ЗОВНІШНЯ ПОЛІТИКА ТА НАЦІОНАЛЬНА БЕЗПЕКА

УДК 343.98

О. В. ОРЛОВ, Ю. М. ОНИЩЕНКО

УЗАГАЛЬНЕННЯ МІЖНАРОДНОГО ДОСВІДУ СТВОРЕННЯ ДЕРЖАВНОЇ СИСТЕМИ ПОПЕРЕДЖЕННЯ ТА ЗАПОБІГАННЯ ЗЛОЧИНАМ У МЕРЕЖІ ІНТЕРНЕТ

***Р**озглянуто питання міжнародного досвіду державного регулювання питань боротьби зі злочинами в інтернеті. Надано пропозиції щодо створення подібних структур в Україні.*

Ключові слова: кіберзлочин, кібербезпека, загроза, інтернет, державне регулювання, програми.

***T**he subject of international practices of government regulation of crime control in the Internet has been considered. Suggestions concerning establishment of similar structures in Ukraine have been put forward.*

Key words: cybercrime, cybersecurity, threat, Internet, government regulation, programs.

На перший погляд може здатися, що всесвітню мережу стихійно заполонили інформаційні ресурси украй сумнівної якості і змісту: порнографія, сайти екстремістського характеру, спам, хакери, віруси, нарешті, різноманітні форуми та соціальні мережі, на яких можна не лише безкарно образити будь-яку людину, але і здійснювати цілеспрямовані злочинні дії, що використовують відкритість і наївність учасників цих мереж. Звичайно, проблема регулювання інтернету дуже складна, але і не помічати її держава вже не має права – занадто часто глобальна мережа безкарно використовується з протиправними цілями: порушення авторських прав, шахрайство, наклеп, образи, поширення незаконних матеріалів, може найбільш відомі, але, на жаль, ще не самі значні загрози суспільному життю.

Зрозуміло, що впливати на тих, хто бачить в інтернеті передусім знаряддя для протиправних дій, можна тільки за допомогою судових і правових механізмів. Але вони повинні бути підкріплені й необхідними програмно-технічними засобами. Так, якщо модератор сайту не відстежує інформацію з поширення дитячої порнографії, він потрапляє під карну статтю. Якщо сайт використовується з метою шахрайства, то його власник також несе карну відповідальність. Кількість можливих порушень і кількість законів, під які вони попадають, уже давно перевищує фізичні можливості людини з їх відстеження, тому необхідною стає інтеграція розкиданих законодавчих актів щодо регулювання інтернету в єдиному

документі, розробленому на підставі світового досвіду, та який би регламентував і застосування певних програмно-технічних засобів автоматичного відстеження контенту.

Державне регулювання інтернету з метою перешкоди поширенню екстремізму та порнографії – звичайна практика в усіх розвинених державах світу: США, Росії, Китаї, країнах Євросоюзу і СНД. З урахуванням масштабів інтернету стає усе менш ймовірним, що всі елементи кіберзлочинності будуть обмежені територією окремої держави. У зв'язку з цим досвід інших країн у цій сфері представляє безперечний інтерес для нашої країни.

Проблематика аналізу та попередження злочинності в інтернеті досить часто обговорюється фахівцями у сфері державного управління, інформаційних технологій та інформаційної безпеки в журналах, на семінарах круглих столах, конференціях і засобах масової інформації. Деякі аспекти міжнародного досвіду протидії злочинам у всесвітній мережі вивчали та обговорювали у своїх роботах Ю. Батурин, К. Бєляков, С. Битко М. Вертузаева, В. Голубєв, Д. Дубов, С. Кльоцкін, В. Мілашев, М. Литвинов, М. Омельяненко, А. Осипенко, Т. Тропіна, Н. Селиванова та ін.

Аналіз наукової літератури засвідчив, що при всій значущості теми розвитку боротьби зі злочинами в інтернеті у світі та Україні, вона вивчена ще не в достатньому обсязі. На даний час вітчизняними та зарубіжними вченими обговорено та опубліковано недостатньо наукових праць, які досліджують цю важливу проблематику. Зокрема, не дістала належного висвітлення політика зі створення спеціальних держаних структур попередження даного виду злочинів в Україні.

