій програмних продуктів, виготовлення реєстраційних ключів для умовно-безкоштовних програм тощо.

До найбільш небезпечної категорії хакерів слід віднести розробників комп'ютерних вірусів. Постраждати від їх діяльності може будь-який користувач комп'ютерних систем. Розповсюджують віруси різноманітними способами. В останні роки частіше за все розповсюдження проходить через електронну пошту.

Список використаних джерел:

1. Компьютерные технологии в юридической деятельности / под ред.: В. В. Крылов, Н. С. Полевой. – М. : БЕК, 1994. – 304 с.

2. Вехов В. Б. Компьютерные преступления. Способы совершения, методики расследования / В. Б. Вехов. – М. : Право и закон, 1996. – 182 с.

3. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М. : Горячая линия – Телеком, 2002. – 336 с.

4. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін.]. – Київ : Аванпост-Прим, 2010. – 245 с.

5. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів / Хахановський Валерій Георгійович // Юридичний часопис Національної академії внутрішніх справ. – 2011. – № 1 (1) [Електронний ресурс]. – Режим доступу: http://www.naiau.kiev.ua/chasopis/materials/24#1.

Одержано 03.11.2014

УДК 343.1(477)

Сергій Вікторович ДЖЕВАГА,
ад'юнкт докторантури та ад'юнктури
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ОРГАНАМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Стрімкий розвиток інформаційних технологій на початку XXI століття суттєво вплинув на всі сфери суспільних відносин, надав людині швидкий доступ до світових баз даних, у тому числі до електронних платіжних систем, що також відкриває для зловмисників можливість вчиняти транснаціональні злочини через наявність прогалин у законодавстві про інформаційну безпеку, неналежному контролю за втручанням ззовні та всередині мережі в інформаційну систему, недостатню технологічну та програмну обізнаність, а також у значній кількості випадків легковажної довірливості до зловмисників.

Першим кроком у міжнародній протидії швидко зростаючий загрозі в кібернетичному просторі стало прийняття Радою Європи «Конвенції про кіберзлочинність» від 23 листопада 2001 р. (ратифікований Верховною Радою України із застереженнями і заявами 07.09.2005). Дана конвенція рекомендувала уніфікувати національне кримінальне законодавство з питань комп'ютерних правопорушень та передбачити відповідальність за такі злочини: незаконний доступ; нелегальне перехоплення; втручання в банк даних; втручання в систему; зловживання пристроями; підроблення, пов'язане з комп'ютерами; шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язане з порушенням авторських та суміжних прав. Також прийнято Радою Європи «Додатковий протокол до Конвенції про кіберзлочинність» від 28.01.2003 (ратифікований Верховною Радою України із застереженням від 21.07.2006), який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи.

Генезис протидії ОВС кіберзлочинності починається з 1993 року шляхом створення у структурі управління МВС Державної служби боротьби з економічною злочинністю відділу по лінії захисту інтелектуальної власності. На нашу думку, це пов'язано з тим, що кіберзлочинність дуже негативно впливає на економічний розвиток у сфері інтелектуальної власності та на інші суспільні відносини. Для більш дієвого подолання цього негативного явища у квітні 2012 року в структурі ОВС було

створено самостійний підрозділ по боротьбі з кіберзлочинністю. Проте суттєвого успіху не було досягнуто, тому що в національному законодавстві по протидії кіберзлочинності є багато прогалин, які потребують доопрацювання, тому вважаємо доцільним на законодавчому рівні передбачити повноваження правоохоронному підрозділу оперативно блокувати web-сайти, які розповсюджують шкідливу та піратську інформацію, шляхом внесення до державного реєстру заборонених web-сайтів (створений на законодавчому рівні); зобов'язати провайдерів Інтернету реєструвати персональні дані своїх користувачів в інформаційній базі даних ОВС; зобов'язати адміністраторів комерційних ресурсів перевіряти інформацію про продавця, шляхом порівняння місцезнаходження IP-адреси продавця та місця продажу товару в оголошенні (наприклад, якщо товар продається в м. Харкові, а IP-адреса продавця указує на інше місто або країну), також блокувати оголошення надані через FreeWi-Fi мережі не комерційного користування, зберігати інформацію про оголошення й домовленість між продавцем та покупцем мінімальним строком 6 місяців, та про всі підозрілі оголошення повідомляти ОВС; створити державну інформаційну базу про бот-мережі за якими помічено протиправну активність, що створить можливість блокувати їм доступ до національних інформаційних мереж; встановити кримінальну відповідальність за ненадання або не в повному обсязі відповіді на запит органів досудового розслідування по кримінальному провадженню, а також встановити розумність строків відповіді в залежності від обсягу затребуваної інформації.

Чинний КПК України надає право органу досудового розслідування при здійсненні гласних та негласних (слідчих) розшукових дій залучати спеціалістів, які володіють спеціальними знаннями, що безумовно необхідно для успішного виявлення, розкриття та розслідування кримінальних правопорушень в сфері електронних інформаційних технологій. На етапі виявлення, фіксації та збору доказів органи досудового розслідування можуть залучити спеціаліста, однак конкретних вимог до стажу роботи в цій сфері та наявності посвідчення про закінчення спеціалізованих курсів законодавчо не передбачено. Це дає змогу залучити обізнану особу, яка самостійно здобула знання у цій сфері і не рідко, як показує практика, демонструє професійні навички не гірші, а в деяких випадках кращі від дипломованих спеціалістів.

Початковим етапом фіксації відомостей про протиправну діяльність, яка є у вільному доступі в мережі Інтернет – це

слідча (розшукова) дія «Огляд» (ст. 237 КПК України). Слідчий за бажанням може залучити понятих, але на нашу думку, у залученні понятих немає необхідності, тому що це зайва трата часу на дублювання отриманих даних: пошук понятих для слідчої (розшукової) дії, подальший їх допит, як свідка, та виклик до суду. Як і в матеріальному світі сліди злочину в кібернетичному просторі теж є, інформація яка знаходиться в Інтернеті зберігається значний термін часу, навіть якщо інформацію було видалено, тому є можливість отримати дублікат шляхом запиту до власника хостингового сервісу де містилась інформація, або знайти хеш-тегову інформацію в пошукових сервісах, яка є в публічному доступі.

Один з варіантів фіксації інформації, яка є в публічному доступі здійснюється шляхом скріншоту (програмному фотографуванні зображення з екрану монітору), або створенням дублікату частини або цілого web-сайту за допомогою спеціальних програм. При дублюванні даних, як містять ознаки порушення авторських та суміжних прав, шкідливий код (віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери тощо) – необхідно вказати web-адресу та зробити скріншот джерела розповсюдження, а також вказати контрольну суму файлу (значення, розраховане на основі набору даних з використанням певного алгоритму, що використовується для перевірки цілісності даних при їх передачі або збереженні) одним або декількома алгоритмами хешування: CRC32, MD5 та SHA-1.

Неприпустимо підміняти експертизу консультацією спеціаліста, хоча призначення експертизи не є обов'язковим. Залучення експерта здійснюється у вигляді постанови слідчого, прокурора, ухвали слідчого судді. Висновок експерта документально підтвердить або спростує припущення органу досудового розслідування, що ці програми є предметом, засобом або знаряддям кримінального правопорушення.

Також з нових новел чинного КПК України – є «Контроль за вчиненням злочину» (ст. 271 КПК України), що дає змогу успішно протистояти тяжким та особливо тяжким злочинам в мережі Інтернет, яка на теперішній час має міжрегіональний або міжнародний характер. Для цього необхідно слідчому звернутися до прокурора з клопотанням про проведення негласної слідчої (розшукової) дії «Контроль за вчиненням злочину» (згідно ч. 3 ст. 110 КПК України прокурор прийме рішення у формі постанови), який має 4 форми проведення: контрольована поставка; контрольована та оперативна закупка; спеціальний слідчий експеримент; імітування обстановки злочину.

Знання спеціаліста широко застосовуються у «Контролі за вчиненням злочину», тому що тільки спеціаліст може створити інформаційну пастку, простежити за діями злочинця, встановити його місцезнаходження та інше.

Таким чином, необхідно вказати на неналежний рівень протидії кіберзлочинності спеціалізованими підрозділами ОВС, що обумовлений такими факторами: невідповідність національного законодавства міжнародним стандартам у протидії кіберзлочинності; неналежне технічне оснащення правоохоронних органів та спецслужб; непередбаченість наказами МВС способу оплати послуг залученого спеціаліста. Тому доцільно побудувати дієву систему кібернетичної безпеки України шляхом чіткого визначення державної політики у цій сфері та випереджувального правового реагування на динамічні зміни, що відбуваються у кіберпросторі.

Одержано 04.11.2014

РОЗДІЛ 3
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343

Олександр Людвигович БЕРЗІНЬ,
студент інституту підготовки кадрів для органів прокуратури України Національного юридичного університету ім. Ярослава Мудрого (м. Харків);

Сергій Людвигович БЕРЗІНЬ,
студент інституту підготовки кадрів для органів прокуратури України Національного юридичного університету ім. Ярослава Мудрого (м. Харків)

СУЧАСНІ ПРОГРАМНІ ПРОДУКТИ В РОБОТІ ЮРИСТА

На сьогоднішній час вже не можливо уявити ефективну роботу юриста без застосування сучасних інформаційних технологій, адже грамотне оформлення інформаційних процесів та правильне використання наявних ресурсів є не від'ємною сферою його діяльності.

Попри те, що 97 % правників мають смартфони, використовують у робочих цілях стандартні комунікаційні програми (такі як Facebook, Viber, Skype), з яких всього 7 % представників професії працюють із мобільними версіями баз законодавства, а переважна більшість респондентів (93 %) – не користуються спеціальними мобільними додатками. Більше того, майже ніхто з них не знає про існування останніх. Про такі результати дослідження щодо ступеня проникнення інформаційних технологій на ринок правових послуг стало відомо на прес-конференції «Мобільні додатки на ринку юридичних послуг. Втрати та можливості». Потенційно можливості комп'ютера істотно підвищити ефективність роботи юриста великі. Побіжний погляд на існуючі програмні продукти для юристів дозволяє створити такий перелік категорій програм:

1) правові бази даних (довідкові правові системи, інформаційно-правові системи, інформаційно-довідкові системи та інші назви). Це бази як нормативних актів (нормативних, правових актів), так і судових рішень, консультацій різних фахівців, статей з юридичних і економічних видань, збірники ДСТУ, СНІП, СанПіН і т. д.;

2) юридичні словники;

3) програми – збірники договорів з можливістю пошуку (вибору договору), друку, збереження у файл для подальшого редагування в текстовому редакторі;

4) програми – збірники договорів з можливістю заповнення (автозаповнення) деяких полів договору, таких, як дата, номер договору, сторони договору і т. п. (тобто полів, які не є результатом складного юридичного аналізу ситуації). Іноді існує можливість заповнення предмета договору – але тільки грубого заповнення, без зв'язку інших умов договору з особливістю предмета договору і тільки піддаються на думку розробників програм автозаповнення – купівля-продаж, оренда і т. п.;

5) програми – збірники договорів з можливістю вибору (заповнення) не тільки дати, номери, але і «всіх» умов договору шляхом вибору одного варіанта з декількох по кожному умові договору;

6) ведення обліку (журналу, реєстру) складаються договорів, облік претензійно-позовної роботи (проходження, етапи даної роботи), автоматизація роботи секретарів, суддів, архіваріусів, працівників канцелярії судів, працівників органів державної реєстрації прав на нерухоме майно і т. п.;

7) невеликі програми для автоматизації деяких функцій, здійснюваних юристами (макроси з написання числа прописом, програми по розрахунку держмита, за розрахунками відсотків і т. д.);

8) облік робочого часу юристів, звітність приватнопрактикуючих юристів, адвокатів та інших юристів (суміжне з бухгалтерськими програмами);

9) експертні юридичні системи;

10) інше (наприклад, програми складання фотороботів).

Особливої уваги заслуговує розмежування сучасних інформаційно-правових систем за роботою в режимах online та offline. Відповідно до online правових пошукових систем відносять: офіційний веб-портал Верховної Ради України, правовий портал України Ліга: Закон, правову пошукову систему НАУ-online, мобільну правову систему «ip.Lex.Профі». До offline інформаційно-правових систем відносять: правову систему «ЛІГА:ЗАКОН 9.1», професійну правову систему «МЕГА-НАУ», мобільну правову систему «ip.Lex.закон», правову систему «Інфодиск: Юрист».

Отже, юрист завжди повинен бути готовий правильно і своєчасно реагувати на запити суспільства, володіти методиками і прийомами роботи з мінливим законодавством. Саме тому таким важливим є постійне вдосконалення професійних знань та умінь правознавця, в тому числі він повинен непросто орієнтуватися, але й активно застосовувати сучасні програмні продукти у своїй роботі.

Одержано 29.10.2014

УДК 343.98

Євгенія Олексіївна ГЛАДКОВА,
кандидат юридичних наук,
старший науковий співробітник науково-дослідної лабораторії
з проблем протидії злочинності
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ

Аналіз практики інформаційно-аналітичного забезпечення протидії злочинності дозволяє зробити однозначний висновок про те, що в сучасній Україні в системі правоохоронних органів використовувані організаційні підходи до налагодження та врегулювання цих відносин не є адекватними характеру і масштабам загроз національній безпеці з боку злочинності.

При цьому удосконалення цих підходів має відбуватись синхронно із позитивним розвитком самої практики протидії злочинності, впровадженням в неї новітніх підходів та засобів діяльності. Реальність, в якій відбувається протидія злочинності, характеризується різноманітністю форм прояву, тому її забезпечення також слід організовувати з урахуванням об'єктивних закономірностей відповідних процесів.

Що стосується інформаційно-аналітичного забезпечення функціонування правозастосовних механізмів ведення ефективної боротьби зі злочинністю, правоохоронними органами робиться також недостатньо, внаслідок чого їх оперативно-службова діяльність є такою, що потребує суттєвої оптимізації та підвищення результативності.

З урахуванням цього варто розглянути деякі шляхи удосконалення інформаційно-аналітичного забезпечення діяльності правоохоронних органів через призму специфіки сучасного стану функціонування правоохоронної системи.

Перш за все, варто звернути увагу на те, що чимало проблем із реалізацією механізмів інформаційно-аналітичного забезпечення спричинено недосконалістю розробки відповідних питань у нормативно-правових актах, а також відвертою декларативністю окремих їх положень. Так, наприклад, Указ Президента України «Про єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю» хоча і є, на перший погляд, актуальним та доцільним, втім, породжує більше питань, ніж пропонує відповідей на них.

Про необхідність створення єдиної інформаційної мережі правоохоронних органів говорять вже принаймні років двадцять, саме з того моменту, коли стало зрозуміло, які переваги має машинна обробка, систематизація та накопичення інформації у порівнянні з ручними їх аналогами. При цьому якихось більш-менш вдалих ідей відверто бракує, пропозиції та рекомендації, які маємо, є занадто узагальненими та позбавлені прикладного змісту.

У повній мірі це стосується і аналізованого рішення. З його змісту аж ніяк не можна зрозуміти, яку саме ідею покладено в основу створення єдиної комп'ютерної інформаційної системи. Якщо мається на увазі комплексне забезпечення правоохоронної діяльності, то намагання її реалізувати за всіма напрямками одночасно остаточно поховає усі подальші спроби. Вважаємо, що мету треба визначити конкретно, тим самим окреслюючи коло відносин, які підлягають упорядкуванню (наприклад, інформаційне забезпечення розкриття, розслідування та запобігання злочинів).

Є певні сумніви і щодо доцільності створення Міжвідомчої координаційної групи, адже досвід організації та функціонування подібних утворень з очевидністю свідчить про те, що зиск від їх роботи часто настільки мізерний, що мінімізує будь-які здобутки. При цьому більш ефективними є організаційні форми розробки та прийняття рішень, пов'язані з діяльністю конкретної структурної системи протидії злочинності. Тим більше, що з тексту Указу логічно випливає, що відповідна робота має проводитись під егідою та керуванням апарату Ради національної безпеки і оборони України.

Далі хотілось би висловити низку власних думок з приводу якісного удосконалення відповідних механізмів створення інформаційної системи правоохоронних органів з питань боротьби зі злочинністю.

Майже ні в кого не викликає сумнівів той факт, що існуюча система реєстрації оперативно-розшукової та слідчої інформації, особливо в правоохоронних органах України, фактично мало пристосована і неефективна для використання в розкритті, розслідуванні та запобіганні злочинам. Проте, проблема одержання об'єктивної інформації на всіх стадіях протидії злочинності є однією з найбільш значимих і актуальних. Її характер і види можуть змінюватись залежно від динаміки розвитку криміногенної ситуації та моделювання обставин вчиненого злочину. Однак непорушним і беззаперечним при цьому завжди є один із критеріїв її добору – зв'язок із подією злочину.

Якщо розглядати цю вимогу змістовно, вона виявляється набагато ширшою, адже її всеосяжний характер з точки зору забезпечення умов для вирішення завдань кримінального провадження в рамках вимог КПК України, має вихід і на дослідження всіх обставин справи, виявлення причин і умов, що сприяють вчиненню злочину, з метою їх усунення.

Якщо абстрагуватися від конкретних географічних координат і діючих осіб, то модель механізму протидії злочинності в ідеалі повинна виглядати в такий спосіб (на прикладі торгівлі людьми). Правоохоронні органи мають справу із серією вчинених злочинних актів, що мають подібність до системної діяльності. Є також певна група осіб, яка обґрунтовано підозрюється у вченні цих злочинів. На початковому етапі завданням є протиставити їх діям деяку систему заходів у рамках єдиного оперативного задуму. Це необхідно для того, щоб у процесі реалізації окремих заходів мати можливість вчасно виявити, попередити і припинити окремі злочинні дії. Одночасно при цьому повинні бути вирішені питання документування злочинної діяльності, тобто забезпечення в наступному її розкриття та розслідування.

Це обумовлює об'єктивну потребу створення відповідного Центру при РНБО України, що здійснюватиме функції стратегічного аналізу інформації. Подібна структура могла б одночасно відігравати роль основного довідково-інформаційного концентратора і координувати роботу всіх правоохоронних та інших органів України в напрямку організаційного, методичного та інформаційного забезпечення боротьби зі злочинністю, здійснюючи при цьому:

– підготовку узагальненої інформації з окремих напрямків оперативно-розшукової діяльності з одночасною розробкою рекомендацій з її удосконалення на основі аналізу і прогнозів розвитку оперативної обстановки по лініях роботи;

– підготовку необхідної бази для створення надійних оперативних позицій на основі оцінки й аналізу архівних та інших матеріалів за весь період розробки кримінального середовища, інших документів (до початку стадії активної протидії);

– контроль, координацію і надання практичної допомоги по інформаційному забезпеченню територіальних органів;

– взаємодію в рамках інформаційного обміну з аналогічними структурами правоохоронних органів країн СНД, інших іноземних держав з питань забезпечення розшуку і затримання осіб, причетних до вчинення злочинів з ознаками організованої злочинної діяльності;

– розробку заходів і пропозицій, спрямованих на оптимізацію тактики боротьби зі злочинністю, встановленню міжнародних зв'язків між фігурантами, що мешкають в державах ближнього і далекого зарубіжжя;

– організацію заходів щодо інформаційного обміну з іншими суб'єктами оперативно-розшукової діяльності з питань, що становлять взаємний оперативний інтерес;

– організацію заходів щодо впізнання з використанням створеної картотеки на основі фото-, кіно-, відеоматеріалів, в тому числі наданих Інтерполом, осіб, причетних до вчинення злочинів;

– розробку ідеології заходів щодо психологічної протидії пропагандистським акціям привабливості життя на межі закону, а також підготовку й оцінку матеріалів і документів про протиправні дії для використання у ЗМІ.

