І н ф о р м а ц і й н а б е з п е к а

УДК 004.738.5:343.346.8

ГОРОВА С.В., *кандидат наук із соціальних комунікацій,* старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України

ХАКЕРСЬКІ АТАКИ ЯК ЗАГРОЗА ІНФОРМАЦІЙНОМУ ПРОСТОРУ УКРАЇНИ

Анотація. *У статті розглядаються особливості прояву одного з видів кіберзлочинності – хакерства та підходи до його нейтралізації.*

Ключові слова: *інформація, хакер, кіберзлочинність, органи державної влади.*

Аннотация. *В статье рассматриваются особенности проявления одного из видов киберпреступности – хакерства и подходы к его нейтрализации.*

Ключевые слова: *информация, хакер, киберпреступность, органы государственной власти.*

Summare. *The article deals with the features of the display of one of types of cybercrime – hacking and approaches to its neutralization.*

Key words: *information, hacker, cybercrime, public authorities.*

Постановка проблеми. Внаслідок динамічного розвитку комп’ютеризації, в усіх сферах людської діяльності, інформаційних і телекомунікаційних технологій проявляються і факти негативного їх використання, що стали відомі, зокрема як хакерство. У зв’язку з цим актуалізуються проблеми протидії цьому негативному явищу. Вони знаходять своє відображення в матеріалах ЗМІ, які є джерелом узагальнення для науково-практичної роботи.

Аналіз останніх досліджень і публікацій. Розробкою питань інформаційної безпеки займаються вітчизняні та зарубіжні науковці, а саме: О.А. Баранов, В.М. Бутузов, В. Д. Гавловський, Б.А. Кормич, А.І. Марущак, В.М. Панченко, В.Г. Пилипчук, В.Б. Хлевицький, В.С. Цимбалюк, О.М. Юрченко та інші, проте сучасний стрімкий розвиток інформаційного суспільства безупинно дає новий матеріал для науково-практичних узагальнень.

Актуальність дослідження обумовлена стрімкістю розвитку інформаційних процесів у суспільстві та необхідністю реагування на негативні аспекти їх прояву.

Метою статті є аналіз фактологічного матеріалу, пов’язаного з хакерськими атаками на сайти органів державної влади, громадських організацій та інші джерела електронного інформування, і розгляд підходів до нейтралізації даного негативного явища.

Виклад основного матеріалу. Як свідчать матеріали ЗМІ, хакерська активізація в Україні розгортається. Все більш чітко проявляється її політична складова, пов’язана зі зростаючою опозиційністю до владних структур. Минулого року ворожа до влади діяльність виявилася у конкретних випадах. Найбільш помітним при цьому став випадок, датований 31 січнем минулого року, коли представники Міністерства внутрішніх справ України відреагували на протиправні дії власника файлообмінника EX.ua., пов’язані з порушенням прав на інтелектуальну власність. Варто зауважити, що спонуканням до рішучих дій правоохоронців стали також скарги зарубіжних власників інтелектуальних продуктів. Про те, що скарги ці були далеко не безпідставними свідчить

також та обставина, що на сьогодні в міжнародних рейтингах Україну віднесено до п’ятірки найбільш критичних у правовому відношенні країн-піратів інтелектуальної продукції. Таким чином, реакція правоохоронних органів: здійснення обшуків і вилучення серверів EX.ua була цілком закономірною. В той же час, вона викликала організовану відповідь хакерських структур. Веб-сайти Президента України, Уряду України, СБ України, МВС України, Національного банку України, Конституційного Суду України, Державною податкової служби України, правлячої Партії регіонів піддалися хакерським DDoS-атакам. Упродовж двох тижнів доступ до цих ресурсів був проблемним і для зовнішніх користувачів, і для співробітників відомств. Фактично, тоді хакери добилися відновлення роботи файлообмінника EX.ua.

