Фесик Антон Володимирович
(Харківський національний університет внутрішніх справ)

УДК 343.97

РОЛЬ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

У статті досліджено сучасну роль органів державної влади у протидії кіберзлочинності крізь велику кількість негативних проявів (в першу чергу девіантних проявів) функціонування соціального середовища та доцільність покращення захисту від кіберзлочинності.

Ключові слова: *кіберзлочинність, безпека, суспільство, інформатизація, інформаційна безпека, глобальна мережа, законопроекти, сервер.*

В статье исследована современная роль органов государственной власти в противодействии киберпреступности сквозь большое количество негативных проявлений (в первую очередь девиантных проявлений) функционирования социальной среды и целесообразность улучшения защиты от киберпреступности.

Ключевые слова: *киберпреступность, безопасность, общество, информатизация, информационная безопасность, глобальная сеть, законопроекты, сервер.*

In the article the modern role of public authorities is investigational in counteraction of киберпреступности through plenty of negative displays(first of all девиантных displays) of functioning of social environment and expediency of improvement of protecting from киберпреступности.

Key words: *киберпреступность, safety, society, informatization, informative safety, global network, bills, server.*

Постановка проблеми. У сучасних умовах науково-технічного прогресу чітко виділяється тенденція комп'ютеризації, створення розгалужених систем обробки даних, що включають електронно-обчислювальні машини (комп'ютери) системи і комп'ютерні мережі. Комп'ютеризація охоплює практично усі сторони життя суспільства та держави в цілому, від контролю за повітряним і наземним транспортом, до вирішення проблем національної безпеки.

Постійно збільшується кількість користувачів глобальної інформаційної мережі Internet. У США їх вже 158 мільйонів осіб, в Європі – 95 млн, в Азії – 90 млн, в Латинській Америці – 14 млн, а в Африці – 3 млн. У Росії, за різними оцінками, кількість користувачів Інтернет мережі складає від 3,5 до 8 мільйонів осіб. За оцінками різних дослідницьких компаній загальна кількість користувачів Internet в Україні на початок 2012 року складає близько 4,5 мільйонів [2]. Сьогодні можна говорити, що Internet охоплює усі країни світу, оскільки із застосуванням високих технологій (використання мобільних супутникових облаштувань

зв'язку) можливе підключення до мережі Internet з будь-якої точки земної кулі. Якщо ж говорити про розгорнуту інфраструктуру, то в такому контексті Internet охоплює сьогодні більше 150 країн світу.

Саме тому метою цієї статті є дослідження сучасної ролі органів державної влади у протидії кіберзлочинності, а також стану кримінально-правового забезпечення діяльності органі внутрішніх справ у боротьбі з кібер-шахраями.

На жаль, розвиток науково-технічного прогресу пов'язаний з впровадженням сучасних інформаційних технологій, призводить до появи нових видів злочинів, зокрема, до незаконного втручання в роботу електронно-обчислювальних машин, систем і комп'ютерних мереж, розкраданню, привласненню, виявлення та копіювання комп'ютерної інформації не для загального користування, небезпечному соціальному явищу, що дістали поширену назву «комп'ютерна злочинність» і навіть «комп'ютерний тероризм». За своїм механізмом, способами здійснення та приховання ці види злочинів мають певну специфіку, характеризуються високим рівнем завуальованості, латентності та низьким рівнем розкриваності.

Відносна новизна вищевикладених злочинних посягань, з блискавичною швидкістю створюють серйозні перешкоди в роботі правоохоронних органів, що виявилися не готовими до адекватного протистояння і боротьби з новим соціально-правовим (все частіше кримінально правовим) явищем. Сьогодні проблема комп'ютерної злочинності і кібертероризму, вийшла зі сфери контролю правоохоронних органів і є серйозною державною і міжнародною проблемою, про що заявив Президент України на саміті ООН в Нью-Йорку, який проходив ще в 2000 році. У своєму виступі Президент України підкреслив, що досягнення інформаційної революції стали все частіше використовуватися правопорушниками і зловмисниками, тому доцільно було б розглянути можливість розробки міжнародної конвенції по боротьбі з комп'ютерним тероризмом.

З точки зору національної безпеки України, спостерігається небезпечна тенденція, пов'язана зі збільшенням технічної і технологічної залежності нашої держави від рівня розвитку комп'ютерних технологій. Це при тому, що вітчизняне виробництво конкурентоздатних засобів інформатизації і зв'язку практично не розвивається. Інформатизація як державних, так і комерційних структур здійснюється в основному на базі зарубіжної технології і комп'ютерної техніки. Відсутня достатня державна підтримка фундаментальних і прикладних вітчизняних досліджень у сфері попередження і боротьби з кіберзлочинністю, що

не дозволяє нашій державі на рівних входити до світової інформаційної системи.

Особливо гостро питання забезпечення інформаційної безпеки, як однією з важливих складових національної безпеки держави, визріває в контексті появи транснаціональної (трансграничною) комп'ютерної злочинності і кібертероризму.