Вважаємо, що для вирішення цих та інших завдань в структурі Центру необхідно створити потужну інформаційну службу, яка обслуговуватиме спільні банки даних правоохоронних органів, з використанням автоматизованих систем обробки інформації та єдиних класифікаційних ознак. Ці банки можуть бути сформовано через комп'ютерну мережу за спеціальними кодами та відповідними допусками до різних обсягів інформації, з обов'язковим використанням аналогічної інформації Інтерполу, Європолу, координаційних бюро СНД тощо.

Природно, що для проведення цих робіт необхідний деякий статистичний мінімум, формування якого слід здійснювати на основі єдиних критеріїв добору інформації. Технічно це могло б виглядати як закріплення у відомчих нормативних актах обов'язкової для всіх осіб, що здійснюють боротьбу зі злочинністю, статистичної картки на подію злочину з інтегрованими в неї системними блоками різних відомостей, які підлягають встановленню. Облік і обробка карток повинні здійснюватися централізовано, а заповнюватись – по кожному зафіксованому факту (а не тільки по розпочатому провадженню). У плані вирішення проблеми збору і концентрації подібного роду інформації цілком можливою до застосування представляється й інша схема наповнення банків даних по принципу заповнення так званих опитувальних аркушів, які містять типовий перелік запитань, з наступною їх обробкою на ПЕОМ.

Таким чином, маємо всі підстави зробити висновок про необхідність зміни підходів до інформаційно-аналітичного забезпечення боротьби зі злочинністю. Воно не повинно бути епізодичним, як форма реагування на нові відомчі настанови.

В організаційному плані варто вести мову про деяке зміщення акцентів убік оперативних обліків на відміну від інформації, отриманої процесуальним шляхом.

Одержано 17.10.2014

УДК 004.056

Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ;

Олексій Павлович МАКАРЕНКО,
інженер-електронік відділення комп'ютерних мереж та експлуатації комп'ютерів інформаційно-технічного відділу Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ОЦІНКИ БЕЗПЕКИ ПРОГРАМНИХ ЗАСОБІВ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ПРАВООХОРОННИХ ОРГАНАХ

У сьогоденні проблема безпеки програмного забезпечення (ПЗ) і створених на його основі інформаційних систем (ІС) в правоохоронних органах повстає як ніколи актуально. Мережеві додатки є в даний час об'єктом численних атак кіберзлочинців для отримання інформації обмеженого доступу. Типи заходів щодо захисту цих додатків і їх число зростає пропорційно до зростання кількості і рівня небезпечності кібератак. Особи, відповідальні за безпеку своїх інформаційних середовищ, повинні розуміти, що ризики присутні в будь яких програмних засобах. Кожна вразливість має пов'язану критичність, яка заснована на різних факторах. Озброївшись цими знаннями, відповідна стратегія управління ризиками може бути розроблена з урахуванням пріоритетів дій по скороченню цих загроз.

По вимогах безпеки ПЗ й ІС перевіряються з метою контролю функціональної відповідності, захисту від несанкціонованого доступу, виявлення недекларованих можливостей (НДМ), що реалізують події, небезпечні з погляду збереження інформації в недоторканості. Перевірки можуть здійснюватися як незалежними представниками замовника або самого розроблювача в процесі розробки й виробництва ПЗ, так і експертами іспитових лабораторій або атестаційних комісій на випробуваннях ПЗ й ІС [1].

Які види загроз безпеки слід розглядати в першу чергу?

Корисною відправною точкою відліку є ознайомлення з описами вразливостей, що підтримуються спільнотою OWASP

(Open Web Application Security Project). Там можна знайти сотні статей, що визначають недоліки безпеки загального застосування. OWASP також підтримує Топ-10 [2] з найкритичніших вразливостей мережевих додатків. Хоча список OWASP Топ 10 є дуже корисним документом для підвищення обізнаності безпеки, як і більшість списків такого роду, він не є ні вичерпним, ні достатнім визначенням безпеки додатків.

Прийоми виявлення вразливостей:

1. Ручний (експертний аналіз)
2. Статичний аналіз безпеки (по шаблону)
3. Динамічний аналіз безпеки

При ручному підході виявлення вразливостей застосовується експертний аналіз, тобто фахівець, що проводить дане дослідження, покладається на свої знання й досвід. Даний підхід не має на увазі використання, яких або автоматизованих засобів. Зрозуміло, що даний прийом має більші витрати за часом і припускає наявність фахівців високої кваліфікації. Даний підхід уважається найефективнішим з погляду точності й повноти покриття перевірок.

Прийом виявлення вразливостей «по шаблону» має на увазі використання матеріалів і наробітків отриманих виходячи з досвіду роботи в даній області. При підході виявлення вразливостей «по шаблону» часто застосовується автоматизований підхід пошуку вразливостей по заданих шаблонах (спискам потенційно небезпечних сигнатур). Часто при даному підході використається сполучення методів автоматизованого й ручного пошуку вразливостей. Використаються засоби автоматизованого пошуку вразливостей коду PREfix, FlawFinder, RATS, UCA, ITS4, AK-BC і інші. Крім того постає проблема пов'язана з тим, де саме взяти ці списки (бази) потенційно небезпечних сигнатур. На даний момент зложилася така практика, що кожна іспитова лабораторія або навіть окремий департамент тестування використають свої власні бази сигнатур. Природно це приводить до частих розбіжностей. Тому виникає необхідність створення стандарту, у якому будуть наведені списки потенційно небезпечних сигнатур. Можна скористатися позитивною практикою вже існуючої в міжнародних проектах CWE, або відомим ресурсом для Web-додатків OWASP. Тим не менш, основним обмеженням цих автоматизованих інструментів є те, що в даний час вони можуть знайти тільки приблизно 50–80 % від типів вразливостей, які повинні бути оцінені, щоб забезпечити повне уявлення про ризики.

Динамічний аналіз є обов'язковим підходом при виявленні вразливостей. Він дозволяє проводити тестування при

безпосереднім виконанні програмного виробу. У процесі динамічного тестування програмного комплексу реалізується складений список тестів, спрямований на досягнення, або провал порушення функцій безпеки продукту. Таким чином визначається можливість або неможливість експлуатувати знайдену потенційно небезпечну сигнатуру в рамках працюючого програмного продукту, при заданому тестовому оточенні.

Існує ряд підходів до оцінки безпеки програм з використанням різних комбінацій автоматизованих і ручних методів аналізу із зовнішньої (чорний ящик) і внутрішньої (білий ящик) точки зору. Комбінований підхід дозволяє більш ретельно перевіряти можливі вразливості і точніше оцінити безпеку ПЗ.

Хоча потрібно розуміти, що будь-які засоби автоматизації є лише допоміжними інструментами для експерта, що проводить тестування. Головні виводи про наявність вразливостей у програмному продукті робить експерт, що проводить тестування по вимогах безпеки. Так само встає важливе питання про необхідність створення стандарту тестування по вимогах безпеки, у якому будуть наведені списки (бази) потенційно небезпечних сигнатур, які є найбільш актуальними для правоохоронних органів.

Список використаних джерел:

1. Performance Testing Microsoft .NET Web Application [Електронний ресурс]/ Microsoft Application Consulting and Engineering (ACI) Team. – Microsoft Press, 2003. – Режим доступу: http://www.avaxhm.com/ebooks/mspress_performance_testing_microsoft_net_web_app.html.

2. OWASP Top 10 [for 2014] [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Одержано 28.10.2014

УДК 004.942

Алексей Феликсович ЛАНОВОЙ,
кандидат технических наук, доцент,
доцент кафедры программной инженерии
Харьковского национального университета радиоэлектроники

ИСПОЛЬЗОВАНИЕ ЯЗЫКА ОПИСАНИЯ МОДЕЛИ ПРЕДМЕТНОЙ ОБЛАСТИ ПРИ ИССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Компьютерные преступления – это преступления, основным объектом посягательства которых является конфиденциальность, целостность, доступность и безопасное функционирование компьютерных данных и систем. Остальные киберпреступления, помимо компьютерных систем, посягают

на другие объекты (в качестве основных): безопасность общества и человека (кибертерроризм), имущество и имущественные права (кражи, мошенничества, совершенные посредством компьютерных систем или в киберпространстве), авторские права (плагиат и пиратство) [1]. Основной проблемой при расследовании и противодействии киберпреступности является фиксация самого факта совершения противоправного деяния, которое может быть классифицировано как киберпреступление. Одним из методов проведения таких исследований является моделирование.

Модель – это материальное, концептуальное или математическое представление системы, процесса с определенными правилами, которые позволяют управлять их взаимодействиями. Агентная модель представляет реальный мир в виде многих активных подсистем – агентов, которые образуют внешнюю среду и в процессе функционирования могут изменять как саму внешнюю среду, так и свое поведение. Для облегчения процесса построения модели введем общий синтаксис описания элементов:

объект – сущность, обладающая набором Атрибутов, необходимых для описания элементов модели;

атрибуты – задают основные и дополнительные существенные свойства Объекта, которые позволяют описать, как Объекты взаимодействуют между собой в среде моделирования.

Определим базовые примитивы в терминах предметной области Компьютерная сеть (Network) [2; 3], в рамках которой целесообразно рассматривать проблему киберпреступлений.

Узел (Node) – это физическое устройство, подсоединенное в сеть и функционирующее на соответствующем уровне модели OSI.

Сеть (Network) – это коммуникационный путь между Узлами, который позволяет производить информационный обмен на 1–3 уровне модели OSI.

ПО (Software) – операционные системы, утилиты, приложения или сервисы.

Объект (Artifact) – файл (текстовый, графический или любого другого вида) или учетные данные (аккаунт, имя пользователя, пароль или ключ).

Система ограничений (Constraint) – ограничения, накладываемые на модель, предметную область и действия агента.

Цель (Objective) – относительные цели моделирования.

Агент (Actor) – человек, участвующий в моделировании, и оказывающий влияние на поведение модели.

Процесс (Process) – активное взаимодействие между заранее определенными элементами модели, вызывающее изменение всей модели или ее отдельных элементов.

Сообщение (Message) – передача информации, данных или инструкций между элементами модели.

Объекты в модели могут быть представлены в виде иерархического набора основных и дополнительных атрибутов, например:

Уникальный идентификатор объекта (OID): Обозначение;

Тип объекта (OT): Узел (Node);

Основные атрибуты: Имя (Name, N), Флаг узел/шлюз (Host / Gateway, H/G), Операционная система (OS), Адрес Узла (Internet Address, IA), Адрес(а) интерфейсов (Local Address, LA), Таблица маршрутизации (Routing Table, RT), Таблица ARP (ARP Table, AT), Открытые порты (Listening Ports, LS);

Дополнительные атрибуты: Аккаунты (Accounts, AC), Приложения (Applications, AP), Объекты (Artifacts, AF), Сервисы (Services, S).

Моделирование процесса атаки на информационную систему осуществляется на основе Сценария. Сценарий – это логическая конструкция, которая описывает предметную область и объекты моделирования в терминах нотации. В качестве примера рассмотрим следующий сценарий:

«Необходимо провести исследование безопасности узла с сетевым адресом 10.0.10.0/24. Время моделирования – 1 час».

Исходя из анализа постановки задачи, выполним декомпозицию сценария:

Описание объекта моделирования: представлено на описательном уровне.

Узлы объекта моделирования: Атакующая и атакуемая платформы. Представляются в виде взаимодействующих между собой агентов.

Сеть: коммуникационный путь (или пути) между платформами агентов с использованием существующей сети 10.0.10.0/24.

Агенты: Один атакуемый и не менее одного атакующего.

Ограничения: 1 час модельного времени.

Цель: Идентифицировать атаку на открытые порты.

Предложенный метод формирования модели на основе формализованного языка описания модели позволит упростить процесс ее создания, повысить степень адекватности реальным ситуациям, а в целом – позволит более эффективно организовать противодействие киберпреступности во всех ее проявлениях.

Список использованных источников:

1. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы [Электронный ресурс] / Тропина Татьяна Львовна. – Владивосток, 2007. – Режим доступа: http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1. – 15.09.2009.

2. EDURange: A Cybersecurity Competition Platform to Enhance Undergraduate Security Analysis Skills / The Evergreen State College Olympia, Washington [Электронный ресурс]. – Режим доступа: http://blogs.evergreen.edu/edurange/.

3. Kim A. C. A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals [Электронный ресурс] / A. C. Kim, W. H. Park and D. H. Lee // International Journal of Network Security. Vol. 7, no. 1. – 2013. – P. 181–188. – Режим доступа: http://www.sersc.org/journals/IJSIA/vol7_no1_2013/17.pdf.

Одержано 16.10.2014

УДК 343

Александр Николаевич ЛЕПЁХИН,
кандидат юридических наук, доцент
начальник кафедры правовой информатики
Академии МВД Республики Беларусь (г. Минск)

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Современные реалии борьбы с преступлениями в сфере информационных технологий свидетельствуют о необходимости расширения профессионального инструментария, используемого при осуществлении данной деятельности. Одним из направлений совершенствования является использование различных технологий сбора, обработки и анализа информации, имеющей значения для раскрытия и расследования киберпреступлений, поскольку содержание, объем, каналы поступления информации отличаются достаточно широким спектром и все они, в той или иной мере, связаны с использованием информационных технологий. Данные факторы, способствуют более широкому внедрению систем автоматизированного сбора и обработки информации.

Традиционно, в качестве основных средств аналитической деятельности рассматриваются соответствующие аппаратно-программные комплексы и различные технические устройства, с помощью которых осуществляется обработка оперативно-розыскных и иных сведений фактографического и криминалистического характера с наиболее высоким качеством

конечных результатов. При этом задачами любой информационно-аналитической системы являются эффективное хранение, обработка и анализ данных. Эффективное хранение информации достигается наличием в составе информационно-аналитической системы целого ряда источников данных. Обработка и объединение информации достигается применением инструментов извлечения, преобразования и загрузки данных. Анализ данных осуществляется при помощи современных инструментов специализированного анализа данных.

С увеличением объема производимой и обрабатываемой информации проблема анализа исходной информации для принятия управленческих решений оказалась настолько серьезной, что началась разработка и внедрение в различные сферы нового вида информационных систем – информационно-аналитических систем (ИАС), под которыми понимают комплекс аппаратных, программных средств, информационных ресурсов, методик, которые используются для обеспечения автоматизации аналитических работ в целях обоснования принятия управленческих решений и других возможных применений [1, с. 38].

Данные в ИАС могут заноситься как вручную, так и автоматически. На этапе первоначальной фиксации данные поступают через системы сбора и обработки информации в так называемые транзакционные базы данных или операционные базы данных. Поскольку транзакционные источники данных, как правило, не согласованы друг с другом, то для анализа таких данных требуется их объединение и преобразование. Поэтому на следующем этапе решается задача консолидации данных, их преобразования и очистки, в результате чего данные поступают в так называемые аналитические базы данных. Аналитические базы данных, например, хранилища данных или витрины данных, и есть те основные источники, из которых аналитик черпает информацию, используя соответствующие инструменты специализированного анализа.

При этом информационно-аналитическая система структурного подразделения правоохранительных органов должна обеспечивать пользователям доступ к аналитической информации, защищенной от несанкционированного использования. Таким образом, архитектура информационно-аналитической системы насчитывает следующие уровни:

– сбор и первичная обработка данных;
– извлечение, преобразование и загрузка данных;
– хранение данных;
– представление данных в витринах данных;

– анализ данных;
– Web-портал.

Эффективность работы правоохранительных органов по противодействию компьютерной преступности в значительной степени зависит от системы информационного обеспечения, которая осуществляет весомую поддержку органам внутренних дел в предупреждении, раскрытии и расследовании преступлений, предоставляя статистическую, аналитическую и справочную информацию, а также определяется внедрением инновационных методов, форм и технологий, которые позволят использовать ранее недоступные схемы сбора информации. Информационное обеспечение процессов раскрытия и расследования преступлений, а иногда и их выявления, рассматривается ныне в качестве основного фактора повышения эффективности оперативно-служебной деятельности органов внутренних дел [2, с. 4].

Одним из программных средств обработки и анализа различной информации является пакет I2 Analyst's Notebook [3], который служит для графической презентации информации об объектах и связях между ними в форме диаграмм, а также, для анализа собранной информации. В зависимости от характера информации, объекты представляются на диаграмме в виде картинки, а также в виде других символов, таких как линии тем, рамки событий, прямоугольники, круги, текстовые блоки, объекты OLE. Analist's Notebook выполняет интеграционную функцию для данных, происходящих из разных источников. В случае других внешних источников, данные берутся и визуализируются на диаграмме посредством интерфейсов, соединяющих Analyst's Notebook с базами данных пользователя или через непосредственный импорт данных и автоматическую переработку их на объекты и связи. Соединяющие интерфейсы, делают доступной часть функциональности, соответствующих им баз данных, уровня Analyst's Notebook. Механизм непосредственного импорта из внешних источников, основан на загрузке файла, который включает входные данные и переработку их на диаграмму, с использованием правил, определённых в шаблоне импорта. Входные данные могут происходить из файлов в форме TXT, CSV, TSV, XML, а также из буфера Windows. Связи между объектами представлены линиями, которые соединяют объекты. Элементы диаграммы описываются при помощи информационных карт, атрибутов и комментариев. Analyst's Notebook позволяет создавать разнообразные диаграммы, в зависимости от применяемого актуального

аналитического метода. Они делают упор на структуру сообщений между объектами или могут подчёркивать хронологию событий. Диаграммы сообщений используются для анализа связей между объектами, напр., связей между лицами, лицами и фирмами, лицами/фирмами и адресами и т. д., что позволяет понять структуру взаимных реляций. Они также помогают при анализах, касающихся движения товаров и облегчат идентификацию главных лиц, их сообщников, методы их действий или способы коммуникации. Диаграммы взаимосвязей могут также служить для представления и анализа большой совокупности данных, которые касаются, напр., телефонных разговоров, сделок на банковских счетах или движения в интернете, что позволяет идентифицировать общие элементы, группы элементов, тесно связанных между собой осуществить идентификацию посредников во взаимосвязях.

Следует отметить, что в настоящее время имеется достаточное количество различных программных продуктов по сбору, обработке и анализу информации. Вместе с тем, отметим что, несмотря на достаточно большой выбор специализированных программных продуктов информационно-аналитического назначения, типовых систем для решения широкого спектра задач, обеспечивающих одинаково эффективную работу как с документальной, так и со структурированной информацией не имеется. Поскольку возможности всех систем индивидуальны, а применяемые алгоритмы и методы обработки информации различны для схожих задач пользователей, поэтому выбор программного продукта для решения конкретных задач должен осуществляться в соответствии с поставленными перед аналитическими подразделениями целями.

Таким образом, активное внедрение специализированных программных продуктов (ИАС) для решения задач раскрытия преступлений в сфере высоких технологий позволит повысить эффективность данной деятельности, в том числе, и с использованием инициативного поиска информации в сети Интернет и ее последующей обработки с помощью указанных компьютерных программ.

Список использованных источников:

1. Белов В. С. Информационно-аналитические системы. Основы проектирования и применения : учеб. пособие / В. С. Белов ; Моск. гос. ун-т экономики, статистики и информатики. – М., 2005. – 111 с.

2. Миллер Л. Ю. Интеграционный метод в теории и практике оперативно-розыскной деятельности органов внутренних дел : монография / Л. Ю. Миллер ; под общ. ред. Г. К. Синилова. – М. : Издат. дом Шумиловой И. И., 2008. – 24 с. – (Препринт).