Пізніше, в червні-липні минулого року хакери своїми атаками виявляли солідарність із захисниками української мови. У той час, коли народні депутати України обговорювали та ухвалювали проект закону України “Про основи мовної політики”, що розширює сферу використання регіональних мов, у тому числі російської, разом із державною українською, вони періодично блокували веб-сайти Верховної Ради України, Партії регіонів.

У серпні минулого року міністр юстиції України звернувся до суду з позовом про анулювання реєстрації “Інтернет-партії”. Приводом для скарги стала відсутність у неї необхідної кількості регіональних осередків. 23 січня 2013 року Окружний адміністративний суд міста Києва задовольнив даний позов. У відповідь хакери “помстилися” міністрові юстиції України. Офіційний сайт Головного управління юстиції по Київській області був зламаний хакерами. У першій половині дня 6 лютого на сторінці відомства з’явився текст наступного змісту : “Лавринович, давай, до побачення!.. Будь-які подальші наміри щодо свободи Інтернету в Україні будуть супроводжуватися агресивними атаками на основні веб-бандитські ресурси української влади”.

Політичні акції хакерів поступово урізноманітнювались. 4 лютого відбувся мітинг активістів проти заборони “Інтернет-партії” України. В акції брали участь близько ста осіб у масках Гая Фокса. Вони розмістили біля будинку Міністерства юстиції України плакати з написами: “Інтернет-партії бути!” та “Інтернет сильніший за юстицію”. Лідер партії Дмитро Голубов оголосив про початок всеукраїнської кампанії “Мін’юст без Лавриновича”.

Як свідчать заяви Дмитра Голубова, його організація не має наміру обмежуватись лише акціями, направленими проти влади в Інтернет-середовищі: “Ми будемо продовжувати нашу кампанію “Мін’юст без Лавриновича”, робитимемо усе можливе, щоб такого міністра в Україні не було”, – зазначає новий політичний лідер. При цьому, особливо на себе звертає увагу його твердження про те, що “усі акції, за які ми беремося, закінчуються успішно. Ми заблокували усі законопроекти, що були спрямовані проти Інтернету, це і “податок на Інтернет”, це і офіси для Інтернет-магазинів, це і закон про цензуру в Інтернеті. У справі з EX.ua ми також досягли позитивного результату – сервери було повернено компанії. Навіть таку велику машину, як піраміда МММ, ми знищили, як я і обіцяв, з точністю до дня. А діячам, подібним до Лавриновича, далеко до Сергія Мавроді, – таких, як він, ми просто проковтнемо як муху”.

Лідер “Інтернет-партії” декларував також наміри взяти участь у виборах мера м. Києва в 2013 році. При цьому, Д. Голубов обіцяє ефективне використання найновіших Інтернет-технологій: “Ці вибори увійдуть до світової політичної історії і будуть дуже веселими” [1].

Слід зазначити, хакерські справи набувають популярності також і на регіональному рівні. При цьому, в дискредитації органів державної влади хакери вдаються до прямого

хуліганства. Так, у м. Львові в ніч на 14 лютого хакери “зламали” офіційний сайт Головного управління МВС України у Львівській області, розмістивши на ньому гіперпосилання на веб-сторінку з інформацією про місця продажу наркотичних засобів. Реагування на дану провокацію знову ж таки було досить пасивним. У своєму коментарі начальник Відділу зв’язків з громадськістю ГУ МВС України у Львівській області Світлана Доброволська лише підтвердила факт даної події, розголошеної місцевими ЗМІ, підтвердила неправомірний доступ до інформації хакерів і повідомила про те, що дану подію внесено до Єдиного реєстру досудових розслідувань [2]. Про наслідки розслідування даної справи громадськість повідомлена не була.