Термін «кібертероризм» утворений з'єднанням двох слів: кіберпростір і тероризм [3]. Поняття «кіберпростір» (у науковій літературі частіше зустрічаються синоніми – «віртуальний простір» або «віртуальний світ») означає модельований за допомогою комп'ютера інформаційний простір [4, с. 10–14], у якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого накопичувального електронного засобу, спеціально призначеного для їх зберігання, обробки і передачі. Кібертероризм є серйозною соціально небезпечну загрозу для людства, порівняну з ядерною, бактеріологічною та хімічною зброєю, причому міра цієї загрози в силу своєї новизни, не до кінця ще усвідомлена та врахована. Досвід, який вже накопичений світовою спільнотою в цьому сегменті з усією очевидністю свідчить про безперечну уразливість будь-якої держави, тим паче, що кібертероризм не має державних кордонів, кібертерорист своїми діями може загрожувати інформаційним системам, розташованим практично у будь-якій точці земної поверхні. Виявити та нейтралізувати віртуального терориста складно через приховані слідів, що залишаються ним, на відміну від реального світу, де слідів в результаті певних дій залишається набагато більше. На сьогодні дещо розгубленість викликають терористичні акти пов'язані з використанням глобальної мережі Internet у правоохоронних органів.

На відміну від звичайного терориста, який для досягнення цілей використовує вибухівку або іншу зброю, кібертерорист використовує сучасні інформаційні технології, комп'ютерні системи та мережі, програмне забезпечення для несанкціонованого проникнення в комп'ютерні системи та вчинення вдалої атаки на інформаційні ресурси потерпілої сторони. В першу чергу це комп'ютерні, програмні закладки і віруси, у тому числі і мережеві, здійснюючі змінення модифікації або знищення інформації, так звані «логічні бомби», «троянські коні», програми-сніффери, а також інші види інформаційних помилок чи завдань результатом яких є суспільно небезпечні наслідки [3].

Прикладом кібертероризму може служити вбивство в 1998 році в США з використанням сучасних інформаційних технологій. Коли в одній з клінік США, у важкому стані і під охороною ФБР знаходився з вогнепальним пораненням особливо важливий свідок. Через Інтернет хакер-вбивця отримавши несанкціонований доступ до локальної мережі клініки та здолавши ряд шлюзів і захисних бар'єрів зробив переналаштування кардіостимулятора, внаслідок чого пацієнт помер.

Ще одним прикладом кібертероризму може служити найбільша вірусна атака проти підприємства «Укртелеком» 16–19 листопада 2001 року. Дії вірусу Nimda (анаграма слова «admin») серйозним чином вплинули на працездатність обчислювальної мережі «Укртелекому», яка налічувала більше 700 комп'ютерів і десятки серверів. Це привело до тимчасового відключення комп'ютерів «Укртелекому» від мережі Інтернет, а також до виведення з ладу корпоративної системи електронної пошти. Вірусом виявилися заражені сотні комп'ютерів корпоративної мережі, порушена робота ряду серверів, зокрема, порушено функціонування сервера корпоративної електронної пошти Генеральної дирекції «Укртелеком».

Резюмуючи з приводу проблеми кібертероризму, можна сміливо стверджувати, що це суспільно небезпечне явище як для усієї світової спільноти, так і для нашої держави.

Станом на сьогодні Кабінет Міністрів України схвалив законопроект № 2483, спрямований на боротьбу з кіберзлочинами. До списку злочинів, що становлять загрозу національної безпеки, влада пропонує віднести несанкціоноване втручання в роботу державних інформаційних ресурсів, пропаганди в Інтернеті культу насильства, жорстокості, порнографії і сепаратизму. Цей законопроект був розроблений МВС України з метою створення правової основи для захисту громадян в кіберпросторі. Окрім цього, у МВС України повідомляють, що в проекті закону відсутні положення, що містять ознаки дискримінації. «Ухвалення законопроекту спрямоване виключно на створення юридичного базису, як для національної системи кібернетичної безпеки, так і для формування і подальшого вдосконалення загальнодержавної системи протидії кіберзлочинності та кібертероризму», – підкреслив Міністр внутрішніх справ України Віталій Захарченко.

На сьогодні, оцінивши загальнодоступну інформацію, можна сказати, що боротьба з кіберзлочинами закінчується закриттям таких сайтів як EX.ua – за звинуваченням у поширенні контрафактної продукції, erio.com.ua – за, нібито, поширення порнографії. Іноді боротьба з кіберзлочинністю доходить навіть

до вилучення серверів у місцевих провайдерів без яких-небудь пояснень.

Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 від 23 листопада 2001 року класифікує злочини у сфері інформаційних технологій (кіберзлочини) на чотири групи. У **першу групу** злочинів, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, входять: незаконний доступ, незаконне перехоплення, дія на комп'ютерні дані (протиправне умисне ушкодження, видалення, погіршення якості, зміна або блокування комп'ютерних даних) або системи. До **другої групи** входять злочини, пов'язані з використанням комп'ютерних засобів. **Третю групу** складає виробництво(з метою поширення через комп'ютерну систему), пропозиція та(чи) надання в користування, поширення і придбання дитячої порнографії. **Четверту групу** складають злочини, пов'язані з порушенням авторського права і суміжних прав.