3. Программное обеспечение для криминального анализа «Analyst's Notebook» [Электронный ресурс] – Режим доступа: http://www.acsys.com. – Дата доступа: 27.10.2014.

Одержано 29.10.2014

УДК 65.012.8+004

Ірина Андріївна МАНЖАЙ,
викладач кафедри фінансів, обліку і аудиту
факультету права та підприємництва
Харківського економіко-правового університету

АНАЛІЗ ПАРОЛІВ ДО МЕРЕЖНИХ СЕРВІСІВ

За останні півроку в світі сталося декілька суттєвих витоків конфіденційної інформації про ідентифікаційні дані користувачів мережних ресурсів. Серед них найбільш резонансними можна назвати літні викиди баз даних до поштових сервісів Google, Yandex та Mail.Ru.

Небезпека оприлюднення таких записів має декілька складових. По-перше, це можливість одержання неавторизованого доступу до листів користувачів, що у свою чергу може призвести як до втрат матеріального та репутаційного характеру, так і до так званого «викрадення особистості».

По-друге, втрата паролю від одного ресурсу для значної частини користувачів є чреватим втратою інших ідентифікаційних даних. Це пояснюється тим, що мало хто з користувачів використовує паролі, які кардинально відрізняються один від одного, для неоднакових мережних ресурсів. Думка про те, що доведеться запам'ятовувати багато паролів та тримати їх у голові, бентежить маси та часто змушує до необдуманих вчинків із застосування одного і того самого паролю до багатьох ресурсів.

Враховуючи викладене, великі корпорації намагаються застосовувати відмінні від текстових паролів засоби автентифікації (наприклад, Google), однак ці намагання поки що не знайшли широкого розповсюдження. Відтак вразливість текстових паролів залишається однією з найбільших небезпек системи інформаційної безпеки.

Аналізуючи оприлюднені дані про імена користувачів і паролі Google, Yandex та Mail.Ru, можна побачити, що майже половина з викрадених паролів Yandex складалися з цифр, що спростило атакуючим здійснення атаки перебором. Найпопулярнішим при цьому виявився пароль «123456». Сполучення «qwe» є дуже популярним як частина паролю в усіх трьох оприлюднених базах. Для російськомовних користувачів

прогнозованим є введення російськомовних назв англійськими буквами у англійській розкладці клавіатури, наприклад, «K.,jxrf» («Любочка»).

Також, аналізуючи викладені паролі, можна побачити, що зловмисники ймовірно, підібравши один з них, автоматично включали його до бази перебору для інших у випадку застосування атаки перебору. Однак, при цьому для одержання ідентифікаційних даних, скоріш за все, використовувалися також інші види атак, як от впровадження троянських застосувань. Часовий проміжок збирання таких баз також вбачається досить тривалим.

Для захисту від подібного штибу атак найбільш вдалим видається застосування двофакторної автентифікації із прив'язкою до номеру мобільного телефону. Звичайно, що як завжди, потрібно бути вимогливим до довжини та складності паролю, не використовувати ненадійні засоби комп'ютерної техніки, застосовувати шифрування тощо. Головне при цьому у жодному разі не використовувати однакові паролі для різних мережних сервісів, адже це призведе до ланцюгової реакції втрати даних.

З іншого боку подібні вади, що допускають користувачі мережних ресурсів, можуть стати в нагоді правоохоронним органам під час попередження та розслідування злочинів, а також розшуку осіб.

Одержано 31.10.2014

УДК 65.012.8+004

Олександр Володимирович МАНЖАЙ,
кандидат юридичних наук, доцент,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Ірина Анатоліївна ОСЯТИНСЬКА,
вчитель інформатики
Харківської спеціалізованої школи з поглибленим
вивченням окремих предметів № 133 «Ліцей мистецтв»

ВИКОРИСТАННЯ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОБОТИ З МОБІЛЬНИМИ ТЕЛЕФОННИМИ ПРИСТРОЯМИ

Зі зростанням популярності мобільного зв'язку і можливостей мобільних телефонів по зберіганню та обробці інформації все більш важливим завданням для правоохоронних органів

стає аналіз вмісту мобільних телефонів тих осіб, які підозрюються у вчиненні кримінальних правопорушень. Дійсно, адже сучасний мобільний телефон – це фактично маленький комп'ютер, який об'єднує в собі багато різних функцій, серед яких:

– телефонна та адресна книги;
– щоденник зі списком зустрічей і справ;
– пристрій для обміну повідомленнями (SMS, MMS, E-mail);
– записна книжка;
– диктофон;
– фотоапарат та відеокамера;
– програвач мультимедіа

і багато інших функцій, включаючи власне здійснення та отримання дзвінків.

Усі перераховані вище дані можуть містити або орієнтуючу інформацію для правоохоронних органів, або доказову інформацію та сліди, що можуть бути проаналізовані за наявності відповідного інструментарію.

Непоодинокими є випадки, коли за допомогою аналітичної обробки даних з мобільних пристроїв вдавалося розкривати неочевидні злочини або злочини минулих років, кількість яких з кожним роком невпинно збільшується.

Слід також зауважити, що зроблені за допомогою сучасних мобільних пристроїв (наприклад, iPhone) фотографії з працюючим функціоналом GPS нерідко містять в собі інформацію про координати місця фотографування, що дозволяє в окремих випадках з'ясувати місцезнаходження шуканої особи. Більше того у практиці правоохоронних органів траплялися випадки, коли за локалізацією даних з мобільних апаратів вдавалося знаходити викрадене майно, відшукувати безвісти зниклих дітей.

Усе це дає підстави говорити про існуючу потребу більш інтенсивного використання спеціалізованого програмного забезпечення для аналізу інформації з мобільних пристроїв правоохоронними органами України.

Серед таких програм варто відзначити Mobile Phone Examiner Plus (MPE+), яка легко інтегрується з Forensic Toolkit (FTK), «Мобильный Криминалист» від розробника ЗАТ «Оксиджен Софтвер», яка дозволяє серед іншого відновлювати окремі видалені повідомлення, MOBILedit! від розробника COMPELSON Labs, криміналістичний програмний продукт XRY шведської компанії Micro Systemation.

Здебільшого названі програмні продукти використовують у своїй діяльності експертні служби, але є потреба у їх засвоєнні

не лише спеціалістами вузького профілю, але й більшістю слідчих та оперативних працівників. Це дозволить суттєво покращити стан виявлення, попередження та розслідування злочинів, що є особливо важливим у такий складний для України період.

Одержано 30.10.2014

УДК 621.397.43

Микола Володимирович МОРДВИНЦЕВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційної та економічної безпеки
навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ СТВОРЕННЯ ІТ-СИСТЕМ ВІДЕОФІКСАЦІЇ ДЛЯ РЕАЛІЗАЦІЇ ЗАВДАНЬ ПРАВООХОРОННИХ ОРГАНІВ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В КРАЇНІ

Міністерство внутрішніх справ має намір забезпечити відеокамерами всі українські блокпости навколо зони антитерористичної операції на сході країни [1].

Метою цього нововведення є відеофіксація всіх транспортних засобів, що в'їжджають / виїжджають їх зони АТО в цілях посилення контролю за переміщенням зброї, боєприпасів та інших заборонених в цивільному побуті предметів.

Ефективність застосування систем відеоспостереження підтверджується зарубіжним досвідом правоохоронної діяльності. МВС України, реалізуючи свої першочергові завдання щодо забезпечення безпеки громадян, дотримання прав людини, охорони громадського порядку виступає з ініціативою облаштування громадських місць системами відеоспостереження.

Особливе місце займає відеоспостереження в забезпеченні економічної безпеки фінансових установ.

Використання систем відеоспостереження в країнах Європейського Союзу та США значно сприяє оперативності реагування на правопорушення, швидкому встановленню осіб, які їх здійснюють, запобігання терористичним актам, пошук свідків правопорушень.

Наявність подібних систем є стримуючим чинником для правопорушника, навіть за відсутності співробітника правоохоронних органів.

На думку міліції, використання систем відеоспостереження в громадських місцях дозволить зменшити кількість правоохоронців на вулицях і при цьому зробить їх роботу більш ефективною.

В роботі пропонується спосіб відео документування за допомогою засобів відео фіксації, при цьому відбувається порівняння координат об'єкта, що має мобільний телефон або GPS навігатор із зоною спостереження відеокамери, і автоматичне об'єднання фрагментів появи об'єкта в зоні видимості в один відеозвіт [2].

В даний час є всі технічні можливості для розробки і впровадження системи автоматичного створення відеозвіту (САСВ) за допомогою IP - камер.

Пропонується створення САСВ, в результаті якої правоохоронні органи зможуть отримати фільм про діяльність об'єкту спостереження. У той же час держава отримує можливість поліпшити систему безпеки при проведенні масових заходів.

САСВ має три складових: система панорамної зйомки, система ближньої зйомки, система індивідуальної зйомки.

Система панорамної і ближньої зйомки припускає встановлення IP-камер на вулицях, майданах, в великих будівлях, стадіонах. При цьому встановлюється два види камер: ближньої і дальньої зйомки. Камери далекої зйомки документують панорамну картинку об'єкта, в який потрапить об'єкт спостереження, а камери ближньої зйомки виробляють зйомку в зоні своєї видимості на малій відстані. Останні доцільно встановлювати в приміщеннях.

Для того щоб отримати відео звіт про діяльність об'єкту спостереження правоохоронні органи замовляють цю послугу у мобільного оператора. Вказуючи номер мобільного телефону об'єкта спостереження. Мобільний оператор визначає точне положення туриста і сектор спостереження тієї чи іншої IP-камери за певною програмою записує відео фрагмент, коли турист перебуває в зоні зйомки тієї чи іншої камери. Переходячи із зони зйомки від однієї камери до іншої, комп'ютерна програма монтує ці фрагменти в один фільм. Чергування фрагментів камер ближнього спостереження з фрагментами панорамних камер створить більш повне сприйняття відвідуваного об'єкта. Перемикання на панорамну IP-камеру відбувається при виході об'єкта із зони спостереження ближньої IP-камери.

Система індивідуальної зйомки передбачає доповнення створюваного фільму-звіту фрагментами індивідуальної IP-камери. Для цього особа яка веде спостереження повинна мати IP-камеру якщо існує покриття Wi-Fi, або камеру, сполучену з мобільним телефоном по якому передавати відео потік. При цьому фрагменти індивідуальної IP-камери через засоби мобільного оператора або через Wi-Fi канали зв'язку будуть автоматично вмонтовані у фільм-звіт.

Системи відеоспостереження крім правоохоронних органів можуть бути реалізовані в найрізноманітніших сферах діяльності, пов'язаних з використанням інформаційних технологій, а саме:

– в IP-телефонії для підключення зовнішніх IP-камер;

– в соціальных мережах, для відображення відеофільмів;

– в туристичному бізнесі для створення відеозвітів.

Таким чином, проект може бути реалізовано не тільки за державні кошти, а на сам перед за кошти мобільних операторів, інвесторів пов'язаних з туризмом та IP-телефонією.

Автоматичне створення відеофільмів може бути використане для туристів, які відвідують нашу країну і місто, в тому числі вболівальників, які приїжджають на різні змагання.

Щоб залишилася пам'ять від відвідування українських міст і стадіонів туристам необхідно фотографувати своїм фотоапаратом або відеокамерою відвідувані місця. Для того, щоб сфотографуватися на тлі того чи іншого пам'ятного місця буде необхідно просити когось про цю послугу. Або створювати агентства, які повинні супроводжувати уболівальників або туристів для зйомки і створення фільмів про відвідування міст, пам'яток, стадіонів. Для п'ятдесяти тисяч уболівальників, що проездили одночасно, як це трапилося на ЄВРО-2012, таке завдання не зможе вирішити ні одне туристичне агентство. Пропонується створення САСВ, в результаті якої вболівальники та туристи зможуть отримати фільм про відвідування найбільш цікавих місць в містах України, включаючи стадіони та інші місця відпочинку.

Для того щоб отримати відео звіт про відвідування того чи іншого міста України турист замовляє цю послугу через мобільного оператора. Посилаючи зі свого телефону СМС певного змісту на певний номер мобільного оператора. Мобільний оператор визначає точне положення туриста і сектор спостереження тієї чи іншої IP-камери за певною програмою записує відео фрагмент, коли турист перебуває в зоні зйомки тієї чи іншої камери як вже було описано При вході в зону спостереження IP-камери на мобільний телефон туриста може передається СМС яка підтверджує що, він увійшов в зону видимості панорамної IP-камери або камери ближньої дії.

Система індивідуальної зйомки передбачає доповнення створюваного фільму-звіту фрагментами індивідуальної IP-камери. Для цього турист повинен придбати IP-камеру. Прикладом може служити бездротова IP-камера TrendNet TV-IP110W, що має можливість кріплення на більшості поверхонь, швидкість мережі до 54 Мб/с.

При знаходженні об'єкта в зоні видимості трьох типів камер, пріоритет віддається індивідуальної IP-камері. Необхідно відзначити, що фільм може бути змонтований, як на карті пам'яті туриста, так і на порталі інтернет-ресурсу. При цьому фільм може транслюватися прямо з сайту компанії надає ці послуги. Туристу необхідно тільки отримати пароль доступу до своїх даних і передати його тій людині, якій він дає дозвіл на перегляд цього матеріалу. Матеріал може транслюватися по скайпу в реальному масштабі часу в момент, коли відбувається подія, або бути записаний на карту пам'яті або диск за замовленням туриста.

Таким чином, їдучи з нашого міста і країни, турист отримує на згадку фільм про ті місця, які він відвідував у період перебування в ньому, змонтований автоматичним монтажером, а також можливість спілкуватися з друзями, близькими, родичами безпосередньо з того місця, де він в даний момент знаходиться.

Необхідно відзначити, що установка великої кількості панорамних камер в містах України та трансляція в інтернеті зображень пам'яток культурних об'єктів в реальному масштабі часу повинна призвести до збільшення притоку туристів в міста України. При великій кількості панорамних камер в зоні одного об'єкта його трансляція панорамними камерами може вестися за певною програмою. Така зміна фрагментів зйомки може надати велику привабливість об'єктів зйомки.

Однією з привабливих особливостей цього проекту є те, що в місті підвищується ступінь безпеки за рахунок відео спостереження в місцях великого скупчення людей [3].

У цьому масштабному проекті можуть брати участь: міська влада, мобільні оператори, виробники IP-камер, власники готелів, органи внутрішніх справ.

Висновки: удосконалення системи відеоспостереження дозволяє більш ефективно реалізовувати роботу правоохоронних органів що до забезпечення економічної безпеки.

Запровадження пропонованої системи відеоспостереження може бути реалізовано в сфері туризму, IP-телефонії, соціальних мережах з залученням коштів бізнес-інвесторів. Проект потребує узгодження дій всіх організацій, що беруть участь у проекті.

Список використаних джерел:

1. Все блокпосты вокруг зоны АТО обеспечат видеокамерами, – МВД // INSIDER [Електронний ресурс]. – Режим доступу: http://www.theinsider.ua/rus/politics/53ec86aedc383/. – 14 авг. 2014 г.

2. Патент на корисну модель № 73635. Спосіб відео документування переміщень об'єкта за допомогою системи відео фіксації / Мордвинцев М. В., Машкаров Ю. Г. – 2012. – 4 с.

3. Свидетельство на полезную модель № 36912. Система автоматизированного видеонаблюдения и распознавания объектов и ситуаций / Кан И. А. и др. – 2004.

Одержано 01.10.2014

УДК 343.98

Олег Сергійович ПАНШУТІН,
курсант факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ;

Роман Русланович САВЧЕНКО,
курсант факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ ЗА КРИМІНАЛЬНИМИ ПРОВАДЖЕННЯМИ ЩОДО КІБЕРЗЛОЧИНІВ

При проведенні досудового розслідування за кримінальними провадженнями щодо злочинів, вчинення яких пов'язане з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (злочини, що відносяться до розділу XVI КК України та інші правопорушення, що відносяться до інших розділів КК України) [1], для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання, якими володіє експерт.

Згідно із ст. 69 КПК України «експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань» [2].

Так при розслідуванні зазначених вище видів злочинів, з метою встановлення обставин вчинення злочину, проводять інженерно-технічні експертизи, а саме: комп'ютерно-технічна (комп'ютерної техніки і програмних продуктів); телекомунікаційна (телекомунікаційних систем та засобів). Порядок призначення та проведення даних експертиз регламентовано «Інструкцією про призначення та проведення судових експертиз та експертних досліджень» [3].

При проведенні зазначених вище експертиз об'єктом дослідження, як правило виступають:

– комп'ютерно-технічні засоби (системні блоки персональних комп'ютерів та серверів, ноутбуки, нетбуки, планшети тощо);

– носії комп'ютерної інформації (накопичувачі на жорстких та гнучких магнітних дисках, лазерні оптичні диски та приводи до них, флешносії тощо);

– периферійна техніка (сканери, принтери, багатофункціональні пристрої тощо);

– телекомунікаційне мережеве обладнання (комутатори, маршрутизатори, модеми тощо);

– термінали рухомого мобільного зв'язку (мобільні телефони, 3G-модеми) тощо.

Для проведення криміналістичного дослідження зазначених об'єктів експерт повинен використовувати затвердженні методики [4] та використовувати спеціальне криміналістичне обладнання та програмне забезпечення.

При цьому, криміналістичне обладнання та програмне забезпечення, що використовується для проведення експертиз, у зв'язку з тим, що об'єктами дослідження можуть бути пристрої різних типів підключення та фірм розробників (наприклад, накопичувачі на жорстких дисках типом інтерфейсу підключення IDE, SATA або SCSI; мобільні телефони на базі операційної системи Android або iOS; тощо) повинно бути багатофункціональним та мати, за можливості, програмні інструменти необхідні для проведення повного та якісного дослідження (наприклад, функцію копіювання вмісту носія інформації, відновлення видаленої інформації, контекстний пошук тощо).

Таке криміналістичне обладнання та програмні продукти можна поділи на такі основні групи:

– блокувачі запису, що гарантують випадкове невнесення змін до носія інформації, якій досліджується під час проведення експертного дослідження;

– засоби для зйому інформації з накопичувачів на жорстких магнітних дисках;

– засоби для зйому інформації з терміналів мобільного зв'язку.

На теперішній час експерти мають можливість вибирати із запропонованих фірмами-розробниками різні програмні продукти та криміналістичне обладнання. Всі вони відрізняються своїми базовими функціональними можливостями, а відповідно і ціною. Тому обрання певного програмного чи апаратного продукту є не тривіальною задачею та потребує проведення порівняння технічних характеристик цих продуктів й обрання одного з них за певними критеріями.

Список використаних джерел:

1. Кримінальний Кодекс України : закон України від 05.04.2001 № 2341-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14. – Редакція від 23.10.2014.

2. Кримінальний процесуальний Кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17. – Редакція від 22.08.2014.

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ М-ва юстиції України від 08.10.1998 № 53/5 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0705-98. – Редакція від 22.01.2013.

4. Реєстр методик проведення судових експертиз / М-во юстиції України [Електронний ресурс]. – Режим доступу: http://rmpse.minjust.gov.ua.

Одержано 29.10.2014

УДК 004.738

Віталій Анатолійович СВІТЛИЧНИЙ,
викладач кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Костянтин Едуардович ПЕТРОВ,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та захисту інформації
факультету права та масових комунікацій
Харківського національного університету внутрішніх справ

ВІД ІДЕНТИФІКАЦІЇ КОМП'ЮТЕРА ДО ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА У МЕРЕЖІ ІНТЕРНЕТ

Однією з проблем з якою стикається працівник правоохоронних органів при розслідувані злочинів, які були здійсненні через мережу Internet є визначення комп'ютера користувача мережі з якого були здійснені кримінальні дії (кіберзлочини). Погрішність ідентифікації, заснованої на IP-адресі (до недавнього часу облік був основним методом ідентифікації), складається з погрішностей передачі і погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через proxy-сервер уся підмережа, яка за ним ховається, у більшості випадків матиме єдиний IP-адрес. З іншого боку, працюючи через комутоване з'єднання, користувач при кожному підключенні отримуватиме від провайдера новий IP-адрес і т. д.