У ЗМІ звертають увагу на те, що, виходячи з повідомлень у соціальних мережах і відеозвернень в Youtube, раніше “за свободу українців в Інтернеті і за українську мову” боролися хакери східноєвропейського крила міжнародної групи Anonymous. Лідер “Інтернет-партії” України Дмитро Голубов підтверджує причетність Anonymous до атак, покликаних захистити файлообмінник EX.ua та його партію, яку він називає “партією піратів”. “Хакери не люблять, коли хтось лізе в їх середовище і розповідає, що тут можна робити, а що ні. Хакери не люблять, коли людям забороняють викачувати піратську музику і фільми, й всіляко намагаються знищити свободу в Інтернеті. Вони завжди відповідають, діючи з різних куточків планети”, – заявив Д. Голубов. А ось участь Anonymous в акціях на захист української мови він категорично заперечує.

В даній позиції є своя логіка, адже, при вирішенні внутрішньополітичних питань втручання організації з міжнародним статусом є, фактично, втручанням у внутрішні справи держави. Дана обставина може дискредитувати зарубіжних покровителів Anonymous.

У той й же час, факт такого втручання досить складно встановити при наявності значної кількості активістів, опозиційно налаштованих громадян, причому з технічною освітою, в умовах недостатнього контролю за поширенням різного роду хакерських програм. І, як підкреслив провідний експерт з антивірусних програм російської “Лабораторії Касперського” Віталій Камлюк, “у цьому сенсі Україна, як і багато інших країн світу, не залишилася осторонь від антиглобалістського руху хакерів-активістів, яскравими представниками якого є група Anonymous”.

Звертає на себе увагу ще одна думка, висловлена В. Камлюком про те, що поряд із хакерами-правопорушниками, що вправляються у злочинних заробітках за допомогою Інтернет-технологій, в українському інформаційному просторі набувають ваги хакери-політики. “У них є тверда політична позиція. Вони зацікавлені в тому, щоб дістати цінну інформацію, опублікувати її разом з політичним повідомленням або висловити протест у вигляді атаки, що виводить з ладу устаткування серверів, знову-таки, з політичним підтекстом”, – говорить експерт “Лабораторії Касперського”. Цю категорію політиків правомірно називати хакерською, оскільки, вона активно використовує Інтернет-технології з порушенням діючого законодавства.

Слід підкреслити, що демонстративна опозиційність хакерського співтовариства активно вітається з опозиційними партіями у Верховній Раді України. Так, на думку народного депутата партії Юлії Тимошенко “Батьківщина” Андрія Шевченка, Інтернет в Україні є опозиційним за визначенням. Він прогнозує, що кількість “віртуальних реакцій на дії влади” буде зростати.

Звертає на себе увагу відображення у ЗМІ того факту, що в структурах Міністерства внутрішніх справ України набуває чіткості уявлення про небезпеку розвитку хакерських тенденцій в українському інформаційному просторі. Характерним при цьому є тиражування рядом видань позиції начальника Управління по боротьбі з

кіберзлочинністю МВС України М. Литвинова, який наполегливо пропонує врегулювати питання контролю за Інтернетом і зниження технічної анонімності. Головна умова повноцінної свободи слова полягає якраз не в тому, щоб анонімно висловлюватися, а навпаки, заявити свою точку зору без ризику переслідування за це. Але в цілому питання контролю за Інтернет-простором настільки непросте, що його до кінця не вирішила жодна країна, хоча у багатьох з них Інтернет вже став об’єктом державного регулювання, що одночасно урівноважується контролем з боку громадськості. М. Литвинов вважає цей варіант найбільш прийнятним і для України.

Спеціалісти з проблем захисту інформації в автоматизованих системах України протягом останнього десятиріччя працюють над розвитком вітчизняної бази наукового забезпечення вирішення наявних проблем, у тому числі хакерських, систематизації ризиків, рівнів актуалізації й протидії, розробки організаційно-правових аспектів їх нейтралізації [3, с. 18-27].