Мета статті – дослідити та проаналізувати міжнародний досвід попередження злочинності в інтернеті та створення спеціальних підрозділів з боротьби з такими злочинами, а також надати рекомендації щодо створення подібних структур у нашій державі.

Сполучені Штати Америки. Повноваження органів державної влади та правоохоронних структур щодо боротьби з кіберзлочинами у США закріплено в низці нормативно-правових актів. У квітні 2009 р. у Сенаті США був зареєстрований законопроект "Акт про кібербезпеку, 2009", який пропонує значно розширити повноваження федеральної влади у сфері безпеки комп'ютерних мереж. Він розроблений Національною розвідкою США. Цей законопроект може істотно вплинути на структуру і саму суть сучасного інтернету. У тому числі законопроектом передбачається обов'язкова ідентифікація користувачів Інтернету в інтересах безпеки держави [6].

На даний час у США боротьбою з кіберзлочинністю та злочинами в інтернеті займається декілька державних структур, серед яких відзначимо такі:

– US Cyber Command. Кібернетичне командування США (United States Cyber Command, USCYBERCOM) – підрозділ збройних сил США, що знаходиться в підпорядкуванні стратегічного командування США. Розташовано на території

військової бази Форт-Мід. Основними завданнями командування є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж США. USCYBERCOM планує, координує, об'єднує, синхронізує і проводить заходи по керівництву операціями і захисту комп'ютерних мереж міністерства оборони; готує і здійснює повний спектр військових операцій в кіберпросторі, забезпечує свободу дій США і їх союзників в кіберпросторі і перешкоджає аналогічним діям супротивника [7]. USCYBERCOM здійснює координацію і інтеграцію операцій, що проводяться, кіберпідрозділами збройних сил США, експертизу кібернетичного потенціалу міністерства оборони США і розширює можливості його дій в кіберпросторі;

– Комп'ютерна команда екстреної готовності США (United States Computer Emergency Readiness Team, US – CERT) – частина Національного відділу кіберзахисту Міністерства внутрішньої безпеки США. Створена у вересні 2003 р., US – CERT є партнером Міністерства внутрішньої безпеки США і державним і приватним сектором, призначеним для координації реагування на загрози з Інтернету. Ця установа випускає інформацію про поточні питання безпеки, уразливостях і експлойтах через National Cyber Alert System і працює з постачальниками програмного забезпечення для створення патчів (спеціальних програмних застосувань), що усувають вразливості в системах безпеки. US – CERT знаходиться у складі Федерального центру управління інцидентами уряду США і виступає координатором з питань комп'ютерної безпеки США;

– відділ комп'ютерної злочинності і інтелектуальної власності (Computer Crime and Intellectual Property Section, CCIPS) – відділ у карних справах Міністерства юстиції США з розслідування комп'ютерних злочинів (хакерство, віруси, "черв'яки") і порушення прав інтелектуальної власності. Спеціалізується в зоні пошуку і захоплення цифрових доказів у комп'ютерах і мережах. CCIPS працює з урядовими організаціями, приватним сектором, академічними установами, і іноземними організаціями.

Країни Європейської спільноти. Законодавче регулювання інтернет-простору вже давно практикується в країнах Європи, де давно усвідомили всі загрози і небезпеки, що містяться в безконтрольному використанні можливостей Інтернету різними деструктивними силами. При цьому одно з найбільш серйозних обмежень національного законодавства про комп'ютерні злочини полягає в тому, що воно не дозволяє ефективно боротися з глобальним явищем кіберзлочинності. Для вирішення цієї проблеми була розроблена Європейська конвенція про кіберзлочинність, прийнята Комітетом міністрів Ради Європи в листопаді 2001 р. [8].

Хоча в багатьох країнах Євросоюзу існують організації, які борються з кіберзлочинцями, їх кадрові і фінансові можливості сильно розрізняються. Часто повноваження таких структур досить обмежені, а засобів недостатньо. Крім того, розслідування часто проводяться лише в межах однієї країни.

