вірусу Stuxnet дійсно могла створити небезпеку для життя працівників ядерних об'єктів. Але без добровільного зізнання про політичні мотиви організаторів дану дію вкрай складно класифікувати як кібертероризм, швидше, як кібердиверсію [5].

Список використаних джерел:

1. Степко О. М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ*. Сер. : Економіка, право, політологія, туризм. 2011. Вип. 1(3). С.90-99.
2. Крутских А. В. Война или мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности (сборник статей); под ред. В. П. Шерстюка. М.: МЦНМО, 2004. С.85-96.
3. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism : USA PATRIOT ACT. 2001. URL: http://frwebgate.access.gpo.gov (дата звернення: 13.10.2017).
4. Critical Infrastructure Resilience Strategy / Australian Government URL: http://www.tisn.gov.au/. (дата звернення: 13.10.2017).
5. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. К .: НІСД, 2011. 30 с.

Одержано 30.10.2017

УДК 004.056.5:343.34

Єлизавета Георгіївна БЄЛЯЄВА,
курсант 2-го курсу факультету № 4 Харківського національного університету внутрішніх справ

Олексій Михайлович РВАЧОВ,
старший викладач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВІРУСИ-ШИФРУВАЛЬНИКИ, ЯК ГОЛОВНА ЗБРОЯ КІБЕРТЕРОРИСТІВ

Проблема поширення світом кібертероризму з кожним роком набуває все більшого значення, а отже питання протидії кібертероризму стає ще більш актуальнішим. Кібератаки складають велику загрозу, як суто національній, так і міжнародній безпеці країн.

На теперішній час в законодавстві України визначення поняття «кібертероризм» не наведено в жодному з нормативно-правових документів, хоча цей термін і вживається в деяких нормативних документах та законодавчих актах.

В Законі України «Про боротьбу з тероризмом» від 20.03.2003 дане визначення терміну «технологічний тероризм – злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру» [1].

З цього визначення можна припустити, що технологічний тероризм включає в себе й так званий кібертероризм.

Цілями для кібертероризму є: незаконне втручання в роботу комп'ютерних систем і отримання доступу до особистої та банківської інформації, військовим та державним конфіденційним даним; виведення з ладу обладнання та програмного забезпечення, створення перешкод, порушення мереж електроживлення; крадіжка цифрових даних; витік секретної інформації у відкритий доступ; поширення дезінформації за допомогою захоплених каналів засобів масової інформації; порушення роботи каналів зв'язку [2].

Найпопулярнішим методом кібертероризму є ураження комп'ютерних систем та пристроїв шкідливим програмним забезпеченням шляхом використання: вразливостей операційних систем та програмного забезпечення; методів соціального інжинірінгу; незаконне втручання в роботу популярних інформаційних ресурсів (вебсайти та сервери оновлення для програмних продуктів).

В ст. 361-1 Кримінального Кодексу України використовується термін «шкідливі програмні засоби», але в національному законодавстві не наведено визначення цього терміну [3]. За результатами аналізу визначень цього терміну від провідних антивірусних компанії, можна сформулювати наступне визначення: «шкідливе програмне забезпечення – це програма, яка була навмисно створена для виконання несанкціонованих, часто шкідливих дій, на електронному пристрою без відома його власника» [4, 5].

Виділяють кілька типів шкідливого програмного забезпечення: шпигунські, рекламні, фішингові, троянські, здирниць-

кі програми, віруси, черв'яки, руткіти та програми, націлені на захоплення контролю над браузером [5].

До одних з наймасштабніших кібертеракт 2017 року, на теперішній час, можна віднести ураження соціального, економічного та державного секторів шкідливим програмним забезпеченням з сімейства «Petya». А за цей рік ще стали відомими такі віруси як «WannaCry», «EternalRocks» (також відомий як MicroBotMassiveNet).

Події, які сталися у червні 2017 року показали світу усю небезпечність вірусів-шифрувальщиків та незахищеність комп'ютерів користувачів. Вірусні атаки торкнулися соціального сектору, енергетичних компаній, державних інтернет-ресурсів та локальних мереж, укрмедіа та ряд інших великих підприємств, що в результаті призвело до величезних збитків. Станом на 28 червня 2017 року вірус заразив 12 500 ПК у 64 країнах світу.

Як встановили спеціалісти, зараження вірусом відбувалося через оновлення української програмного забезпечення для подачі бухгалтерської звітності «M.E.Doc», а також під час відкриття користувачами фішингових листів електронної пошти, що містили файли із вірусом.

Після свого запуску вірус шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує і шифрує головний завантажувальний запис (MBR) – дані, необхідні для завантаження операційної системи і проводить перезавантаження комп'ютер, та під виглядом перевірки жорсткого диску починає шифрувати файли на ньому. В результаті всі файли, що зберігаються на комп'ютері, стають недоступними. Потім програма вимагає грошовий викуп у біткоїнах за розшифровку і відновлення доступу до файлів.