Завдання ідентифікації користувача не втрачає своєї актуальності в зв'язку постійною гонкою технологій захисту інформації і технологій неправомірного отримання доступу до інформації. Актуальність цього завдання для мережі Інтернет підвищується використанням незахищених каналів передачі даних.

Завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів таких як MAC або IP-адрес в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь на питання те ж цей пристрій або ні, але не повідомляє точний тип пристрою і спосіб його використання конкретним користувачем. Окрім ідентифікаторів, можливе використання додаткової інформації, яка затребувана у разі обробки непрямих ознак, на підставі інформації отримуваної з датчиків пристрою і в результаті роботи програмного забезпечення на пристрої. В даному випадку мається на увазі визначення типу діяльності користувача за даними глобальних систем позиціонування і гіроскопа, а також застосування методів динамічної і статичної біометрії, таких як, рисунок вен на долоні, відбиток пальця, веселкова оболонка ока, геометрія кисті руки або особи, 3D-проекція черепа, клавіатурній почерк, форма вуха, голос і будь-яка інша відмітна ознака може служити для ідентифікації людини біометричною системою.

Використовуємо поняття відбиток пристрою, стосовно інформації що залишається на серверах і інших пристроїв реєстрації, а поняття відбиток особи в пристрої до інформації що побічно характеризує людину за інформацією що залишилася у використаному їм пристрої. Прикладом відбитку пристрою служить запис в log-файлі сервера, а відбитком особи інформація про використані програми, час і тривалість використання програм, набір використаних файлів і інших ресурсів.

Особливе місце серед програмного забезпечення з точки зору завдання ідентифікації пристрою займає браузер, як програма, за допомогою якої користувач дістає доступ до більшості Internet-ресурсів. Для ідентифікації використовується інформація cookies-файлів та інформація про встановлені шрифти і плагінах. Вирішуючи задачу ідентифікації з використанням непрямих ознак, слід враховувати швидкість зміни конфігурацій апаратного і версій програмного забезпечення вживаного користувачем, а так само біологічні ритми до яких схильна людина. Динамічні біометричні ознаки людини змінюються впродовж півроку. Статичні біометричні ознаки зберігаються упродовж усього життя.

Рішення задачі ідентифікації людини і пристрою використовуватиметься при реалізації концепції «програмний агент», для визначення психофізіологічного стану людини і в завданнях з області безпеки, для створення механізмів відстежування шляху. Ідентифікація пристрою і людини є проміжними цілями. Завдяки ідентифікації пристрою можливе калібрування методів знімання інформації. Кінцевою метою ідентифікації пристрою є ідентифікація людини, отримання прямої або непрямої інформації про нього.

Початковими даними для ідентифікації пристрою і людини пропонується вважати: інформацію про пристрій, інформацію про навколишній світ, інформацію про людину. Складність формалізації початкових даних полягає в неможливості побудови вичерпної безлічі значень деяких ознак. Інформація про використання клавіатури складається з коду клавіші, часу події, типу події. Проте формалізувати ознаку, пов'язану з граматичними і орфографічними помилками що допускаються користувачем при наборі тексту, як мінімум, складно.
Інформація про пристрій складається з: списку і конфігурації використовуваного апаратного забезпечення; списку і конфігурації встановлених програм, і, якщо це можливо, часу установки програм; інформації збереженої на облаштуванні користувача у вигляді cookies-файлів, інших тимчасових файлів; відбитку файлової системи пристрою.

Під відбитком файлової системи розуміється інформація про структуру файлової системи, а не отримання математичної свертки даних у файловій системі. Особлива увага приділяється файлам старше за місяць, в яких не відбувалося змін за цей час. Вони мають достатню стабільність, щоб на деякий час стати ідентифікуючою ознакою. Для створення відбитку файлової системи пропонується використовувати інформацію про їх ім'я, місце розташування, розмір, дату створення і дату редагування.

Інформація про користувача складається з: днів тижня, часу доби використання, тривалості активності програмного забезпечення; друкарських помилках, що повторюються, словах паразитах, помилках при наборі тексту; подіях миші або клавіатури.

Кінцевою метою дослідження завдання ідентифікації людини і пристрою є побудова розпізнавача, здатного із задовільною точністю робити ідентифікацію. Особливість цього пристрою полягає в непостійному наборі вхідних значень, що повинне відбиватися на його внутрішній структурі.

Одержано 09.10.2014

УДК 65.012:34(477)

Михайло Віталійович ЦУРАНОВ,
викладач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ КОМПЛЕКСНИХ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ПРИ ВИКОРИСТАННІ ПРОГРАМНИХ ЗАСОБІВ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Однією з проблем з якою стикається працівник Останнім часом особливу роль для державних і комерційних установ відіграє ефективне використання наявних у них інформаційних ресурсів. У цьому випадку ключове значення набуває інформаційна інфраструктура організації, у якій зазвичай виокремлюють технічне, програмне та організаційне забезпечення.

У зв'язку зі складним фінансовим становищем більшість користувачів у нашій країні звикли використовувати не ліцензовані операційні системи (ОС), при цьому користувачі забувають, що за зломом стоїть істотна зміна внутрішнього коду ОС. Зміна коду тягне за собою можливість появи троянських програм вже відразу при установці ОС, виходячи з цього, ніхто не може гарантувати рівень безпеки системи та можливість її використання для кіберзлочинів.

Шляхом різного роду маніпуляцій з ОС зловмисникам нерідко вдається отримувати значні суми грошей, ухилятися від оподаткування, займатися промисловим шпигунством, знищувати програми конкурентів і т. д.

Однак, навіть використання ліцензійного програмного забезпечення (ПЗ) не дає нам можливості оцінити його ефективність і економічний ефект від його впровадження.

Для вирішення проблеми оцінки рівня захищеності ОС були розроблені численні стандарти безпеки [1–3]. Однак подальший аналіз стандартів показав, що в більшості з них модель порушника і модель загроз будується виробником ОС [4]. Такий підхід не дозволяє достовірно оцінити рівень інформаційної безпеки (ІБ). Це пояснюється тим, що розробник для підвищення рівня сертифіката навмисно становить модель з мінімальною, часто не відповідною реаліям, кількістю загроз. Тому стандарти безпеки не дають реальної кількісної оцінки ефективності засобів захисту ОС.

Більшості керівників і адміністраторів безпеки необхідна кількісна оцінка рівня безпеки ОС, найбільш повно це можна зробити використовуючи комплексні показники ефективності.

В спеціальній літературі можна зустріти наступне визначення показника ефективності – кількісна характеристика властивості ефективності системи або цілеспрямованого процесу, яка є результатом вимірювання або підрахунку [5]. Для того, щоб більш повно оцінити ефективність систем потрібно вирішувати багатокритеріальні задачі.

Під критерієм ефективності слід розуміти – правило або спосіб прийняття рішення з урахуванням ефективності системи.

Проведений аналіз загальних критеріїв ефективності інформаційних технологій показав, що найбільш корисними з соціальної точки зору для суспільства є ті інформаційні технології, які дозволяють заощадити найбільшу кількість соціального часу, вивільняючи його для інших цілей, в тому числі - для цілей розвитку суспільства [6].

В роботі [6] були виділені основні принципи проектування високоефективних технологій, а саме: концентрація ресурсів у просторі, концентрація ресурсів у часі, векторна орієнтація ресурсів.

Для оптимізації та кількісної оцінки ефективності можливих варіантів проектованих або ж вже існуючих інформаційних технологій необхідно правильно вибирати критерії їх ефективності [7].

Важливість правильного вибору цих критеріїв обумовлена необхідністю оптимізації та кількісної оцінки ефективності можливих варіантів проектованих або ж вже існуючих інформаційних технологій. Такими критеріями є функціональні та ресурсні.

При виборі ОС керівники стикаються зі значною проблемою, якій ОС віддати перевагу. Існуючі стандарти і методики оцінки якості ОС не можуть дати однозначну кількісну відповідь на це питання. Для усунення даного недоліку авторами пропонується використовувати комплексний показник ефективності ІБ ОС, який враховує різні фактори, що впливають на характеристики захищеності. Також використання комплексного показнику ефективності дозволить підвищити рівень протидії кіберзлочинам у державних та комерційних установах, шляхом зниження ризику використання заражених троянськими програмами ОС.

Список використаних джерел:

1. Общие критерии оценки защищённости информационных технологий [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Common_Criteria.

2. Международные стандарты информационной безопасности // Your Private Network = Лаборатория Сетевой Безопасности [Електронний ресурс]. – Режим доступу: http://ypn.ru/177/international-standards-of-information-technologies-security/. – 9 авг. 2009 г.

3. Шкала рейтингов международных стандартов информационной безопасности / Рейтинг. Агентство «Кредит-Рейтинг» [Електронний ресурс]. – Режим доступу: http://www.credit-rating.ua/ru/about-rating/scale/12978.

4. Слипченко О. В. Стандарты безопасности операционных систем / О. В. Слипченко, М. В. Цуранов // Системи обробки інформації. – Вип. 4 (102). – 2012. – С. 78–81.

5. Надежность и эффективность в технике : справочник : в 10 т. / ред. совет: В. С. Авдуевский (предс.) и др. – М. : Машиностроение, 1986. – Т. 1 : Методология. Организация. Терминология / под ред. А. И. Рембезы. – 224 с. : ил.

6. Проблема эффективности ресурсов информационных систем [Електронний ресурс]. – Режим доступу: http://kmt.stu.ru/mashukov/posob/htm_inf_men/g18.htm.

7. Оценка эффективности информационных систем [Електронний ресурс]. – Режим доступу: http://www.ibm.com/developerworks/ru/library/l-otcenka_efectivnosti_1/index.html.

Одержано 31.10.2014

УДК 343.915:343.346.8(477)

Вадим Миколайович БАБАКІН,
кандидат юридичних наук, доцент,
докторант Харківського університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ, ЯКІ ВЧИНЯЮТЬСЯ МОЛОДДЮ

За дослідженням, сучасні тенденції розвитку теорії та практики досудового розслідування і оперативно розшукової діяльності у сфері використання інформаційних технологій спираються на застосування технічних засобів у викритті, документуванні та розслідуванні кіберзлочинів. Багатолітній аналіз практичної діяльності слідчих і оперативних підрозділів ОВС свідчить про те, що на сучасному етапі оперативні підрозділи ОВС залишаються недостатньо оснащені науково-технічним арсеналом та на підставі цього, виникають проблеми в організації та ефективності проведення заходів щодо виявлення, попередження та припинення кримінальних правопорушень у сфері кіберзлочинності. Аналіз статистики правоохоронних органів свідчить, що близько 35-40 відсотків злочинів щорічно вчиняються з використанням сучасних телекомунікаційних, комп'ютерних і інших сучасних технологій, а у майбутньому дані показники можуть різко збільшитися. На нашу думку, одним із стратегічних напрямів у протидії кіберзлочинності є удосконалення пошуку, збирання, фіксації та моніторингу оперативної інформації з використання сучасних інформаційних технологій з використанням наявних технічних засобів оперативно-розшукової діяльності, які щорічно удосконалюються.

Масова комп'ютеризація в умовах стрімкого розвитку інформаційних технологій в Україні спостерігається збільшеенням кількості інтернет-користувачів, тому що підключення до глобальної мережі стало доступним і зручним, особливо з числа осіб молодого віку. За результатами дослідження GfK Ukraine, в яких показано, що кількість регулярних інтернет-користувачів старше 16 років в Україні зросла в I кварталі 2013 р. порівняно з IV кварталом 2012 р. на 15,1 % (на 21 % порівняно з I кварталом 2012 р.) і становила 17,34 млн осіб. За підсумками 2012 р. кількість регулярних інтернет-користувачів старше 16 років в Україні становила 15,41 млн осіб, що на 27 % більше, ніж у 2011 р. [1]. Неповнолітні та молодь все активніше освоюють комп'ютерні технології. Мотивація у цієї групи є прагнення заволодіти грошовими коштами. Одні з них спеціалізуються у кримінальному посяганні на грошові кошти шляхом несанкціонованого проникнення в комп'ютерні мережі банківських установ, інші – з використанням пластикових платіжних документів [2].

За дослідженням В. Б. Вехова, особа молодого віку, що вчинила кіберзлочин, розглядається як особистість із властивими їй соціальними, психологічними, психофізичними, етичними якостями. Саме особисті якості молодої особи і зовнішнє середовище у взаємодії послідовно визначають мотивацію прийняття рішення про об'єднання з іншими особами для спільної злочинної діяльності у сфері інформаційних технологій і виконання прийнятого рішення. У той же час, вважає більшість дослідників, при корисливих злочинах особистість «переважає» над ситуацією, а мотив формує мету. Мотив злочинної поведінки формується під впливом соціального оточення, життєвого досвіду особистості; спонукання є внутрішньою безпосередньою причиною злочинної діяльності і виражає особисте ставлення до того, на що направлена злочинна діяльність [3, с. 66]. Вказане дає підстави про те, що при організації і проведенні комплексних і цільових оперативно-профілактичних заходів та протидії кримінальних правопорушень у сфері високих інформаційних технологій, ці психологічні, психофізичні властивості, які притаманні молоді повинні враховуватися оперативними працівниками ОВС, зокрема щодо бажання кожен день удосконалювати свої знання з цих питань і в основному безкоштовно, при спілкуванні з однолітками тощо.

А. В. Соколов і О. М. Степанюк [4, с. 43] класифікують правопорушників на шукачів пригод, ідейних хакерів та комп'ютерних професіоналів. За результатами вивчення кримінальних проваджень, найчастіше до кримінальної відповідальності за вчинення правопорушень у сфері інформаційних технологій

притягувалась молодь у віці 18–35 років. За 5 останніх років кількість кіберзлочинців у віці 16–35 років зросла майже у 4 рази.

На думку С. С. Малигіна й А. Є. Чечетіна, вирішення проблем інформаційного забезпечення діяльності підрозділів ОВС, що займаються попередженням, припиненням і розслідуванням злочинів, у сучасних умовах залежить від їх технічної оснащеності і пов'язано із зростанням професійної майстерності усіх підрозділів, що беруть участь як у збиранні необхідної інформації, так і в наповненні інформаційних систем і використанні цих відомостей у вирішенні завдань оперативно-розшукової діяльності [5, с. 164]. Вважаємо, це стосується і отримання оперативної інформації оперативними підрозділами ОВС відносно неповнолітніх та молоді, які готують вчинити або вчиняють чи вчинили кримінальні правопорушення у сфері високих інформаційних технологій.

Одним з найефективніших способів протидії кіберзлочинам, які вчиняються молоддю, є використання оперативними підрозділами ОВС різноманітних методів та засобів попереджувального характеру. Таким методом є інформування населення, зокрема неповнолітніх та молодих осіб щодо притягнення до кримінальної відповідальності за вчинення правопорушень у сфері інформаційних технологій. Аналіз діяльності практичної діяльності оперативних підрозділів, свідчить про те, що, більшість неповнолітніх та осіб молодого віку під час вчинення кіберзлочинів зберігають ілюзію власної безкарності. Особливо це важливо враховувати оперативним підрозділам ОВС під час організації проведення попереджувальних заходів.

Ураховуючи стрімкі процеси розвитку інформаційних технологій, особливо важливо, щоб заходи, які вживаються правоохоронними органами з метою протидії у кіберзлочинності, були своєчасними та ефективними. Це залежить, насамперед, від наступних умов: 1) забезпечення надійного збереження інформаційної бази даних, яка використовується працівниками правоохоронних органів; 2) збирання й вилучення доказів з електронного документообігу в осіб, які підозрюються в учиненні таких злочинів; 3) отримання оперативної інформації щодо фактів і обставин учинення злочину в мережі Інтернет; 4) встановлення місцезнаходження осіб, підозрюваних у вчиненні злочинів за допомогою використання інформаційних технологій [6].

Таким чином, комплексне та ефективне використання сучасних інформаційних технологій та науково-технічних засобів дає можливість оперативним підрозділам ОВС успішно здійснювати протидію правопорушенням у сфері високих інформаційних технологій, що готуються або вчиняються у молодіжному середовищі.

Список використаних джерел:

1. Інформаційне агентство УНІАН [Електронний ресурс]. – Режим доступу: http://economics.unian.net.

2. Лук'яненко С. О. Аспекти систематизації злочинів в кредитно-фінансовій сфері / С. О. Лук'яненко // Проблеми кодифікації законодавства України : матеріали наук.-практ. конф. / за заг. ред. В. П. Нагребельного, Н. М. Пархоменко. – Київ : Ін-т держави і права ім. В. М. Корецького НАН України, 2003. – С. 214–216.

3. Вехов В. Б. Компьютерные преступления. Способы совершения, методики раследования / В. Б. Вехов. – М. : Право и закон, 1996. – 182 с.

4. Соколов А. В. Защита от компьютерного терроризма : справ. пособие / А. В. Соколов, О. М. Степанюк. – СПб. : Арлит, 2002. – 496 с.

5. Малыгин С. С. Основы оперативно-розыскной деятельности : курс лекций / С. С. Малыгин, А. Е. Чечетин. – Екатеринбург : Изд-во Урал. юрид. ин-та МВД России, 2001. – 306 с.

6. Шепетько С. А. Форми вчинення транснаціональними злочинними організаціями окремих злочинів за допомогою використання мережі Інтернет [Електронний ресурс] / С. А. Шепетько // Боротьба організованою злочинністю та корупцією (теорія і практика). – 2014. – № 1 (32). – С. 150–153. – Режим доступу: http://mndc.com.ua/files/file/arhiv_nomeriv/31_40/32.rar.

Одержано 04.11.2014

УДК 343.23:004

Константин Иванович ДОЛЖЕНКО
соискатель кафедры общеправовых дисциплин
факультета права и массовых коммуникаций
Харьковского национального университета внутренних дел

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ПРАВОВОЙ ЗАЩИТЫ ИМУЩЕСТВЕННЫХ ПРАВ АВТОРА ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ В СЕТИ ИНТЕРНЕТ

В настоящее время актуальным вопросом остается вопрос о защите авторских прав на распространяемую в сети Интернет информацию (литературных, музыкальных и аудиовизуальных произведений, фотографий, иллюстраций, карт, планов, рисунков и др.), компьютерные программы, электронные базы данных, дизайн и содержание интернет-страниц (ссылки, графику, HTML и другие языковые ряды, списки Web-сайтов, составленные организациями или отдельными пользователями и др.). В Украине вопросы относительно защиты авторских прав регламентируются Законом Украины «Про авторские или смежные права», однако транснациональных характер сети Интернет особого внимания требуют аспекты защиты имущественных прав автора при электронном

копировании информации (контента сайта), создании гипертекстовых ссылок, загрузки информации на персональный компьютер и др. Исходя из этого многие юристы считают, что программная защита информации более эффективна по сравнению с ее правовой защитой.

Целью данной работы является исследование нормативно-правовой базы по защите информации, распространяемой в сети Интернет.