При цьому, слід звернути увагу на те, що позиція кваліфікованих спеціалістів МВС України з даного питання була викладена в законопроекті, розробленому Міністерством внутрішніх справ України на виконання доручень Кабінету Міністрів України відповідно до рішення Ради національної безпеки і оборони України від 25 травня 2012 року “Про заходи щодо посилення боротьби з тероризмом в Україні” та схваленому Кабінетом Міністрів України у березні 2013 року.

Вказаний законопроект спрямований на формування засад державної політики у сфері забезпечення кібернетичної безпеки України шляхом визначення головних реальних і потенційних загроз національній безпеці кібернетичного характеру, основних напрямів державної політики та основних функцій суб’єктів забезпечення національної безпеки в цій сфері.

У законопроекті, зокрема, обумовлюється введення таких основоположних понять, як “кібернетична безпека (кібербезпека)” та “кібернетичний простір (кіберпростір)”.

Фахівці вважають, що прийняття законопроекту закладе правову основу для подальшої нормотворчої діяльності на законодавчому та підзаконному рівнях, спрямованої на створення та вдосконалення національної системи кібернетичної безпеки, протидії кібернетичній злочинності тощо [4].

Дуже важливим у зв’язку з цим є утвердження активного, наступального впливу на злочинність, спрямованого на зміну її як кількісних, так і якісних показників. “Протидію комп’ютерній злочинності слід розглядати як системну діяльність правоохоронних органів, спрямовану на забезпечення безпеки життєво важливих інтересів особи, суспільства, держави від злочинних посягань у сфері комп’ютеризованої обробки інформації, що характеризується активним протистоянням комп’ютерній злочинності та виражається у виявленні, попередженні, припиненні, розкритті та розслідуванні конкретних злочинів такого виду, виявленні та усуненні причин і умов, що сприяють їх учиненню, а також притягненні до кримінальної відповідальності осіб, винних у вчиненні цих злочинів” [5, с. 350].

Нейтралізації нових кіберзагроз має сприяти також виведення на сучасний рівень розшукової, контррозвідувальної та розвідувальної діяльності як державній спеціальній діяльності правоохоронних органів в Інтернет-середовищі. Вдосконаленню даної роботи має сприяти Закон України “Про державну спеціальну діяльність правоохоронних органів”, проект якого підготовлено та подано до Верховної Ради України [6].

Вдосконалення нормативної бази з питань боротьби з кіберзлочинністю актуалізується також і у зв’язку зі зростанням зовнішніх кіберзагроз для інформаційного простору України. Вони пов’язані з появою принципово нового вірусу MiniDuke.

Експерти російської “Лабораторії Касперського” та угорської CrySys Lab, фірм, що його ідентифікували, вважають, що нова шкідлива програма об’єднує старі можливості вірусів з новими досягненнями Adobe Reader по збору геополітичних даних із високопоставлених джерел. “Це дуже незвичайна кібератака. Я пам’ятаю, якось бачив подібні комп'ютерні програми у кінці дев’яностих і початку двохтисячних, – говорить Євгеній Касперський – засновник і глава “Лабораторії Касперського”. – Я здивований тим, що ці види вірусів, що знаходилися у сплячці більше десятиліття, раптом прокинулися і приєдналися до групи нових, більш просунутих і активних комп'ютерних вірусів, що знаходяться в кіберпросторі”.

Є. Касперський також сказав, що MiniDuke дуже добре маскується, написаний на асемблері (мова програмування) і дуже невеликий за розміром – 20 кб. На його думку, саме цей вірус використовувався для комп’ютерних атак на урядові мережі України, Бельгії, Португалії, Румунії, Чехії й Ірландії, а також на два аналітичні центри і центр, що надає медичні послуги в США.

Даний вірус ще повністю не розкрив своїх можливостей. Він залишається націленим на комп’ютерні мережі державних установ України, Бельгії, Португалії, Румунії, Чехії й Ірландії. При розгляді новітніх кіберзагроз слід звернути увагу на ще одну обставину: даний вид небезпек, у силу їх технологічної своєрідності, не ідентифікується, як правило, за географічним принципом. У зв’язку з цим, звертає на себе увагу те, що провідний німецький оператор зв’язку Deutsche Telekom візуалізував карту країн-джерел кібератак, на якій Україна опинилася на 4 місці після Росії, Тайваню та Німеччини. За останній місяць з українських серверів було скоєно 566 531 атак [7].