У червні 2011 р. за підтримки ENISA у Брюсселі з'явився новий європейський підрозділ IT-спеціалістів – "Комп'ютерна група швидкого реагування" (CERT – Computer Emergency Response Team), яка допомагатиме боротися з новітніми комп'ютерними вірусами і виявляти слабкі місця в системі захисту інформації.

Крім того, ENISA розробляє інтернет-стратегію для Єврокомісії і проводить спільно з різними структурами ЄС семінари з кібербезпеки [3].

У січні 2014 р. відбулося офіційне відкриття Європейського центру по боротьбі з кіберзлочинністю ЕС3 (European Cybercrime Centre) в Гаазі. Завданням нової організації є надання інформаційної, оперативної і експертної підтримки розслідуванням на міжнародному і регіональному рівнях. Ця структура повинна функціонувати на базі Європолу.

Організація була сформована в рамках стратегії внутрішньої безпеки ЄС, яка була прийнята в 2011 р. Вона укомплектована новітніми технологіями для проведення розслідувань, пов'язаних з кіберзлочинністю. До складу команди ЕС3 увійшли кращі фахівці Європолу, а також академічні експерти і експерти безпеки з країн – учасниць Євросоюзу.

Одним з основних завдань ЕС3 є збір і обробка даних по кіберзлочинах, здійснених на території Європи. Крім того, структура повинна займатися експертним оцінюванням інтернет-загроз, стимулюванням інформаційного обміну, а також розробкою передових методів профілактики і розслідування кіберзлочинів. До обов'язків організації увійде і надання допомоги правоохоронним і судовим органам, і координування спільних дій зацікавлених сторін, які спрямовані на підвищення рівня безпеки в європейському кіберпросторі.

На церемонії відкриття ЕС3 відбулося підписання спільної заяви Європолу і Імміграційної і митної поліції США (Immigrations and Customs Enforcement, ICE), в якому обидві сторони заявили про готовність об'єднати сили у боротьбі з кіберзлочинністю.

На даний момент об'єкти уваги ЕС3 обмежені трьома видами злочинної діяльності в інтернеті: організоване он-лайн-шахрайство, що заподіює великий збиток фінансовим організаціям і їх клієнтам; поширення дитячої порнографії, кібератаки на ключові інфраструктури і інформаційні системи. Згідно з оцінками Європолу, останніми роками кількість махінацій з платіжними картами європейських емітентів нестримно зменшується, що обумовлено застосуванням передових технологій захисту фінансових операцій [1].

У Великій Британії боротьбою з кіберзлочинністю займається відділ по боротьбі з кіберзлочинами, що входити до складу Агентства по боротьбі з організованою злочинністю. У схваленому в 2006 р. законі про поліцію і юстицію містилися поправки до закону про неправомірне використання комп'ютерних технологій. Максимальний термін ув'язнення за правопорушення, пов'язані зі зломом сайтів урядових організацій і банків, був збільшений до 10 років. Активну

роль у протидії кіберзлочинності у Великій Британії відграє Поліцейський національний відділ по боротьбі зі злочинами у сфері високих технологій (Police National E-Crime Unit), який було створено 1 жовтня 2008 р. і який виконує координуючу функцію в боротьбі з кіберзлочинами в Великобританії та Північній Ірландії (за винятком Шотландії) [9].

У ФРН основну діяльність щодо боротьби з кіберзлочинністю здійснює Федеральна кримінальна поліція. У червні 2011 р. офіційно приступив до роботи Національний центр кіберзахисту (NCAZ). До його завдання входить своєчасне виявлення і запобігання хакерським атакам, а також координація роботи цілого ряду федеральних відомств у боротьбі з кіберзлочинністю. Нова структура працює під егідою Федерального відомства по безпеці у сфері інформаційної техніки (BSI). До роботи центру кіберзахисту підключено Федеральне відомство по охороні Конституції, Федеральне відомство по захисту населення і надзвичайним ситуаціям, а також Федеральне відомство у кримінальних справах (BKA), Федеральна розвідслужба (BND) і бундесвер [2].

У Франції 1 липня 2008 р. шляхом об'єднання двох спецслужб Центрального директорату загальної розвідки (RG) і Директорату стеження за територіями (DST) створено Головне управління внутрішньої розвідки Direction centrale du Renseignement interieur, DCRI. Однією з функцій даного управління є боротьба з кіберзлочинністю.