В международной практике принято употреблять следующие уровни защиты информации: первый – предотвращение (доступ к информации и технологии предоставляется только сотрудниками, которые получили разрешение от владельца информации); второй – выявление (обеспечение раннего выявления и реагирование на преступления и злоупотребление в информационных сетях); третий – ограничение (уменьшение размера потерь на восстановление утраченной или поврежденной информации в случае, если состоялось несанкционированное вмешательство в работу электронно-вычислительных машин, систем и компьютерных сетей); четвертый – восстановление (обеспечение эффективного восстановления утраченной или поврежденной информации).

Механизмы проникновения из Интернета в локальную сеть или локальный компьютер могут быть разными. Например, активные элементы Active-X или Java-аплети Web-страниц, выполняющие деструктивные действия на локальном компьютере; текстовые файлы cookie размещаемые на локальном компьютере некоторыми Web-серверами, позволяют получить конфиденциальную информацию о пользователе локального компьютера; вредоносные утилиты, автоматизирующие создание других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера и т.п. Пресечение проникновения извне на корпоративные узлы организации и защиты внутренних информационных ресурсов обеспечивается при помощи корпоративной (локальной или территориально распределенной) сети – Интранета. Программный или аппаратный барьер между Интернетом и Интранетом устанавливается с помощью брандмауэра (firewall – межсетевой экран: Cisco PIX Firewall, Symantec Enterprise Firewall TM, Contivity Secure Gateway и Alteon Switched Firewall от компании Nortel Networks), посредством которого мониторятся текущие соединения, происходящие в сети, и обеспечивается защита системы от угроз несанкционированного доступа к внутренним информационным ресурсам.

В связи с этим очень часто используют дефиницию «безопасность информационной сети». Несмотря на то, что данная

дефиниция не определена в нормативно-правовых актах, в литературе под безопасностью информационной сети понимают меры, защищающие информационную сеть от несанкционированного доступа, случайного или намеренного вмешательства в работу сети или попыток разрушения ее компонентов. Безопасность информационной сети: включает защиту оборудования, программного обеспечения, данных и персонала; включает разрешение на доступ к данным в сети, который предоставляется администратором сети; состоит из положений и политики, принятой администратором сети, чтобы предотвращать и контролировать несанкционированный доступ, неправильное использование, изменение или отказ в компьютерной сети и сети доступных ресурсов. Пользователи выбирают или им назначаются ID и пароль или другие проверки аутентичности информации, которая разрешает им осуществить доступ к информации и программам в рамках своих полномочий [0]. Понятие «безопасность информационной сети» включает безопасность различных государственных и частных компьютерных сетей, охватывающих и связующих предприятия, государственные учреждения и частных лиц в процесе передачи и распространения информации. Независимо от вида сети (закрытой для публичного доступа или открытой), наиболее часто для обеспечения защиты внутренних сетевых ресурсов используется присвоение им уникального имени и соответствующего пароля.

Таким образом, к ключевым элементам защищенных сетевых служб можно отнести: брандмауэры; антивирусные средства; орудия, которые отслеживают состояние сети, играют важную роль во время определения сетевых угроз; защищенный отдаленный доступ и обмен данными. Безопасный доступ для всех типов клиентов с использованием разнообразных механизмов доступа играет важную роль для обеспечения доступа пользователей к нужным данным, независимо от их местонахождения и используемых устройств. Одним из новых способов, позволяющим обеспечить защиту электронной информации, является использование криптографических методов. К достоинствам криптографических методов относятся защита информации в процессе автоматизированной обработки и передачи данных посредством ее шифрования.

Список использованных источников:

1. Simmonds A. An Ontology for Network Security Attacks / A. Simmonds, P. Sandilands, L. van Ekert // Lecture Notes in Computer Science. – No. 3285. – 2004. – P. 317–323.

Одержано 04.11.2014

РОЗДІЛ 4
КАДРОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343.346.8:004.056.53

Таміла Юріївна ЛАВРОВСЬКА,
студент факультету права та масових комунікацій Харківського національного університету внутрішніх справ;

Марина Володимирівна КРИВОБОК,
студент факультету права та масових комунікацій Харківського національного університету внутрішніх справ

ДОСЛІДЖЕННЯ СТАНУ ОБІЗНАНОСТІ ДЕЯКИХ КАТЕГОРІЙ НАСЕЛЕННЯ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тенденція останніх років щодо стрімкого переходу Низка сучасних противоправних тенденцій у сфері інформаційних відносин та новітній прояв кіберзлочинності – кібертероризм становлять загрозу як окремим громадянам, так і інформаційній безпеці держави. Інформаційна безпека є невід'ємною складовою національної безпеки і важливою самостійною сферою забезпечення національної безпеки [1]. Спеціалісти вважають кіберзлочинність одним з п'яти найбільш поширеніших економічних злочинів в Україні. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини.

Актуальність теми дослідження обумовлена саме тим, що зростання інформаційних технологій зумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції появу нових форм і видів злочинних посягань. Зловмисники активно використовують у своїй злочинній діяльності новітні комп'ютерні засоби і нові інформаційні технології [2].

З кожним роком злочинів в Інтернеті збільшується приблизно на 25–30 %. В Україні вже були прецеденти, коли групи хакерів зупиняли діяльність сайтів держави. Достатньо згадати події 2012 року, коли хакери оголосили протест через те, що був заблокований відомий файлообмінник EX.UA. Таким чином, кіберзлочинність становить реальну загрозу інтересам і держави і особи. Тому соціологічні дослідження щодо моніторингу інформаційної безпеки є вкрай актуальними. За

результатами дослідження «Майкрософт Україна» про рівень комп'ютерної безпеки в Україні, проведеного у 2012 р. в Києві, 92 % українців недостатньо обізнані про кіберзагрози. Саме соціальна інженерія сьогодні стає основним джерелом загроз у мережі. Тільки 30 % респондентів опікується своєю репутацією в Інтернеті, третина користувачів, у яких є діти, майже нічого не знають про загрози в мережі. Також критично вразливі для кіберзлочинців користувачі, старші за 49 років – вони нічого не роблять для того, аби захиститися від кіберзагроз [3].

Тож у суспільстві очевидні тривожні тенденції, що потребують нагального втручання спеціалістів у даній сфері. Для оцінки актуальності проблеми кіберзлочинності було проведено опитування певних категорій населення. Дослідження проводилося методом анкетування. Спеціально розроблена авторами анкета складалась з 22 питань, щодо інформаційної безпеки особи.

За результатами математичної обробки анкет, можна зробити висновки: жертвами кіберзлочинців вважають себе 16 % опитаних, потенційними жертвами можна вважати 84 % респондентів, 86 % вважають кіберзлочинність важливою проблемою, 90 % опитаних бажають поглиблювати знання у галузі захисту інформації. Поряд с тим слід відмітити, що 7 % респондентів взагалі не знають, що таке кіберзлочинність та яку загрозу вона несе для них, тобто фактично вони є 100 % цільовою аудиторією кіберзлочинців.

Отже, робота у галузі навчання основам захисту інформації для визначеної цільової аудиторії, а також програми пропаганди інформаційної безпеки та профілактики кіберзлочинності для населення є актуальною.

Список використаних джерел:

1. Тихомиров О. О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О. О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф. (Київ, 22 берез. 2011 р.). – Ч. 2. – Київ : Вид-во НА СБ України, 2011. – С. 78–82.

2. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю [Електронний ресурс] / А. В. Войціховський // Право і Безпека. – 2011. – № 4 (41). – С. 107–112. – Режим доступу: http://pb.univd.edu.ua/?controller=service&action=download&download=10589.

3. 92 % українців недостатньо обізнані про кіберзагрози / Microsoft Ukraine [Електронний ресурс]. – Режим доступу: http://www.microsoftblog.com.ua/2012/02/07/sid/. – 07.02.2012.

Одержано 29.10.2014

УДК 65.012.8+004

В'ячеслав Валерійович МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів
боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Лілія Магазівна ДОВЖЕНКО,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ЩОДО НЕОБХІДНОГО РІВНЯ ЗНАНЬ СПЕЦІАЛІСТІВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Спеціаліст з протидії кіберзлочинності має завдання збирати, аналізувати і звітувати про докази, отримані з цифрових пристроїв. Він повинен мати рівень підготовки, який дозволить йому свідчити в суді, що може вимагати від нього не просто надання фактичних доказів. Така робота передбачає тлумачення доказів та надання висновків свідка-експерта. Спеціалісти, які виконують ці функції, повинні мати можливість розвивати свої навички і проходити професійну і академічну підготовку, а також користуватись іншими формами підтримання рівня своїх знань шляхом постійного підвищення кваліфікації. Інакше, через інтенсивний розвиток інформаційних технологій в усіх галузях, їхні знання застаріють за лічені місяці.

Розвиток інформаційних технологій призвів до того, що важливі дані можна знайти у різних і найбільш неочікуваних місцях. Тому їх знання та навички повинні давати змогу виконувати процедури наживо, з різними операційними системами і з увімкненим шифруванням. Такі спеціалісти повинні вміти зчитувати дані з усіх сучасних мобільних пристроїв та з дедалі популярніших «хмарних» служб, як от «Dropbox», «iCloud» чи «SkyDrive». Для прикладу, коли хтось купує телевізор «LG», така особа фактично купує комп'ютер разом з Інтернет підключенням і можливостями зберігання інформації, які не поступаються звичайному настільному ПК, та ще й додатковими 500 Гб «хмарного» сховища. Отже, жодне розслідування (кіберзлочину чи якогось іншого злочину) не може вважатись завершеним, доки не буде отримано дані з усіх наявних джерел.

Якщо проаналізувати усі ці факти, стає зрозуміло, що будь-яка підготовка спеціаліста з протидії кіберзлочинності повинна враховувати не тільки поточну ситуацію в Україні,

але й брати до уваги всю наявну інформацію про майбутні тенденції у цій сфері. З огляду на сказане, підготовка повинна охоплювати всі перелічені вище аспекти експертно-криміналістичного процесу, у тому числі збір доказів, створення образів пристроїв, вивчення, аналіз та тлумачення доказів, а також підготовку звітів та інших відповідних видів діяльності. Належне подання цифрових доказів може мати вирішальне значення для будь-якого кримінального судочинства. Тому знання правоохоронця у сфері протидії кіберзлочинності має вирішальне значення для системи кримінального правосуддя. Такі фахівці повинні вміти продемонструвати рівень знань і навичок, які дозволяють їм надавати докази, що можуть бути ефективно використані у суді. Важливо, щоб вони мали чіткий план навчання і підготовки, який визнається в усьому світі і зможе привести їх до високого рівня професійної та/або академічної кваліфікації.

Однак коли йдеться про комп'ютерно-цифрову експертизу, то навіть базові навички становлять проблему для співробітників слідчих та оперативних органів, тому що їхні експертно-криміналістичні можливості обмежені як з огляду на людські ресурси, так і на технологічні аспекти. Саме з цієї причини перед закупівлею експертно-криміналістичного програмного забезпечення співробітники слідчих та оперативних органів повинні пройти відповідну підготовку з користування цими програмами. Також їм необхідно забезпечити достатні фонові знання, необхідні для розуміння принципів роботи і ефективного користування цих інструментів у поєднанні з іншими інструментами.

Враховуючи загальну роль навчальних закладів у системі МВС та той факт, що викладачі які мають досвід у цієї галузі можуть надавати неабияку щоденну допомогу у розслідування складних справ, їхній рівень кваліфікації також має велике значення, особливо коли йдеться про свідчення у суді. Тому викладачі, які спеціалізуються на комп'ютерно-цифровій експертизі, повинні користуватись не лише загальновизнаними програмними інструментами, такими як «EnCase» або «FTK», але й обов'язково проходити підготовчі курси у не постачальників програмних продуктів.

Такі курси нададуть слідчим та оперативним працівникам можливість отримати багато ширшу базу знань і дозволять пояснити, як, чому і коли було створено докази на певному цифровому носії (а не тільки те, як їх було отримано з криміналістичної точки зору), а це один з найважливіших знаннєвих

елементів, які вони повинні передати своїм колегам. Підготовчі курси або тренінги, що пропонуються непостачальниками, мають велике значення ще й через те, що на них навчають користуванню різними безкоштовними інструментами, які інколи перевершують за своєю функціональністю дорогі програмні продукти.

Доцільно проводити низку підготовчих курсів або тренінгів за різними функціями та спеціалізаціями персоналу на конкретні теми цифрової криміналістики, такі як різні операційні системи або типи пристроїв, що вимагають спеціальних знань (наприклад, мобільні телефони або планшети).

Тому навчальні заклади повинні вести облік курсів підготовки або тренінгів, прослуханих кожним викладачем, відстежувати роботу викладачів по завершенні навчання, а потім, за отриманими результатами, намагатись визначити навчально-підготовчі напрямки для кожної особи. Це корисно не тільки для слухача курсів, але й для освітньої системи університету та правоохоронної діяльності в цілому, оскільки статус особи може бути перевірено в межах системи кримінального судочинства.

Одержано 23.10.2014

УДК 65.012.8+004

Mykola M. PEREPELYTSIA,
PhD, associate professor, Chair of Operational and Search Activities, the Research Institute for Training Criminal Police Officers, Kharkiv National University of Internal Affairs

LAW ENFORCEMENT TRAINING STRATEGY FOR CYBERCRIME FIGHTING IN UKRAINE

It has been several decades since high technologies started being actively introduced have into all the spheres of human activity. This process accelerates every year. When the new computer technologies came out, people appeared who began using computers with illegal purpose almost immediately. Before, those were people who had a wealth of knowledge and experience in high technology, but now are not uncommon that the computer infringement is done by ordinary citizens who have only basic computer skills. Because of the circumstances mentioned above, the law enforcement agencies could not remain aloof and now actively fight against cybercrime.

According to statistics, in Ukraine for the period 2005-2009 years high-tech revealed/cleared 3252/2434 crimes, among them

in 2005 – 615/362; in 2006 – 583/415; in 2007 – 656/475, in 2008 – 691/572, in 2009 – 707/610. Thus, during 2002-2010 there was revealed/cleared 989/740 crimes in the field of the use of the electronic-calculated machines (computers), systems and computer networks which are one of cybercrime types and have a clear tendency to growth. During 2011 there was revealed 131 such crimes. During 2012 year were registered 2011 cybercrimes, during 2013 – 4123, cleared near 50 %.

Using of informational technologies in crime investigations are attracting more and more scientific attention. Such technologies often uses by law enforcement authorities in combating cybercrime.

So the aim of the training strategy – comprehensive technical and legal training, retraining and professional development of law enforcement officers in combating cybercrime.

The stakeholders and their learning requirements identified as relevant to the Ministry of Internal Affairs of Ukraine should be as follows:

First Responders (this is a basic level of education which should be delivered to all law enforcement officers of Ukraine):

- Concept an Kinds of Cybercrimes;
- Objects and Subjects of Cybercrime Fighting;
- Organization and Law Principles of Cybercrime Fighting;
- Cybercrime Detection and Prevention;
- Internal and External Cooperation in Cybercrime Fighting;
- International Experience of Cybercrime Fighting;
- Operating Systems Basics;
- Computer Technologies Using in Investigation Methods;
- Criminal Intelligence;
- Information Gathering with Computer Technologies Using;
- Payment Systems.

Undercover Crime Investigator:

- Obtaining Information from Unrestricted Sources;
- Obtaining Identifying Information about Users or Networks;
- Real-time Communications;
- Accessing Restricted Sources;
- Online Communications – Generally;
- Undercover Communications;
- Online Undercover Facilities;
- Communicating through the Online Identity;
- Appropriating Online Identity;
- Online Activity by Investigators During Personal Time;
- Security Vulnerability Using.

Cyber Crime Investigator:
- Introduction to Programming for Cybercrime Investigators;
- VoIP and Wireless Investigations;
- Money Laundering Investigations;
- Investigation of Sexual Abuse of Children on the Internet;
- Linux as an Investigative Tool;
- Special Information Gathering Techniques.

Digital Forensic Expert:
- Mobile Forensic;
- Data Storage Recover and Search;
- Computer Search and Seizure;
- Cloud Computing Investigations;
- Live Data Forensics;
- Malware Analysis and Investigations;
- Macintosh, FreeBSD, Solaris Forensic;
- Cryptography and Steganography;
- Data Mining and Databases.

Одержано 28.10.2014

УДК 343.1

Вадим Сергійович СЕЛЮКОВ,
кандидат юридичних наук,
старший викладач кафедри конституційного та міжнародного права
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ПРОБЛЕМА РЕАЛІЗАЦІЇ ПРАВА НА САМООСВІТУ У КІБЕРПРОСТОРІ

Сучасна освіта зазнає потужної трансформації та шукає відповіді на виклики стрімкого розвитку людської цивілізації. Відбувається еволюція наукового розуміння світу, змінюється культурно-інформаційне середовище і відповідно формуються нові вимоги до новітніх способів отримання знань.

Ядром професійних якостей конкурентоспроможного фахівця, виступає здатність до самоосвіти, яка реалізується через: уміння самостійно проводити пошук та відбір інформації, об'єктивну оцінку необхідності для реалізації і удосконалення професійної діяльності; уміння вчитися самостійно і впродовж всього трудового життя; уміння творчо використовувати суму засвоєних знань, самостійно їх поповнювати і здобувати.

Самоосвіта − придбання систематичних знань в якій-небудь галузі науки, техніки, культури, політичного життя і т. п.,

що передбачає безпосередній особистий інтерес, який проявляється з самостійним вивченням матеріалу. В той же час самоосвіта – засіб самовиховання, оскільки сприяє виробленню цілеспрямованості та наполегливості в досягненні мети, внутрішньої організованості, працьовитості і інших моральних якостей. У широкому сенсі під самоосвітою розуміють всі види придбання знань, пов'язані з самостійною роботою. Основна форма самоосвіти – вивчення наукової, науково-популярної, учбової, художньої та іншої літератури і преси. Самоосвіта передбачає також можливість використання всіляких допоміжних засобів: прослухування лекцій, доповідей концертів, фонозаписів; консультації фахівців; перегляд спектаклів, кінофільмів, телепередач; відвідини музеїв, виставок, галерей; різні види практичної діяльності – досліди, експерименти, моделювання і тому подібне. Дедалі більшого значення

Інтернет як один із провідних засобів спілкування та отримання інформації набуває першочергового значення в освітньо-виховному просторі. Віртуальне середовище настільки глибоко ввійшло до життя сучасного суспільства, що воно безпосередньо відбивається на процесі соціалізації особистості. А найдинамічнішою й наймінливішою соціальною групою цього суспільства є молодь. Під впливом Інтернету змінюється стиль життя молоді – змінюються структура дозвілля, звичні канали отримання інформації, характер міжособистісних взаємодій. Активізується роль Інтернету в підготовці молоді до практичної професійної діяльності.

За останні два десятиріччя Інтернет перетворився на незрівнянний глобальний ресурс, що охоплює світи знань і розваг. Маючи понад 2,27 млрд користувачів у всьому світі, Інтернет є засобом зв'язку, що постійно зростає. Він лежить у точці опори наших суспільств, які дедалі більше з'єднуються одне з одним загальною мережею, рухаючи вперед економіки світу, сприяючи торгівлі та комерції, допомагаючи підвищувати якість охорони здоров'я, виробництва продовольства та освіти. За таких колосальних кроків великого значення набув захист життєво важливих систем та інфраструктур Інтернету від нападів кіберзлочинців.

У Конвенції ООН про права дитини та Загальній декларації прав людини визнається право на освіту й доступ до інформації, а також право брати участь в іграх і розважальних заходах. Конвенції також надає захист від усіх форм експлуатації та від схиляння до будь-якої незаконної діяльності. Ці фактори є ключовими у негативному впливі кіберпростору на особистість людини.