Зростаючий вплив кіберзлочинності на життя різних країн світу обумовлює усвідомлення цієї загрози у глобальному вимірі. Виходячи з того, що “кібервійни” – тема досить актуальна сьогодні у багатьох країнах, у світі, досить правильним і стимулюючим виглядає рішення американської влади нагороджувати медаллю солдатів армії, що беруть участь у кібервійнах і проявили себе на службі. Про установу нової нагороди повідомляється на офіційному сайті Міністерства оборони США.

“Поява нової нагороди говорить про зміни принципів військових дій”, – підкреслив генерал американської армії Мартін Демпсі (Martin Dempsey), голова комітету начальників штабів при Міністрові оборони. З розвитком технологій кібернападу наступний “Перл-Харбор” може статися у віртуальному просторі, вважає колишний Міністр оборони США Леон Панетта.

У Deutsche Telekom підтверджують, що число Інтернет-загроз постійно зростає – щодня виявляють близько 200 тис. нових зразків шкідників. Тільки у пастках Deutsche Telekom збираються записи про 450 тис. атак на день.

Висновки.

Аналіз ситуації дає підстави для констатації декількох серйозних проблем.

По-перше, в експертному середовищі існує точка зору про те, що Інтернет-співтовариство в Україні повністю опозиційне нинішній владі. Ця ситуація небезпечна і, як вже писалося раніше, вимагає реагування;

По-друге, наведені приклади несанкціонованих дій, спрямованих на державні й інші інформаційні ресурси в країні, є у своїй сукупності важливим питанням національної інформаційної безпеки. У зв’язку з цим представляються необхідним посилення контролю за виконанням чинного законодавства і вдосконалення законодавчого забезпечення у сфері функціонування Інтернет-ресурсів.

По-третє, міжнародне співтовариство звинувачує Україну (не розділяючи правослухняних громадян і зловмисників) в інтелектуальному піратстві. Нині ці

звинувачення доки існують на декларативному рівні, проте, за ними прослідують санкції. Враховуючи, що на заході проблемам інтелектуальної власності приділяється дуже велика увага, ці санкції будуть відчутними. Тому важливим завданням для законодавчої влади в Україні є необхідність прискореної роботи щодо рішення проблем захисту інтелектуальної власності в інформаційній сфері.

Використана література

1. Князев К. Голубов : “Таких, как Лавринович, мы просто проглотим”. – Режим доступа : //www.proit.com.ua/article/gosregulation/2013/02/13/165322.html

2. Хакеры разместили рекламу наркотиков на сайте областной милиции. – Режим доступа : //www.expert.org.ua/statias/?st=2&id=104657

3. Голубєв В.О. Проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій : навч. посіб. / Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. ; за заг. ред. д-ра юрид. наук, проф. Р.А. Калюжного. – 2002. – С. 18-27.

4. – Режим доступу : //www.kmu.gov.ua/control/uk/publish/article?art_id=246124630

5. Бутузов В.М. Протидія комп’ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В.М. Бутузов. – К. : КИТ, 2010. – 350 с.

6. Юрченко О.М. Щодо поняття спеціальної діяльності правоохоронних органів під час проведення гласних, негласних слідчих (розшукових) дій / О.М. Юрченко, І.В. Сервецький // Часопис Нац. ун-ту “Острозька академія”. Серія “Право”. – 2012. – № 2 (6). – Режим доступу : //www.lj.oa.edu.ua/articles/2012/n2/12yomsrd.pdf

7. Україна потрапила у п’ятірку країн-джерел кібератак. – Режим доступу : //www.ua.for-ua.com/ukraine/2013/03/09/121734.html

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~