У Голландії в 2006 р. було створено підрозділ – "Обмін інформацією про кіберзлочинність" (NICC) як частину Національної бази по боротьбі з кіберзлочинністю, що у свою чергу є державно-приватною організацією. Першими, хто приєднався до інформаційного обміну, були фінансові служби. Це створило основу для обміну інформацією між Агентством національної поліції, Головною службою розвідки і безпеки, Урядовою групою реагування на комп'ютерні загрози, банками, і банківською асоціацією Голландії. NICC є координатором цих структур [10].

В Угорщині створено підрозділи по боротьбі з кіберзлочинами Національного бюро розслідувань поліції Угорщини, Управління по фінансовій експертизі, а також національний механізму по управлінню інцидентами – CERT – Угорщина.

У Словаччині для боротьби з кіберзлочинами на національному рівні організовано Департамент по боротьбі з кіберзлочинністю при Бюро судової і кримінальної поліції Президії Поліції Словацької Республіки.

У Румунії підрозділ по боротьбі з кіберзлочинністю було створено в Директораті з розслідування справ, пов'язаних з організованою злочинністю і тероризмом Генеральної прокуратури при Вищому касаційному суді. Спеціальний підрозділ по боротьбі з комп'ютерними злочинами здійснює свою діяльність при Генеральній інспекції поліції Румунії (Директорат по боротьбі з організованою злочинністю), починаючи з 2003 р.

Російська Федерація. Основним підрозділом по боротьбі з кіберзлочинністю та злочинами в інтернеті є Управління "К" Міністерства

внутрішніх справ Росії. Цей підрозділ здійснює боротьбу зі злочинами у сфері інформаційних технологій, а також з незаконним обігом радіоелектронних засобів і спеціальних технічних засобів. У суб'єктах Російської Федерації функціонують відповідні структурні підрозділи служби кримінальної поліції – відділи "К". Управління є одним з найзаконспірованіших підрозділів МВС Росії, входить до складу Бюро спеціальних технічних заходів Міністерства внутрішніх справ Російської Федерації. Основні функції цього підрозділу такі: боротьба з порушенням авторських і суміжних прав, виявлення незаконного проникнення в комп'ютерну мережу; боротьба з розповсюджувачами шкідливих програм, виявлення порушень правил експлуатації ЕОМ, системи ЕОМ або їх мережі, виявлення використання підроблених банківських карт; боротьба з незаконним обігом радіоелектронних і спеціальних технічних засобів, протидія шахрайським діям, що здійснюються з використанням інформаційно-телекомунікаційних мереж, включаючи інтернет [4].

Ще одною державною структурою по боротьбі зі злочинами у сфері інформаційних технологій є російський центр реагування на комп'ютерні інциденти (RU – CERT). Основне завдання центру – зниження рівня загроз інформаційної безпеки для користувачів російського сегменту інтернету. З цією метою RU – CERT сприяє російським і зарубіжним юридичним і фізичним особам при виявленні, попередженні і припиненні протиправної діяльності, що має відношення до розташованих на території Російської Федерації мережевим ресурсам.

RU – CERT здійснює збір, зберігання і обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережевих атак на території РФ.

Для реалізації поставлених завдань RU – CERT взаємодіє з провідними російськими IT-компаніями, суб'єктами оперативно-розшукової діяльності, органами державної влади і управління РФ, зарубіжними центрами реагування на комп'ютерні інциденти і іншими організаціями, що здійснюють свою діяльність в галузі комп'ютерної і інформаційної безпеки.

RU – CERT входить до складу міжнародних об'єднань CSIRT/CERT центрів (FIRST, Trusted Introducer) і офіційно в рамках цих об'єднань виконує функції контактної сторони в Російській Федерації.

Діючи в рамках нормативної правової бази РФ, RU – CERT не уповноважений займатися вирішенням питань, що знаходяться у веденні правоохоронних органів. У цих випадках необхідно звертатися в регіональні підрозділи ФСБ або МВС РФ [11].