Отже, узагальнюючи проблему взаємозв'язку самоосвіти та кіберпростору, можна констатувати, що освітній процес як в Україні так і в цілому світі виходить на новий рівень. Це пов'язано з стрімким розвитком інформаційних технологій. Враховуючи, що майже кожна особа, що досягла 10-річного віку вміє користуватися Інтернетом, є вірогідність негативного впливу кіберпростору на розвиток особистості, що є детермінуючим фактором у процесі самоосвіти з використанням інтернет-ресурсів. Як висновок варто наголосити на необхідності більш ретельного контролю як з боку держави так і зі сторони освітніх закладів, а також сім'ї, за негативними явищами, що найчастіше зустрічаються в мережі Інтернет задля недопущення негативного впливу на особистість шляхом розповсюдження інформації порнографічного характеру, закликів до експлуатації людей, пропаганда антисоціальних поглядів, розповсюдження наркотичних речовин.

Одержано 14.10.2014

УДК 65.012.8+004

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент,
начальник кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Ірина Миколаївна РЯЗАНЦЕВА,
кандидат юридичних наук,
доцент кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

РЕКОМЕНДАЦІЇ ЩОДО ПІДГОТОВКИ ФАХІВЦІВ З КОМП'ЮТЕРНО-ЦИФРОВИХ ЕКСПЕРТИЗ

Сьогодні комп'ютери стали як об'єктом, так і засобом скоєння різних злочинів. Кількість кримінальних правопорушень, здійснюваних за допомогою комп'ютерних систем, таких як шахрайство, дитяча порнографія та злочини проти інтелектуальної власності, невпинно зростає. Швидкий розвиток інформаційних технологій дуже серйозно впливає на підходи до підготовки борців зі злочинністю, незалежно від злочинів, яким вони протидіятимуть – у сфері кібернетичних чи інформаційних технологій, торгівлі наркотиками або викрадення

автомобілів. Усі повинні усвідомити, що комп'ютери стали чудовим засобом комунікації, який може забезпечити злочинців безпечним каналом зв'язку. Злочинці часто вдаються до електронних платежів як безпечного методу відмивання грошей. Сучасна правоохоронна діяльність неминуче передбачає виявлення і збір цифрових доказів практично стосовно будь-якого злочину.

Якщо проаналізувати існуючі програми підготовки фахівців для підрозділів боротьби з кіберзлочинністю в системі вузівської підготовки МВС України, стає зрозуміло, що вони не пропонують комплексного рішення перелічених вище проблем.

Тому запровадження сучасної, сталої і стандартизованої методики підготовки фахівців у сфері боротьби з кіберзлочинністю, застосовної як до курсантів, так і до підвищення кваліфікації дійсних працівників правоохоронних органів, повинно бути обов'язковим кроком.

Перш ніж запропонувати рекомендації, було проаналізовано чинні навчальні програми підготовки фахівців орієнтованих на боротьбу з кіберзлочинністю інших університетів та перелік тем модулів, оскільки це єдиний спосіб визначити відповідність навчальним планам підготовки фахівців за спеціалізацією «боротьба з кіберзлочинністю» в системі вузівської підготовки МВС України.

Нижче подано перелік тем аналогічного за спрямованістю модуля, орієнтованого на боротьбу з кіберзлочинністю, який викладається у рамках програми «Комп'ютерно-цифрова експертиза та розслідування кіберзлочинів» Дублінського університетського коледжу [1]:

– COMP 40100: Комп'ютерно-технічна експертиза;

– COMP 40110: Мережеві розслідування;

– COMP 41430: Linux для слідчих;

– COMP 41560: Експертиза мобільних телефонів;

– COMP 41650: Розслідування, пов'язані зі шкідливим програмним забезпеченням;

– COMP 41660: Експертиза наживо;

– COMP 41480: Розслідування сексуальних насильств щодо дітей в Інтернеті;

– COMP 41300: Розслідування та аналіз справ про відмивання грошей;

– COMP 41580: Розслідування, пов'язані з протоколом VoIP та бездротовими технологіями;

– COMP 41330: Розслідування з використанням відкритих джерел;

– COMP 41590: Поглиблений курс комп'ютерно-технічної експертизи;

– COMP 40120: Програмування для слідчих;

– COMP 41570: Поглиблений курс з написання програм-сценаріїв;

– Дипломна робота.

Або інший приклад програми, що пропонується Единбурзьким університетом імені Непера [2]:

– Мережева безпека;

– е-Безпека;

– е-Безпека (D/L);

– Мережева безпека (D/L);

– Поглиблений курс з хмарної та мережевої експертизи;

– Поглиблений курс з хмарної та мережевої експертизи (DL);

– Хост-орієнтована експертиза;

– Хост-орієнтована експертиза (DL);

– Лідерство, навчання і розвиток;

– Управління програмними проектами;

– Аудит у сфері безпеки і відповідність;

– Поглиблений курс з професіональної практики;

– Дипломна робота.

У порівняні з існуючими навчальними програмами підготовки фахівців в системі МВС із боротьби з кіберзлочинністю, навіть якщо зміст занять модернізувати, модулі з інформаційних технологій не передбачають достатньої кількості годин для успішного розкриття тем. Як приклад, візьмімо «EnCase», підготовка з якого передбачає щонайменше 120 годин, а модуль «Сертифікований етичний хакінг» розраховано щонайменше на 360 годин. Така сама мінімальна кількість годин виділяється на аналіз шкідливого програмного забезпечення, але уся чотирирічна навчальна програма не передбачає такої кількості годин на теми, пов'язані з кіберзлочинністю.

Серед головних причин, що призвели до нинішньої ситуації слід виділити такі як:

– відсутність допомоги експертів у цій галузі на етапі його формування;

– недостатність або відсутність досвіду у сфері кіберзлочинності серед співробітників навчальних закладів та практичних працівників в системі МВС;

– відсутність рекомендацій;

– відсутність досвіду щодо стандартів та процедур у сфері комп'ютерно-цифрової експертизи та доказів тощо.

Якщо коротко перелічити теми, які необхідно запровадити, то важливо зауважити, що на першому етапі співробітникам

у сфері комп'ютерно-цифрової експертизи та доказів необхідно пройти відповідну підготовку, котра дозволить їм виявляти й опрацьовувати цифрові докази та застосовувати відповідні процедури під час розслідування кіберзлочинів і підготовки цифрових доказів у формі, прийнятній згідно з українськими правовими стандартами. Підготовка з питань процедур і стандартів, прийнятих наразі у цілому світі, повинна здійснюватись на такому базовому рівні і підкріплюватись основами експертизи даних та мережевої експертизи.

На цьому етапі співробітникам необхідно хоча б засвоїти основи використання цифрових експертних інструментів, як от «EnCase» та «FTK», і продуктів для експертизи мобільних пристроїв («UFED» та «Cellebrite»).

У рамках підготовки фахівців з комп'ютерно-цифрової експертизи необхідно охопити такі проблемні області, як:

– комп'ютерно-цифрова експертиза даних (за різними типами операційних систем);
– експертиза мобільних пристроїв;
– експертиза наживо;
– експертиза зловмисних програм і зворотній аналіз;
– «хмарна» експертиза;
– Wi-Fi та шифрування;
– мережева експертиза;
– перехоплення даних та мережева безпека;
– різні види комп'ютерно-цифрової експертизи (напр., зчитування пристроїв на базі «eprom», автомобільні пристрої збереження даних, дані GPS-навігаторів).

Таким чином отримані знання в таких галузях відповідають зобов'язанням, взятим Україною в результаті приєднання до Будапештської конвенції (про кіберзлочинність) з її додатковими протоколами. Головна мета полягає в охопленні усіх основних сфер кіберзлочинності (телекомунікації, електронний вандалізм, тероризм та здирництво, викрадення телекомунікаційних послуг, телекомунікаційне піратство, порнографія та інші злочинні матеріали, телемаркетингове шахрайство, злочини електронного переказу коштів, електронне відмивання грошей), а також урахування тих аспектів інформаційних технологій, які зустрічаються в будь-якому розслідуванні як кіберзлочинів, так і «класичних» злочинів.

Список використаних джерел:

1. MSc in Forensic Computing & Cybercrime Investigation [Електронний ресурс]. – Режим доступу: http://www.ucd.ie/cci/education/prospective_students/fcci_programmes/msc_fcci/modules_available.html. – Назва з титул. екрана.

2. Advanced Security and Digital Forensics [Електронний ресурс]. – Режим доступу: http://www.courses.napier.ac.uk/AdvancedSecurityand DigitalForensics_W56731.htm.

Одержано 23.10.2014

УДК 351.74(477)

Ганна Михайлівна ШОРОХОВА,
науковий співробітник науково-дослідної лабораторії з проблем організації навчального процесу заочного та дистанційного навчання навчально-наукового інституту заочного та дистанційного навчання Харківського національного університету внутрішніх справ

ПІДГОТОВКА ПРАЦІВНИКІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

У нинішній надзвичайно складній соціально-політичній ситуації та криміногенній обстановці в державі, проблемам боротьби з кіберзлочинністю приділяється значна увага, однак результати цієї боротьби залежать від функціонування ефективної системи підготовки, перепідготовки і підвищення кваліфікації співробітників відповідних підрозділів Міністерства внутрішніх справ України.

Для запобігання злочинної діяльності в сфері використання комп'ютерних технологій важливого державного значення набуває підготовка працівників оперативних підрозділів правоохоронних відомств, на які покладаються завдання виявлення, розкриття і профілактики цих суспільно небезпечних явищ.

Ефективність підготовки співробітників органів внутрішніх справ, безумовно, залежить від багатьох чинників. Значне місце серед них посідає фахова та спеціальна підготовка. В свою чергу, ефективність спеціальної підготовки залежить від інформаційної культури працівника, яка повинна включати в себе не тільки добре володіння навичками роботи з комп'ютером, а й загальне орієнтування у інформаційному всесвіті. Тільки за такої умови можливо значно підвищити та закріпити рівень підготовки на практиці. В науковій літературі вже спостерігалися дискусії стосовно залучення фахівців з технічною освітою для вирішення низки завдань, що стоять перед органами внутрішніх справ, зокрема для підвищення ефективності боротьби зі злочинами в сфері використання комп'ютерних технологій. Справді залучення спеціалістів законодавчо врегульовано та з давніх-давен є чинним інститутом кримінального судочинства. Але поряд з цим існує ряд суттєвих недоліків.

Так, спеціалісти та експерти залучаються для надання допомоги, а не для запобігання та розкриття злочинів безпосередньо, виходячи з розбіжності професійного мислення. Певні труднощі із залученням спеціалістів виникають при здійсненні негласних оперативно розшукових заходів.

Все це переконливо свідчить про необхідність розробки та впровадження спеціальної підготовки працівників органів внутрішніх справ для боротьби зі злочинами в сфері використання комп'ютерних технологій.

Харківський національний університет внутрішніх як флагман відомчої освіти здійснює підготовку спеціалістів у сфері інформаційної безпеки. Так, у складі Університету у 2013 році створено факультет підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми.

Факультет готує бакалаврів за наступними напрямами підготовки:

– правознавство (слідство), спеціалізація «Боротьба з кіберзлочинністю».

– правознавство (кримінальна міліція), спеціалізація «Протидія торгівлею людьми».

– правознавство (кримінальна міліція), спеціалізація «Боротьба з кіберзлочинністю».

– системи технічного захисту інформації за спеціалізацією «Боротьба з кіберзлочинністю».

Головним напрямом практичної діяльності випускника університету є підвищення ефективності правоохоронної діяльності органів внутрішніх справ за допомогою використання сучасних засобів управління, впровадження комп'ютерних систем обробки та аналізу інформації, впровадження в діяльність органів внутрішніх справ сучасних інформаційних технологій та методик використовування технічних засобів. Випускники факультету відповідно до напрямів підготовки отримують такі навички та знання, як розслідування комп'ютерних злочинів; проведення комплексу оперативно-розшукових заходів при розслідуванні комп'ютерних злочинів; побудова комплексної системи захисту інформації; пошук та аналіз інформації оперативно-розшукового, довідкового та управлінсько-адміністративного характеру в інформаційних системах та мережах; інформаційні системи та технології у роботі правоохоронних органів; технічне забезпечення інформаційно-управляючих систем та комп'ютерних мереж тощо. Кафедри інформатики та інформаційних систем та технологій в діяльності органів внутрішніх справ викладають дисципліни інформаційного та апаратно-

програмного напряму. Кафедра інформаційної безпеки готує фахівців з систем технічного захисту інформації та боротьби з кіберзлочинністю для практичних підрозділів органів внутрішніх справ.

Для підготовки висококваліфікованих кадрів для підрозділів боротьби з кіберзлочинністю та торгівлею людьми навчальний заклад має достатній потенціал та досвід. Також для якісної підготовки працівників однією з головних складових є оновлення матеріально-технічної бази та оснащення профільних навчально-тренувальних класів сучасними комп'ютерними розробками.

При факультеті діє навчально-тренувальний центр протидії кіберзлочинності та моніторингу кіберпростору на громадських засадах, учасниками та консультантами якого стали курсанти та працівники університету. Основним напрямом діяльності центру є вивчення питань протидії кіберзлочинності та моніторингу кіберпростору.

В свою чергу Харківський національний університет внутрішніх зробив великий внесок у вирішення питання підготовки висококваліфікованих працівників органів внутрішніх справ для боротьби з кіберзлочинністю.

Одержано 21.10.2014

УДК 159.95

Світлана Владиславівна ЖИДЕЦЬКА,
здобувач кафедри соціології та психології
Харківського національного університету внутрішніх справ

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ НАВЧАЛЬНО-ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ КУРСАНТА

Бурхливий розвиток науки і техніки, постійне зростання вимог до людини зробили її життя надто стрімким і плинним.

Як показує історія, розвиток і прогрес, які приносять людству нові блага і можливості, на жаль, завжди супроводжуються негативними явищами. Так, комп'ютеризація і розвиток цифрових технологій, які спростили людині життя, полегшили існування в багатьох сферах та в деякій мірі перевернули уявлення про роботу, кар'єру, дозвілля, фінанси, в той же час поставили перед загрозою. Довіряючи свої особисті дані, листування, гроші інтернет-простору, ми наражаємось на велику небезпеку.

Розповсюдження комп'ютерних вірусів, шахрайство з картками, крадіжки з банківських рахунків, викрадання інформації породило нову категорію злочинів – кіберзлочини або злочини в сфері комп'ютерних технологій.

Лавиноподібна й повсюдна комп'ютеризація всіх сфер людської діяльності ставить перед вищою школою питання про організацію ефективного масового навчання кваліфікованих користувачів незалежно від кінцевої професійної орієнтації майбутніх фахівців. Уміння використати у своїй професійній діяльності засоби обчислювальної техніки й телекомунікацій варто розглядати як критерій загальної грамотності, порівняний на сьогоднішній день із традиційним трактуванням даного поняття (як уміння читати, писати й лічити).

Знання й застосування інформаційно-комп'ютерних технологій відкриває для майбутніх працівників органів внутрішніх справ нові можливості не тільки в плані засвоєння нових знань, розширення кола спілкування в мережі Інтернет, але й в аспекті розуміння, розпізнавання технік кіберзлочинності, організації протидії їх реалізації.

Заняття в супроводі мультимедійних презентацій, on-line тестів і програмного забезпечення дозволяють курсантам поглибити знання, провести заняття, що більш запам'ятовуються, більш цікаві та яскраві. «Я почув і забув. Я побачив і запам'ятав. Я зробив і зрозумів» (Конфуцій).

Можна рекомендувати до використання в години, що відведені на самостійну підготовку курсантів: інтернет-ресурси; комп'ютерні лекції; електронну бібліотеку; електронний підручник (по тематиці кіберзлочинності).

Можливості використання інтернет-ресурсів величезні. Глобальна мережа Інтернет створює умови для одержання необхідної курсантам інформації, що перебуває в будь-якій точці земної кулі.

У процесі професійного становлення, вивчення інформаційно-комп'ютерних технологій у курсантів формуються наступні компетенції:

– здатність до аналізу юридично значимих процесів і явищ у сфері світової кіберзлочинності й використання отриманих знань на практиці при рішенні професійних завдань;

– здатність вдосконалювати й розвивати свої професійно важливі якості й загальнокультурний рівень.

Використання інформаційно-комп'ютерних технологій у навчальному процесі є більш ефективним при засвоєнні

змістовної частини матеріалу; формуванні певних умінь та навичок; можливості подання інформації в аудіо-, відео- або іншому форматі.

Використання інформаційно-комп'ютерних технологій сучасних в навчальному процесі створює сприятливі умови для формування особистості курсантів та відповідає запитам сучасного суспільства.

Список використаних джерел:

1. Про ратифікацію Конвенції про кіберзлочинність : закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5–6. – Ст. 71.

2. Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій : посібник / М. І. Камлик, Б. В. Романюк, В. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк ; за заг. ред. Я. Ю. Кондратьєва. – Київ : НАВСУ, 2000. – 64 с.

3. Біленчук Д. П. Кібершахраї – хто вони? / Д. П. Біленчук // Міліція України. – 1999. – № 7–8. – С. 32–34.

Одержано 03.11.2014

РОЗДІЛ 5
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

УДК 343.1

Лариса Дмитрівна ВАРУНЦ,
кандидат юридичних наук,
старший викладач кафедри конституційного та міжнародного права
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ЩОДО БОРОТЬБИ ПОЛІЦІЇ КАНАДИ З КІБЕРЗЛОЧИННІСТЮ

Безперечно, на сучасному етапі розвитку людського суспільства важливим стратегічним ресурсом що потребує охорони, є інформація, яка містить надзвичайно широкий спектр зведень: від простих даних про громадян країни до стратегічних державних програм. Саме тому ці дані все більше стають предметом злочинних зазіхань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем, забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Як наслідок – поява нового виду злочинності – «комп'ютерної» або кіберзлочинності.

На наш погляд, одним із важливих напрямків діяльності поліції є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідуванням яких займається підрозділ КККП по боротьбі з комп'ютерною злочинністю, опираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами.

Діяльність підрозділу направлена на розслідування та розкриття злочинів, пов'язаних із комп'ютерами і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектору; дає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами.

Враховуючи ту обставину, що інформаційна система дозволяє передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2500 точок доступу, до яких входять близько 1285 федеральних і провінційних

поліцейських відділень. 1180 підрозділів спеціалізованих відділів КККП підключені до ліній системи.

Безперечно, даний напрямок діяльності поліції є важливим, оскільки економічні втрати досягли широких масштабів, деякі злочинці діють на міжнародному рівні, організованою групою.

Слід визнати, що канадське законодавство щодо визначення комп'ютерної злочинності потребує вдосконалення. Враховуючи те, що завдання, які стоять перед підрозділами поліції щодо боротьби з комп'ютерною злочинністю носять міжнародний характер і не є специфічними для Канади, вони активно співпрацюють з іншими країнами з метою розробки міжнародного законодавства в даному напрямку.

Розкриття комп'ютерних злочинів являє собою складне завдання, у першу чергу через фактор часу, оскільки передача даних може бути виконана майже миттєво, часто буває даремно шукати які-небудь докази, що підтверджують порушення міжнародного законодавства. За даними КККП, у даний час безліч комп'ютерних злочинів здійснюється дітьми, що не досягли дванадцятирічного віку. Згідно з кримінальним кодексом Канади, для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та намір особи заподіяти своїми діями шкоду. Такий підхід потребує чіткого встановлення параметрів доступу до комп'ютерної техніки з метою попередження порушень. Необхідно враховувати дані щодо осіб, параметри доступу з урахуванням обмежень, можливість службовцями «експериментувати» з програмами. Кваліфіковану консультацію щодо можливої неправомірної поведінки в даному напрямку може надати міністерство юстиції чи відповідний підрозділ КККП.