На даний момент в Україні кіберзлочинами вважаються злочини проти інформаційної безпеки (передбачені розділом XVI Кримінального Кодексу України), злочини у сфері використання платіжних карток, злочини у сфері телекомунікацій загальнокримінального характеру (шахрайство, поширення наркотиків, зброї за допомогою телекомунікаційних технологій і так далі), злочини у сфері обороту протиправного контенту та злочини у сфері господарської діяльності й електронної комерції (ігровий бізнес, нелегальна діяльність фінансових пірамід, збування не ліцензованої програмної продукції тощо [4, с. 10–14].

Отримати статистичні дані з більшості таких злочинів практично неможливо. У МВС України це пояснюють відсутністю законодавчої бази, що окремо визначає поняття «кіберзлочину». Тільки повідомляється, що за останній рік кіберзлочинці часто проявляли себе у сфері «…незаконного поширення письмових творів, зображень, що пропагують культ насильства і жорстокості, що носять порнографічний характер; шкідливого програмного забезпечення, використовуваного зловмисниками для крадіжки інформації, необхідної для автоматизації користувачів при здійсненні платіжних операцій, електронного банкінгу, доступу до електронних поштових скриньок, персональних сторіночок в соціальних мережах, адміністративних панелей веб-ресурсів».

Минулого року в представленому Pricewaterhousecoopers огляді економічних злочинів значилося, що кіберзлочинність стала одним з п'яти найпоширеніших економічних злочинів в України.

Як суспільство, так і влада опинилися в ситуації вибору між двома полюсами державної політики у сфері контролю над глобальною мережею Internet, іменованими політикою «Мережевого захисту» і «захисту інформації».

Як показує практика, українська влада більше тяжіє до другої моделі. Чого варта тільки нещодавно зареєстрована реінкарнація законопроекту № 6523 про «захист» авторського права (проект закону № 0902). Цей документ фактично створює можливості для введення цензури в інформаційному просторі країни. Понад усе від цього постраждають незалежні Internet-ЗМІ. Згодом, особи, які нелегально поширюють контент, повинні будуть нести адміністративну та кримінальну відповідальність. Але, найцікавіше, що посилення відповідальності торкнеться не лише конкретних осіб – розповсюджувачів, але і провайдерів телекомунікаційних послуг, власників сайтів, хостинг-провайдерів, за допомогою ресурсів яких поширюється небажана інформація.

Окрім цього Україна підтримала членів Міжнародного союзу електрозв'язку на конференції в створенні нової стратегії боротьби з Internet-піратством. На конференції в Дубай був прийнятий новий стандарт технології Deep Packet Inpection (DPI), що дозволяє управляти трафіком в мережах зв'язку, який набуде чинності у 2015 році. Основна функція DPI – управління інтернет-трафіком, вона дає можливість операторові встановлювати принципи тарифікації, управляти стискуванням трафіку.

Після прийняття відповідних законодавчих змін, у тому числі і законопроекту, що визначає відповідальність за пропаганду в Інтернеті культу насильства, жорстокості, порнографії та сепаратизму, свобода слова в мережі Internet може стати прерогативою влади.

На сьогодні в Російській Федерації однієї з головних причин закриття веб-ресурсів і притягнення до відповідальності користувачів являється поширення інформації порнографічного або екстремістського характеру. В Україні ж боротьба з екстремізмом і антисистемною діяльністю ще не досягла масштабів сусідньої країни. Хоча експерти прогнозують посилення контролю над інформацією політичного характеру, поширюваною в мережі Internet.

Цей законопроект носить загальний декларативний характер. Але якщо проаналізувати подібні законопроекти, які подавалися народними депутатами України, то в них йшла мова про комплексну зміну законів України. Зокрема, це посилення відповідальності за кіберзлочини. Якщо згадати недавні атаки сайтів державних органів України, то подібні дії кваліфікувалися б як терористичний акт, а це покарання до 12 років позбавлення волі.

Також Міністерству оборони України планувалося надати функції планування, реалізації методів протидії й нейтралізації кіберзагроз національним інтересам України у військовій сфері. Якщо цей законопроект буде ухвалений, то для його реалізації потрібно змінювати інші нормативно-правові акти державного характеру. На жаль, проектів таких змін ще немає [4, с. 10–14].

Список використаних джерел:

1. Кримінальний кодекс України : від 5 квіт. 2001 р. № 2341-III // Офіційний вісник України. – 2001. – № 21. – Ст. 920.
2. Белоус А. Нас мало, но мы с «мышками» / Александр Белоус. [Електронний ресурс]. – Режим доступу : www.investgazeta.net.
3. Мотуз О В. «Виртуальный терроризм – реальность нашего времени» / Мотуз О В. // Журнал «Internet Zone» [Електронний ресурс]. – Режим доступу : http://www.izcity.com
4. Балюк В. Украинский сегмент сети Internet сегодня / В. Балюк // Сети и телекоммуникации. – 1999. – № 2. – С. 10–14.

Стаття надійшла до редакції 28.04.2013