Республіка Білорусь. Управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ (далі – МВС) Республіки Білорусь є самостійним оперативно-розшуковим підрозділом Міністерства, безпосередньо підпорядкованим першому заступникові Міністра внутрішніх справ – начальникові головного управління кримінальної міліції. Для здійснення взаємодії з іншими правоохоронними органами і організаціями застосовується умовне найменування Управління "К" МВС Республіки Білорусь.

Управління координує діяльність підрозділів головного управління кримінальної міліції МВС і органів внутрішніх справ при виявленні ними злочинів проти інформаційної безпеки.

27 лютого 2001 р. у структурі кримінальної міліції МВС з'явилося управління оперативно-організаційної роботи, у складі якого до листопада 2002 р. активно діяло спеціалізоване відділення по розкриттю злочинів у сфері високих технологій.

28 листопада 2002 р. на підставі наказу Міністра внутрішніх справ, з метою вдосконалення організації роботи названих підрозділів, в МВС було створено самостійне управління, що здійснює практичну діяльність по розкриттю злочинів у сфері високих технологій (Управління "К") [5].

Сьогодні Управління "К" складається з трьох відділів:

1) з розкриття злочинів проти інформаційної безпеки, який відповідає за розкриття і профілактика злочинів проти інформаційної безпеки;

2) з розкриття злочинів у сфері телекомунікацій займається розкриттям і профілактикою злочинів у сфері телекомунікацій;

3) комп'ютерно-технічного забезпечення підтримує роботу комп'ютерної техніки.

Таким чином, державне регулювання інтернету з метою протидії зростаючій кількості злочинів з використанням комп'ютерних технологій є загальноприйнятою практикою в багатьох державах. Для ефективної боротьби зі злочинами в інтернеті відомчих ініціатив вже недостатньо. Необхідно взяти найкраще із зарубіжного досвіду боротьби з кіберзлочинами в інтернеті. Потрібне створення повноцінного Центру по боротьбі з кіберзлочинністю, з наданням йому статусу міжвідомчої координації у сфері попередження, розкриття і розслідування загальнокримінальних кіберзлочинів.

Пропонується створення в даній організації таких структур:

– відділ боротьби зі злочинами у сфері інформаційної безпеки, займається виявленням і документуванням виготовлення і поширення спеціальних технічних засобів;

– відділ боротьби із злочинами у сфері платіжних систем;

– відділ боротьби із злочинами у сфері інтелектуальної власності;

– відділ боротьби із злочинами у сфері інформаційно-телекомунікаційних технологій;

– відділ боротьби із злочинами у сфері господарської діяльності;

– відділ міжнародної співпраці.

Література:

1. В Гааге открыт центр по борьбе с киберпреступностью ЕСЗ [Электронний ресурс]. – Режим доступа : http://www.securitylab.ru.

2. В Германии сегодня открылся Национальный центр киберзащиты [Электронний ресурс]. – Режим доступа : http://www.cybersecurity.ru.

3. Европа объявила войну интернет-гангстерам [Электронний ресурс]. – Режим доступа : http://poslezavtra.com.ua.

4. Управление_“К” [Электронний ресурс]. – Режим доступа : http://ru.wikipedia.org.

5. Управление по раскрытию преступлений в сфере высоких технологий (Управление “К”). История [Электронний ресурс]. – Режим доступа : http://mvd.gov.by/ru.

6. Cybersecurity Act of 2009 (Reported in Senate - RS) [Електронний ресурс]. – Режим доступу : http://thomas.loc.gov.

7. U.S. Department of Defense, Cyber Command Fact Sheet, 21 May / [Електронний ресурс]. – Режим доступу : http://www.stratcom.mil.

8. Convention on Cybercrime. Budapest, 23.XI.2001 [Електронний ресурс]. – Режим доступу : http://conventions.coe.int.

9. What we do. Mayor’s Office for Policing and Crime 2014 [Електронний ресурс]. – Режим доступу : http://content.met.police.uk.

10. ISAC [Електронний ресурс]. – Режим доступу : http://www.samentegencybercrime.

11. RU – CERT [Електронний ресурс]. – Режим доступу : http://www.cert.ru.

Надійшла до редколегії 31.03.2014 р.