Слід зазначити, що методика розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, ними займаються спеціалізовані поліцейські підрозділи. З огляду на небезпеку комп'ютерної злочинності, тенденцію її розвитку, впливу на світове співтовариство, у рамках ООН регулярно проводяться симпозіуми з профілактики і припинення комп'ютерної злочинності. Як один із напрямків фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом удосконалення системи автоматичного контролю. На попередження та зменшення злочинів щодо незаконного використання телекомунікаційних систем на міжпровінційному, державному і міжнародному рівні спрямовані

дії управління по боротьбі з економічними злочинами. Допомагає поліцейським підрозділам Інформаційний центр.

Поліцейська діяльність щодо попередження та розкриття діянь, пов'язаних з кіберзлочинністю, спрямована і на різнобічний розвиток відносин з якомога більшим суспільним колом через засоби масової інформації, консультативні зустрічі з представниками громадськості, взаємовідносини з різноманітними органами влади і управління, громадськими організаціями, окремими громадянами.

Таким чином, поліція є важливим партнером у співтоваристві відомств, що займаються боротьбою зі злочинністю, в тому числі кіберзлочинністю, забезпеченням дотримання прав людини, забезпеченням захисту федеральних державних комп'ютерних центрів, приватного сектора.

Одержано 14.10.2014

УДК 343.1

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент,
доцент кафедри конституційного та міжнародного права
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ДІЯЛЬНІСТЬ НАТО У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

За сучасних умов активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують інформаційні технології для реалізації своїх намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної і міжнародної безпеки.

Шпигунство, руйнування, крадіжка військових і промислових секретів та інші злочини за допомогою комп'ютерних технологій активно поширюються і удосконалюються. Напади на організацію чи країну стимулюються, розробляються і здійснюються організованими фахівцями. Це далеко вже не ті «хакери», які здійснювали напади на системи заради розваги.

Досвід вірусу «Стакснет», який, за повідомленнями, серйозно зашкодив ядерній програмі Ірану в 2010 році, вказує на перехід від кіберсвіту до фізичного світу. Вода, електроенергія, лікарні, безпека повітряних перевезень, оборона, банківські послуги – усі вони залежать від інформаційних мереж.

Так багато існує чуттєвих сайтів, пошкодження яких може завдати шкоди організації чи усій країні.

Кількість кібернападів зростає щодня як проти систем НАТО, так і проти важливих систем країн-членів організації. НАТО повинна мати здатність надавати допомогу в сфері кіберзахисту своїм членам, допомагаючи їм запобігати таким нападам, виявляти їх, а в разі нападу швидко реагувати заради зменшення шкоди.

Задля протидії різним проявам кіберзлочинності НАТО у 2011 році розпочала формулювати концепцію Групи швидкого реагування. Створення цієї групи стало результатом перегляду політики кіберзахисту НАТО, яка була переглянута міністрами оборони в червні 2011 року. Зазначені фахівці з кіберзахисту відповідальні за надання допомоги країнам-членам, які звертаються по допомогу в разі нападу національного значення.

Кібернапади такого типу, яких зазнали Естонія і Грузія, в майбутньому стануть найбільш поширеною формою кібернападів. Все частіше в суспільстві проявляється суміш протестів або звичайних воєнних дій з кібернетичним елементом. Тому групи швидкого реагування повинні бути готовими до дій негайно в міру необхідності у допомозі.

Технічний центр Сил реагування НАТО на комп'ютерні інциденти (NCIRC) став мозковим вузлом боротьби Альянсу проти кіберзлочинності. NCIRC відповідає за кіберзахист усіх сайтів НАТО, незалежно від того, належать вони постійним штабам, чи штабам, розгорнутим на час операцій чи навчань.

NCIRC досяг цілковитої оперативної готовності на початку 2013 року. Розробляються умови співробітництва, в тому числі між експертами, які користуються взаємною довірою і представляють країни, промисловість, академічні кола і НАТО. Ці домовленості зрештою відкриють доступ до спеціальних знань в усіх сферах кібербезпеки. Готуються також вимоги до експертів, які будуть брати участь у місіях з надання допомоги, визначаються сфери їх компетенції.

Усі процедури Групи швидкого реагування і можливі дії визначені в посібнику, над яким продовжують працювати експерти у галузі протидії кіберзлочинності і фахівці з планування на випадок надзвичайних ситуацій цивільного характеру. У цьому посібнику будуть розписані рекомендації щодо реагування НАТО на прохання країн Альянсу і партнерів про допомогу в захисті їхніх інформаційних і комунікаційних систем.

Маючи Групи швидкого реагування НАТО зможе, на запит, запропонувати професійну і добре організовану допомогу своїм країнам-членам і партнерам, але передусім тим країнам,

які поки що не мають ресурсів для створення такого роду оборонних сил. Це одна з версій військового принципу взаємодопомоги і колективної оборони.

Сили швидкого реагування складатимуться з постійного ядра з шести спеціалістів, які здатні координувати і виконувати місії Групи швидкого реагування. У певних сферах будуть також задіяні національні експерти і експерти з НАТО. Їх кількість і характер залежатимуть від місії, яку необхідно буде виконати.

Групи швидкого реагування матимуть усе необхідне оснащення: комп'ютерне і телекомунікаційне обладнання, таке як супутникові телефони і обладнання для цифрового збирання свідчень, криптографії, цифрового судового аналізу, зниження вразливості, безпеки мереж тощо.

Будь-яка країна – член НАТО, яка постраждала від серйозного кібернападу, зможе звернутися до НАТО по допомогу. Такий запит розгляне Комісія з менеджменту кіберзахисту (CDMB). Прохання про допомогу, які надходитимуть від країн – нечленів НАТО, будуть потім затверджуватися Північноатлантичною радою.

В разі приведення в дію Групи швидкого реагування зможуть відреагувати на інцидент протягом 24 годин.

Слід відмітити, що кіберзлочинність не має державних кордонів, – отже, й зусилля з протидії їй – справа не однієї держави. Потрібна плідна міжнародна співпраця багатьох країн світу як на державному рівні, так і на рівні співробітництва між урядовими організаціями та представниками бізнесу у сфері розповсюдження ІТ-технологій.

Україна як активний учасник кіберпростору також потребує взаємодії у справі протидії різноманітним посяганням на комп'ютерні мережі. Так, Служба безпеки України почала відпрацювання з НАТО спільних механізмів боротьби з кіберзлочинністю.

В Ялті 11–13 жовтня 2011 року відбулися міжнародні експертні консультації «Україна-НАТО». В обговоренні, організованому Радою національної безпеки і оборони України, взяли участь представники НАТО, СБУ, Державної служби спеціального зв'язку та захисту інформації України, Міністерства оборони України, Служби зовнішньої розвідки України, МВС, МЗС; міністерства оборони Естонії, наукових інститутів Туреччини, Румунії, Франції та Польщі.

Експертні консультації у рамках роботи групи «Україна-НАТО» мали на меті відпрацювання механізмів міжнародного співробітництва та спільних програм із залученням представників гілки державного управління та приватного сектора

у питаннях захисту інформаційної сфери держави. Вітчизняні та іноземні учасники робочих зустрічей обговорили найбільш актуальні питання розвитку систем захисту кіберпростору, зокрема, особливості забезпечення кібернетичної безпеки за умов інформатизації; взаємодії державного та приватного секторів у питаннях захисту інформаційної сфери держави; особливості обробки персональних даних в контексті кібернетичного захисту; проблеми формування недержавного сектору безпеки України; сучасні загрози інтернет-простору. Представники Ради національної безпеки і оборони України розповіли про роботу над проектом Стратегії України у галузі кібернетичного захисту. Під час Консультацій сторони обмінялися досвідом із питань протистояння кібернетичним загрозам. Обговорювалися суто практичні аспекти – особливості правозастосовчої діяльності, розслідування, попередження та протидії кіберзлочинності, шляхи розбудови системи реагування на кібернетичні атаки на національні інформаційні інфраструктури тощо.

На думку багатьох фахівців, відсутність міжвідомчої структури, яка координуватиме діяльність державних органів та спецслужб гальмує роботу у справі протидії кіберзлочинності. Нині функції захисту інформації з обмеженим доступом покладено на різні структури (Держспецзв'язку, СБУ, МВС). Для більш тісного і ефективного співробітництва у боротьбі з кіберзлочинністю, підкреслюється на необхідності створити Україною міжвідомчої структури з боротьби з кіберзлочинністю для координації дій державних органів у цій сфері.

Одержано 14.10.2014

УДК 343

Вікторія Василівна ГВОЗДЕЦЬКА,
студент інституту підготовки кадрів для органів юстиції України Національного юридичного університету імені Ярослава Мудрого (м. Харків)

РОЗВ'ЯЗАННЯ ПРОБЛЕМИ КІБЕРЗЛОЧИННОСТІ В ЗАРУБІЖНИХ КРАЇНАХ

Скоєння та розслідування кіберзлочинів – це міжнародна проблема для підрозділів боротьби з кіберзлочинністю. Тому для ефективної протидії цим явищам потрібно обмінюватися досвідом із фахівцями з різних країн.

У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту

про стан світової кібербезпеки. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. Звіт був складений спеціально для того, щоб допомогти урядам та організаціям зрозуміти, на скільки вони кібернетично захищені в порівнянні з іншими країнами.

Базою для складання звіту були дослідження групи експертів у складі 80 фахівців з 27 країн. Вони надали компанії Security & Defence Agenda офіційні висновки про поточну готовність до кібератак інформаційних систем різних країн. Таблиця показує стан готовності до кібератак інформаційних систем окремих країн (вищий рейтинг – кращий захист).

Рейтинг	**Країна**
5	–
4,5	Фінляндія, Ізраїль, Швеція
4	Данія, Естонія, Франція, Німеччина, Нідерланди, Іспанія, Великобританія, США
3,5	Австралія, Австрія, Канада, Японія
3	Китай, Італія, Польща, Росія
2,5	Бразилія, Індія, Румунія
2	Мексика

Європейське агентство з мережної та інформаційної безпеки у своїй «Програмі надійності та захисту ключової інформаційної інфраструктури», як і експерти, які були залучені Security &Defence Agenda, також наполягає на необхідності налагодження співпраці з метою гарантій узгодженості характерних методик кіберборотьби. На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на ключові позиції [1].

Міністром внутрішніх справ Франції Мішель Алліот-Марі 14 лютого 2008 року була оприлюднена французька стратегія з питань боротьби з кіберзлочинністю. В стратегії визначено наступні основні напрями:

1) модернізація методів розслідування за рахунок удосконалення технічних та нормативно-правових актів для ідентифікації користувачів Інтернет;

2) розробка та встановлення правил співробітництва суб'єктів, що надають послуги з Інтернету, зі службами зацікавленими в боротьбі проти кіберзлочинності;

3) створення нових форм інкримінування провини. За вторгнення в особисте життя людини пропонується покарання у виді одного року тюремного ув'язнення й 15000 євро штрафу;

4) приведення у відповідність сучасним вимогам зміцнення дій представників поліції за рахунок створення групи, що буде займатися шахрайствами в Інтернеті;

5) підвищення кваліфікаційного рівня;

6) удосконалення опису ознак незаконних сайтів. Механізм опису ознак таких сайтів повинен сприяти попередженню їхньої посади [2].

Конвенцією Ради Європи про кіберзлочинність встановлені наступні обов'язкові вимоги для врахування у законодавстві країн, які приєдналися:

– надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які необхідні для розкриття злочину (ч. 1 ст. 16, ст. 17 Конвенції про кіберзлочинність);

– збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16 Конвенції про кіберзлочинність);

– встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язані не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, який визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції про кіберзлочинність) [3].

У середовищі, де постійно з'являються та еволюціонують кіберзагрози, не можна залишатися не захищеним: сформована в світі ситуація зобов'язує до постійного вдосконалення методів боротьби з кіберзлочинами та стимулює побудову державної моделі, спрямованої на забезпечення кібербезпеки країни.

Список використаних джерел:

1. Йона О. О. Світові тенденції боротьби з кіберзлочинністю [Електронний ресурс] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204), ч. 1. – С. 59–61. – Режим доступу: http://nbuv.gov.ua/j-pdf/VSUNU_2013_15(1)__11.pdf.

2. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності [Електронний ресурс] / В. М. Бутузов // Боротьба з організованою злочинністю

і корупцією (теорія і практика). – Вип. 19. – 2008. – С. 240–246. – Режим доступу: http://nbuv.gov.ua/j-pdf/boz_2008_19_28.pdf.

3. Конвенція [Ради Європи] про кіберзлочинність : від 21.11.2001 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

Одержано 29.10.2014

УДК 343

Катерина Юріївна ГОРБУНОВА,
студент інституту підготовки кадрів для органів юстиції України Національного юридичного університету імені Ярослава Мудрого (м. Харків)

МІЖНАРОДНА СПІВПРАЦЯ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Актуальність даної теми є досить високою, оскільки інформаційні технології на сьогодні є не тільки принципово новим засобом масової комунікації – вони охоплюють практично всі сфери людської діяльності. Технічне удосконалення телекомунікаційних систем глобального зв'язку і спрощення доступу до використання комп'ютерних технологій для широкого кола користувачів, веде до трансформації злочинності, яка для реалізації протиправних намірів переміщується у кіберпростір. З цією метою як організовані злочинні угруповання наймають ІТ-фахівців, так і самі ІТ-фахівці створюють структуровані злочинні спільноти за мафіозними типами (наприклад, Carder-Planet) [1]. За оцінками експертів Міжнародної торгової палати, число кіберзлочинів, зростає, причому пропорційно числу інтернет-користувачів. За даними Інтерполу, Інтернет став тією сферою, де рівень злочинності зростає найшвидшими темпами [2].

Інтернет в наш час надав можливість здійснювати злочини на великій відстані, безконтактно, без фізичного зближення жертви та суб'єкта злочину, а також можливо проведення таких незаконних операцій багаторазово та з великою швидкістю, що призводить до значних ускладнень при їх розкритті. Через що багато злочинів мають високий рівень латентності та низький рівень розкриття. Тому це зумовлює те, що країни повинні співпрацювати між собою у боротьбі з цим явищем, для більшої ефективності.

В Україні функції боротьби з кіберзлочинністю зосереджено в руках однойменного Управління (далі – УБК), яке підпорядковане Міністерству внутрішніх справ України. На теперішній

час в УБК налагоджено конструктивну взаємодію щодо боротьби з кіберзлочинністю практично з усіма з відомствами та правоохоронними органами багатьох інших країн. Останнім часом в УБК було накопичено багато інформації про контингент осіб, причетних до організації та здійснення кіберзлочинів. У відповідному банку даних є не тільки громадяни України, останніми роками кількість іноземних громадян також істотно зросла. Це підкреслює необхідність широкої міжнародної співпраці. У багатьох країнах розроблена та активно застосовується нормативно-правова база, присвячена питанням боротьби з кіберзлочинністю. Як правило, відповідні норми викладено у декількох законодавчих, а також підзаконних актах, що мають відомчий або міжвідомчий характер. Прикладом останніх є Online Investigative Principles for Federal Law Enforcement Agents 1999 р., FBI Domestic Investigations and Operations Guide від 15.10.2011 (США), Постанова Державної Ради КНР від 20.09.2000 № 292 «Заходи щодо управління сферою Інтернет-послуг» тощо. У Німеччині питанням боротьби з кіберзлочинністю присвячено § 20 k Закону «Про федеральне управління кримінальної поліції та співробітництво федерації і земель за кримінальними справами» від 07.07.1997, згідно з яким в окремих випадках дозволяється проводити санкціонований негласний онлайн обшук. У Китаї ст. 11 Закону КНР «Про органи державної безпеки» від 22.02.1993 також опосередковано зачіпає проблеми кібербезпеки. Теж саме стосується Regulation of Investigatory Powers Act (Великобританія), Copyright Act, Act on Punishment of Activities Relating to Child Prostitution and Child Pornography (Японія). Підрозділи боротьби з кіберзлочинністю беруть участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим із їх використанням (сфера боротьби з кіберзлочинністю). Міжнародна співпраця є одним і з пріоритетів у діяльності УБК. Так наприклад, у березні 2013 року за підтримки посольства Великобританії в Україні на базі Національної академії внутрішніх справ проведено тренінг з питань боротьби з дитячою порнографією в Інтернеті. Та багато інших тренінгів та стажувань [3].

Слід зазначити, що на сьогоднішній день у міжнародному співтоваристві налагоджена система співробітництва. США та

більшість країн ЄС виносять питання по боротьбі з кіберзлочинністю на перші місця. Для України така тенденція є досить позитивною, хоча власна стратегія щодо боротьби з кіберзлочинністю тільки розробляється [4]. Таким чином, можна зробити висновки, що та ситуація, яка відбувається у світі примушує до забезпечення захисту держави від кіберзлочинів, розробляти певні ефективні концепції, програми та методи для боротьби з нею, формувати висококваліфікований особовий склад підрозділами боротьби з кіберзлочинністю, а також більш тісно взаємодіяти на світовій арені з даного питання.

Список використаних джерел:

1. Сивухін В. С. Конституційні засади транскордонного доступу як форми міжнародного співробітництва у боротьбі з організованою кіберзлочинністю [Електронний ресурс] / В. С. Сивухін // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2013. – № 1 (29). – С. 257–264.- Режим доступу: http://nbuv.gov.ua/j-pdf/boz_2013_1_31.pdf.

2. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю [Електронний ресурс] / А. В. Войціховський // Право і Безпека. – 2011. – № 4 (41). – С. 107–112. – Режим доступу: http://pb.univd.edu.ua/?controller=service&action=download&download=10589.

3. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю [Електронний ресурс]/ М. Ю. Літвінов // Право і Безпека. – 2014. – № 1 (52). – С. 85–89. – Режим доступу: http://pb.univd.edu.ua/?controller=service&action=download&download=17028.

4. Йона О. О. Світові тенденції боротьби з кіберзлочинністю [Електронний ресурс] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204), ч. 1. – С. 59–61. – Режим доступу: http://nbuv.gov.ua/j-pdf/VSUNU_2013_15(1)__11.pdf.

Одержано 29.10.2014

УДК 343.1+004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент,
професор кафедри захисту інформації
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

СИСТЕМА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ FBI U.S.

У контексті реформування правоохоронних органів України представляє інтерес аналіз структури системи протидії кіберзлочинності США, яка головним чином побудована і підтримується у рамках діяльності Федерального бюро розслідувань (FBI).

В організаційно-штатній структурі FBI за напрямом протидії кіберзлочинності передбачено [1]:

– кіберпідрозділ (Cyber Division) штаб-квартири FBI (FBI Headquarters), який координує і узгоджує роботу зі всіма іншими структурами за цим напрямом;

– кібервідділи (cyber squads) зі штатом відповідних агентів та аналітиків у штаб-квартирі та 56 територіальних офісах (field offices) FBI, які розташовані у найбільш великих містах США;

– слідчо-оперативні мобільні кіберкоманди (Cyber Action Teams, CATs), у склад яких входять мінімальна кількість висококваліфікованих агентів, аналітиків, комп'ютерних експертів-криміналістів і експертів зі шкідливого програмного коду, які виїжджають по всьому світу для надання допомоги у розслідуванні найбільш небезпечних для національної безпеки і економіки США кіберзлочинів;

– спеціальні групи із розслідування комп'ютерних злочинів (Computer Crimes Task Forces, зараз їх 93), у склад яких під патронатом FBI входять співробітники інших організацій і відомств, як правоохоронних, так і ні.