Систему можливо запустити навіть після її компрометації, якщо встигнути запустити команду «bootrec/fixMbr» для відновлення MBR, а також працездатності ОС. Але розшифрувати файли вже не вдасться («зловред» шифрує файли максимум на 15 піддиректорії, тобто файли вкладені на більшу глибину, знаходяться в безпеці).

Експерти «Positive Technologies» виявли «kill-switch» – можливість локально вимкнути шифрувальщик. Для запобігання зараженню треба зробити вигляд наче комп'ютер вже є зараженим. Якщо процес має адміністративні привілегії ОС, то перед підміною MBR шифровальщик перевіряє наявність файлу «perfc» без розширення в директорії «C:\Windows\». Для захис-

ту лише потрібно створити файл під назвою «perfc.dll» та зробити його доступним лише для читання аби вірус не зміг внести в нього будь-які зміни. Наявність такого файлу в директорії може бути одним з індикаторів компрометації. Якщо файл у наявності в даній директорії, то процес виконання вірусного програмного забезпечення завершується таким чином.

Але найпростішим способом не дати вірусу поширити шкідливий код це заблокувати у фаєрволі операційній системи доступ до 135, 139, 445 TCP-портів, саме які він використовує для свого розповсюдження [6].

Президент компанії «InfoWatch» Наталія Касперська вважає, що останні вірусні атаки, в тому числі атака вірусу-шифрувальника «Bad Rabbit», організовані з метою кібертероризму, а не заробітку [7]. Ми згодні з даною думкою.

На сьогодні в України існує потреба чіткого визначення на законодавчому рівні значень таких термінів як «кібертероризм» та «шкідливе програмне забезпечення».

Список використаних джерел:

1. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV, редакція від 07.05.2017. URL: http://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 25.10.2017).
2. Угрозы информационной безопасности. Кибервойны. Кибертерроризм // Аналитический центр «Anti-Malware.ru». URL: https://www.anti-malware.ru/threats/cyberterrorism (дата звернення: 25.10.2017).
3. Кримінальний Кодекс України: Закон України від 05.04.2001 № 2341-III, редакція від 03.09.2017 // База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 26.10.2017).
4. Вредоносная программа // Энциклопедия / АО «Лаборатория Касперского». URL: https://securelist.ru/threats/malware-glossary/ (дата звернення: 26.10.2017).
5. Что такое вредоносная программа и как от нее избавиться // Компания AVAST Software. URL: https://www.avast.ru/c-malware (дата звернення: 28.10.2017).
6. Как победить вирус Petya // Хабрахабр / Компания «Positive Technologies». 28 июня 2017 года. URL: https://habrahabr.ru/company/ pt/blog/331858/ (дата звернення: 25.10.2017).
7. Наталья Касперская о последних вирусных атаках: «Это кибертерроризм в чистом виде» // «БИЗНЕС Online»: Деловая электронная газета Татарстана. 26 октября 2017 года. URL:

https://www.business-gazeta.ru/news/362049 (дата звернення: 27.10.2017).

Одержано 30.10.2017

УДК 004.93

Владислав Вячеславович БОРОДАВКА,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

Михайло Віталійович ЦУРАНОВ,
старший викладач кафедри комп'ютерних систем та мереж Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

ВИКОРИСТАННЯ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ ДО LINUX СЕРВЕРІВ ДЛЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

З розвитком інформаційних технологій все більша кількість сервісів переноситься на хмарні платформи і використовує технологію клієнт-сервер для забезпечення безпечної обробки і зберігання даних. Для забезпечення контролю доступу до серверів і серверних приміщень використовуються різні СКУД (Системи контролю управлінням доступом). У цих системах використовуються різні токени для автентифікації користувачів: RFID мітки, смарт-карти, uaTocken і т.д.

Останнім часом все більшого поширення в СКУД отримують системи біометричної автентифікації (БА) користувача. Системи БА – системи, що використовують для ідентифікації особи людей їх біометричні дані [1]. Біометрія передбачає систему розпізнавання людей по одній або кільком фізичним, або поведінковим характеристикам людини. В даний час методи БА стали більш досконалими, а надійна авторизація та автентифікація стають важливими атрибутами повсякденного життя [2, с. 18]. Широке застосування біометричних технологій (БТ) призводить до появи принципово нових видів загроз. Зараз БТ трансформувалися в повноцінний компонент систем захисту, інтеграція яких вимагає продуманого підходу.

Стрімкий розвиток технології клієнт-сервер призвело до виникнення значної кількості нових загроз, багато з яких отримали подальший розвиток в середовищі ОС Linux. Це стало можливим в результаті того, що Linux використовується в якості серверної ОС і за даними компанії Netcraft на вересень 2017 року, вісім з десяти найбільш надійних інтернет-