Систему протидії кіберзлочинності FBI можна окреслити у вигляді взаємопов'язаних вузлів [1]:

– головні пріоритети діяльності FBI у сфері протидії кіберзлочинності;

– ініціативи і взаємодія із партнерами;

– фабули розкритих злочинів;

– дані про злочинців, що розшукуються;

– актуальні кіберзагрози та шахрайства;

– інформаційно-методичні матеріали із захисту від кіберзагроз.

Розкриємо деякі вузли цієї системи більш детально.

До головних пріоритетів у сфері протидії кіберзлочинності FBI відносить:

– протидію вторгненням у комп'ютери та мережі;

– протидію крадіжкам ідентифікаційної інформації (засоби ідентифікації особи, персональні дані, біометричні дані і т. п.);

– підтримка функціонування інтернет-центру прийому заяв про кіберзлочини (Internet Crime Complaint Center, IC3 [2]), основна задача якого здійснювати прийом, первинну перевірку і передачу відповідним правоохоронним структурам заяв про кіберзлочини.

FBI започаткувало такі спільні проекти у сфері протидії кіберзлочинності:

– об'єднана спеціальна група національних кіберрозслідувань (National Cyber Investigative Joint Task Force, NCIJTF), в яку входять близько 19 розвідувальних і правоохоронних структур США і якій делеговано бути координаційним центром для всіх урядових агенцій у сфері внутрішніх національних кіберрозслідувань тероризму, шпигунства і інших злочинів;

– спеціальні кібергрупи (Cyber Task Forces) територіальних офісів (field offices) FBI, діяльність яких зосереджена виключно на загрозах кібербезпеки і підтримки розслідувань NCIJTF на місцевому рівні;

– захищений інформаційний портал iGuardian, через який зареєстровані представники промисловості (приватного бізнесу) та окремі партнери можуть повідомляти про кібервторгнення у свої інформаційні системи в режимі реального часу;

– асоціація InfraGard [3], в яку входять представники приватного бізнесу (private sector), академічні інститути, правоохоронні органи та інші. Основною задачею InfraGard є двосторонній обмін інформацією між її членами у сфері протидії кіберзлочинності; основним комунікативним каналом виступає власна захищена комп'ютерна мережа та портал iGuardian;

– національний альянс кіберкриміналістики та навчання (National Cyber-Forensics & Training Alliance, NCFTA [4]), який об'єднує експертів-криміналістів публічного, приватного та академічного сектору з метою створення системи раннього попередження і профілактики кіберзагроз та підвищення кваліфікації (навчання) співробітників правоохоронних органів, у тому числі і з інших країн, у сфері протидії кіберзлочинності;

– стратегічний альянс робочих груп протидії кіберзлочинності (Strategic Alliance Cyber Crime Working Group), в який з метою об'єднання зусиль у сфері протидії кіберзлочинності входять відповідні підрозділи поліції Австралії, Канади, Нової Зеландії, Великобританії та FBI США.

Інформування про актуальні кіберзагрози, шахрайства та інформаційно-методичні матеріали захисту від них здійснюється за допомогою:

– публікації центром IC3 річних аналітичних звітів, в яких наведені різноманітні статистичні показники по зареєстрованих кіберзлочинах;

– функціонування системи національного кіберінформування (National Cyber Awareness System, NCAS, [5]), яка забезпечується командою реагування на комп'ютерні надзвичайні події (US-CERT) Департаменту внутрішньої безпеки США (Department of Homeland Security) шляхом представлення

можливості підписатися на розсилку електронних листів щодо: виявлених надзвичайно небезпечних для загалу інцидентах з інформаційної безпеки; своєчасного інформування з питань інформаційної безпеки, виявлених вразливостях і експлойтах; щотижневого огляду вразливостей і можливих шляхів їх усунення; порад по загальних питаннях з безпеки для загалу;

– публікації офіційних виступів керівництва FBI перед профільними комітетами конгресу США з оглядом актуальних і перспективних кіберзагроз;

– публікації на сайті FBI опису різних типів кібершахрайства і порад щодо захисту від них;

– публікації на сайті FBI та сайтах партнерів інформаційно-методичних матеріалів із захисту від кіберзагроз та шахрайств.

Розглянута вище структура системи протидії кіберзлочинності FBI USA може стати вихідною моделлю при розробці концепції системи протидії кіберзлочинності для правоохоронних органів України.

Список використаних джерел:

1. The Federal Bureau of Investigation [Електронний ресурс]. – Режим доступу до сайту: http://www.fbi.gov.

2. The Internet Crime Complaint Center [Електронний ресурс]. – Режим доступу до сайту: http://www.ic3.gov.

3. InfraGard [Електронний ресурс]. – Режим доступу до сайту: https://www.infragard.org.

4. National Cyber-Forensics & Training Alliance [Електронний ресурс]. – Режим доступу до сайту: http://www.ncfta.net.

5. National Cyber Awareness System [Електронний ресурс]. – Режим доступу до сайту: https://www.us-cert.gov.

Одержано 07.10.2014

УДК 343.98

Руслан Юрійович СЕНЬ,
інженер відділення захисту інформації
відділу режимно-секретного та документального забезпечення
Харківського національного університету внутрішніх справ

ДОСВІД ІНОЗЕМНИХ КРАЇН У СФЕРІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

В наш час проблема інформаційної безпеки входить до найважливіших питань державних і недержавних структур і суспільства в цілому, так як інформаційні технології використовуються майже у всіх галузях. Окрім тієї шкоди що наноситься інформації шляхом незаконного доступу до неї її зміни

або знищення, інформацію можуть перетворити на серйозну загрозу державній безпеці і правам людини.

Якщо подивитися на зарубіжний досвід роботи поліції протидії злочинам у сфері кіберзлочинів з використанням інформаційних технологій забезпечується двома основними способами: внесення додаткових функцій на існуючі підрозділи або створення спеціальних підрозділів для боротьби з даним видом злочинів.

Створення підрозділів для боротьби зі злочинами у сфері кіберпростору практикується в багатьох країнах світу, таких як: Австралія, Бельгія, Білорусь, Великобританія, Данія, Естонія, Індія, Ірландія, Китай, Південна Корея, Литва, Люксембург, Макао, Малайзія, Нідерланди, Німеччина, Норвегія, ПАР, Перу, Польща, Португалія, США, Сінгапур, Словенія, Таїланд, Фінляндія, Чехія, Швейцарія, Швеція та ін.

До основних функцій цих підрозділів відноситься:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців; – розслідування кіберзлочинів та надання методичної та практичної допомоги іншим галузевим службам та правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактика з громадськістю та засобами масової інформації;

– навчання працівників поліції.

В багатьох країнах, які перераховані вище, спеціальні підрозділи протидії злочинам з використанням інформаційних технологій виконують ще додаткові функції такі як розкриття кіберзлочинів, профілактику та нагляд за телекомунікаційними послугами, експертне дослідження доказів на електронних носіях, створення відповідної бази даних зі злочинами у сфері кіберпростору та постійне її оновлення, надання допомоги банкам у захисті персональної інформації клієнтів.

В Індії підрозділи по розслідуванню кіберзлочинів можуть залучати професійних хакерів для реалізації своїх функцій.

При вчиненні кіберзлочину основна увага приділяється допомозі постраждалому у відновленні пошкодженої або втраченої інформації, вжиття всіх необхідних заходів для збереження доказів.

Ще що є дуже важливим те що в багатьох країнах створені спеціальні пункти з питань щодо протидії кіберзлочинності,

які забезпечують розслідування відповідних злочинів в багатьох країнах.

Проблема кіберзлочинності в Україні є актуальною. Але нажаль злочини в сфері кіберпростору в нашій країні тільки продовжують зростати в різних сферах нашого суспільства. З урахуванням статистики розкритих злочинів в сфері кіберпростору розкриття таких злочинів не змінюється. Проблема пояснюється тим що захист інформації в нашій країні потребує більшої підтримки та розвитку, необхідно на досвіді інших країн удосконалювати власний захист проти злочинів у цій сфері.

Одержано 28.10.2014

УДК 343.1

Тетяна Леонідівна СИРОЇД,
доктор юридичних наук, професор,
професор кафедри конституційного та міжнародного права
факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ПРАВОВА ОСНОВА МІЖНАРОДНОЇ СПІВПРАЦІ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Одним із можливих підходів щодо боротьби з кіберзлочинністю у транснаціональному аспекті і розвитку міжнародної співпраці, є вироблення і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першим документом у цій сфері стала Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р. [1] та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [2]. Прийняття цих актів ознаменувало закладення правового фундаменту у сфері захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання для держав, які не є членами Ради Європи.

Конвенція містить норми матеріального кримінального права щодо видів правопорушень, які охоплюються цим договором серед яких: незаконний доступ, нелегальне перехоплення, підробка, пов'язана з комп'ютером, шахрайство, пов'язане з комп'ютером, правопорушення, пов'язані зі змістом, правопорушення, пов'язані з порушенням авторських та суміжних

прав та ін; норми кримінально-процесуального права щодо проведення процедури розслідування та переслідування; положення щодо міжнародного співробітництва, які регламентують процедуру екстрадиції, надання взаємної правової допомоги. З метою покращення співпраці, Конвенцією передбачено створення сторонами на національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме: a) надання технічних порад; b) збереження даних відповідно до статей 29 (Термінове збереження комп'ютерних даних, які зберігаються) і 30 (Термінове розкриття збережених даних про рух інформації); та c) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних (ст. 35).

Питання боротьби з кіберзлочинністю знаходяться й у центрі уваги органів і інституцій Організації Об'єднаних Націй, зокрема: Генеральної Асамблеї (A/RES 63/195), Економічної і Соціальної Ради (рез. 2009/22), Комісії з попередження злочинності і кримінального правосуддя (док. E/CN.15/2009/15), конгресів ООН з попередження злочинності і кримінального правосуддя, які акцентують увагу на тому, що кіберзлочинність є одним з нових політичних питань у сфері попередження злочинності і кримінального правосуддя, яке потребує розробки шляхів і засобів його вирішення.

Крім того, в останні роки в різних регіонах світу було застосовано низку підходів щодо боротьби з кіберзлочинністю. Так, у 2002 р. Співдружністю націй був розроблений типовий закон про комп'ютерні та пов'язані з комп'ютерами злочинах, який має за мету удосконалення законодавчих норм держав-членів Співдружності у галузі боротьби з кіберзлочинністю і поглиблення міжнародної співпраці. За відсутності цього договору, для розвитку транскордонної співпраці у даній галузі, членам Співтовариства націй необхідно було б укласти між собою низку двосторонніх договорів, які б набагато ускладнили процедуру співпраці. Типовий закон містить положення щодо матеріальних норм кримінального права, а також процесуальні норми і положення про міжнародну співпрацю. Оскільки він має регіональну орієнтацію, положення закону стосуються тільки держав-членів Співдружності (п. 20).

Європейським Союзом також докладено зусиль по узгодженню законодавства щодо кіберзлочинності, яке діє на території держав-членів організації. Для цього були прийняті, зокрема: директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких як електронна торгівля на внутрішньому ринку; рамочне рішення Ради Європейського Союзу 2000/41/ЈНА про боротьбу з шахрайством і фальсифікацією безготівкових платіжних засобів; рамочне рішення Ради Європейського Союзу 2004/68/ЈНА про боротьбу з сексуальною експлуатацією дітей і дитячою порнографією тощо (п. 20–21) [3].

Враховуючи вищеозначене необхідно підкреслити, що боротьба з кіберзлочинністю, яка зачіпає інтереси не тільки окремих держав, групи держав, а й світового співтовариства у цілому, потребує консолідації зусиль усіх зацікавлених сторін. Враховуючи ту обставину, що сучасні технології розвиваються швидше, ніж норми, які регулюють їх застосування, необхідно постійно знаходити шляхи вирішення нових задач, частіше пов'язаних із такими сферами, як захист даних, трансграничний доступ правоохоронних служб до даних і обмін інформації між державними і приватними структурами. Успішне вирішення проблеми залежить від якісного рівня правової основи співпраці, що потребує постійного моніторингу існуючої нормативної бази, внесення змін і доповнень, розробки нових стандартів; важливим є долучення до цього процесу відповідних фахівців у сфері ай-ті технологій, правників, міжнародні інституції по боротьбі зі злочинністю, а також здійснення належної підготовки фахівців для національних підрозділів по боротьбі з кіберзлочинністю.

Список використаних джерел:

1. Конвенция о киберпреступности [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

2. Дополнительный протокол к Конвенции о киберпреступности относительно криминализации деяний расистского и ксенофобского характера, совершаемых при помощи информационных систем [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/RUS/Treaties/Html/189.htm.

3. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Сальвадор, Бразилия, 12–19 апр. 2010 г.) A/CONF.213/1 [Електронний ресурс]. – Режим доступу: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_1_-_Agenda/V1050044r.pdf.

Одержано 14.10.2014

УДК 343.985(477)

Тетяна Анатоліївна ПАЗИНИЧ,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики, судової медицини та психіатрії
факультету підготовки фахівців для підрозділів слідства
Харківського національного університету внутрішніх справ

ПРО ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У БОРОТЬБІ ІЗ КІБЕРЗЛОЧИНАМИ

Тенденція росту кількості кіберзлочинів, а також дослідження проблем, що виникають на практиці при їх розслідуванні, свідчать про недосконаліть системи взаємодії правоохоронних органів України із правоохоронними органами інших держав. На даний момент нагально необхідним є створення єдиного ефективного міжнародного механізму протидії їм.

Існуючі зараз форми міжнародної співпраці правоохоронних органів мають суттєві недоліки у зв'язку з відсутністю єдиного підходу у процедурі формування, використання доказової бази у справах про такі злочини, а також у встановленні, розшуку і притягненні винних до відповідальності.

Дослідження представленої проблематики, обговорення можливих шляхів вирішення зазначених вище проблем, дає підстави сформулювати і представити наші пропозиції щодо удосконалення існуючого механізму боротьби із транснаціональною кіберзлочинністю.

Так, вважаємо доцільним, запропонувати наступне.

Необхідно розширити завдання національного контактного пункту Управління боротьби із кіберзлочинністю МВС України (далі НКП) і покласти на його працівників обов'язок реєструвати в Єдиному реєстрі досудових розслідувань відомості про кримінальні правопорушення, про які повідомляють представники правоохоронних органів інших країн, і ініціювати початок кримінальних проваджень, якщо ці злочини мають транснаціональний характер і зачіпають інтереси нашої держави, суспільства чи окремих громадян.

Провадження повинно відбуватися в рамках спільного розслідування таких злочинів правоохоронними органами держав.

Вважаємо, що основним призначенням НКП повинна бути діяльність, що виражається у наступних формах реагування на повідомлення від правоохоронних органів іноземних держав.

1. Реєстрація відомостей про транснаціональні кіберзлочини (якщо є данні, що вказують про вчинення дій об'єктивної сторони громадянином України, на території України,

або суспільно небезпечні наслідки настали або загрожують інтересам України та її громадян) і забезпечення початку кримінального провадження в Україні по кожному такому факту.

2. Організація припинення кіберзлочину, попередження настання шкідливих наслідків, тощо (наприклад, при виявленні в мережі Інтернет дій осіб хворих на педофілію або осіб, що пропагандують ворожнечу, настрої ксенофобії, заклики до розв'язання війни, тощо).

3. Надання допомоги у розслідуванні кіберзлочинів (якщо вони не несли загрозу інтересам України) за запитами правоохоронних органів іноземних держав в рамках надання оперативної або довідкової інформації, яка не відноситься до охоронюваної законом таємниці.

4. Проведення організаційних заходів (наприклад, вручення документів і підписання їх фізичними особами, повернення викраденого майна та незаконно придбаних предметів чи цінностей).

Такий підхід не тільки не суперечить положенням Кримінального процесуального кодексу України і Положенню «Про порядок ведення Єдиного реєстру досудових розслідувань», а повністю відповідає головним його засадам.

Хотілось би акцентувати увагу на тому, що ті запити правоохоронних органів іноземних держав, в яких містяться повідомлення про вчинення злочинів, які представляють суспільну небезпеку для України і її громадян, повинні сприйматися НКП, як повідомлення про кримінальне правопорушення. Такі повідомлення повинні реєструватися і направлятися для проведення повноцінного провадження досудового слідства згідно кримінального процесуального законодавства України. Закінчуватись провадження у таких справах повинно теж відповідно загальних засад Кримінального процесуального кодексу України.

Впровадження такого порядку реагування на транснаціональні кіберзлочини правоохоронними органами України вирішить декілька внутрішніх проблем.

По-перше, слідчі, які будуть проводити комплекс необхідних слідчих (розшукових) дій, будуть не виконувати «позапланові, безпоказникові» завдання (що зараз має місце на практиці при виконанні запитів), а будуть здійснювати повноцінне провадження у таких справах. Відповідно, вони будуть мати повний спектр процесуальних повноважень, будуть зацікавленні у якості проведенні розслідування, будуть мати змогу налагоджувати особисті зв'язки у співпраці з представниками правоохоронних органів інших держав.

По-друге, слідчі ОВС будуть постійно піднімати рівень кваліфікації у розслідуванні транснаціональних злочинів в рамках міжнародного співробітництва, а не «топтатися на місці», намагаючись вирішити внутрішні проблеми співвідношення національного кримінального процесуального законодавства, міжнародного і законодавства кожної країни учасниці, що ратифікували Конвенцію РЄ «Про кіберзлочинність». Адже на даний момент дуже не вистачає нашим слідчим досвіду і кваліфікації у розслідуванні злочинів зазначеної категорії, а виконання окремих доручень по запитах про правову допомогу не дає змогу набувати їх.

По-третє, Україна буде сприйматися світовою спільнотою як повноцінний партнер у боротьбі з кіберзлочинністю, а не як «помічник» у цій справі.

Ті ж запити правоохоронних органів іноземних держав, в яких міститься прохання надати правову допомогу у справах про злочини, які не представляють суспільну небезпеку для України і її громадян, повинні сприйматися НКП саме як запити тільки про допомогу або сприяння. Саме по таких запитах завданням НКП є організація проведення окремих слідчих дій (направлених на встановлення окремих обставин злочину), організаційних заходів, надання довідкової інформації, тощо.

Одержано 01.11.2014

А 43 **Актуальні** питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Х. : Права людини, 2014. – 200 с.

ISBN 978-617-7266-01-2.

У збірнику висвітлено погляди науковців та практиків щодо правового, організаційного та кадрового забезпечення протидії кіберзлочинності, кримінально-правових, процесуальних та криміналістичних аспектів цієї протидії, використання інформаційних технологій і технічних засобів, а також міжнародний досвід протидії кіберзлочинності.

УДК [351.74:343.85](063)
ББК 67.9(4УКР)611.31я43

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Матеріали
Міжнародної науково-практичної конференції

(українською, російською та англійською мовами)

ISBN 617-7266-01-2

9 786177 266012

Відповідальний за випуск *К. Б. Левченко*
Редактор *О. В. Манжай*
Комп'ютерна верстка: *А. О. Зозуля, П. О. Білоус*

Підписано до друку 07.11.2014
Формат 60 × 84 1/16. Папір офсетний. Гарнітура Bookman Old Style
Друк офсетний. Умов. друк. арк. 11,24. Умов. фарб.-від. 12,16
Умов.-вид. арк. 12,4. Наклад 150 прим.

ТОВ «Видавництво права людини»
61002, Харків, вул. Дарвіна, 7, кв. 35
Свідоцтво Державного комітету телебачення і радіомовлення України
серія ДК № 4783 від 23.10.2014 р.

Надруковано на обладнанні Харківської правозахисної групи
61002, Харків, вул. Іванова, 27, кв. 4
http://khpg.org
http://library.khpg.org