УДК 343.98

О.А. Парфило, *кандидат юридичних наук, старший науковий співробітник, начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України*

Ю.Ю. Нізовцев, *головний спеціаліст (експерт) Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України*

АКТУАЛЬНІ ПИТАННЯ СУДОВО-ЕКСПЕРТНОГО ДОСЛІДЖЕННЯ ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ У МЕЖАХ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

Розглянуто критерії віднесення програмного забезпечення до шкідливого, наведено класифікацію програмних засобів, які можуть бути використані для завдання шкоди, та приклади застосування шкідливих програмних засобів як знаряддя злочину.

Ключові слова: шкідливе програмне забезпечення, комп'ютерно-технічна експертиза, несанкціоноване втручання в роботу інформаційно-телекомунікаційних систем, кібертероризм, кібердиверсія.

Рассмотрены критерии отнесения программного обеспечения к вредоносному, представлена классификация программных средств, которые могут быть использованы для причинения вреда, приведены примеры применения вредоносных программных средств в качестве орудия преступления.

The criteria for classifying malicious software, presents the classification of software that can be used for harm, are examples of Malware as an instrument of crime.

Загальновідомо, що несанкціонований доступ до інформаційних ресурсів можливий за умови їх недостатньої захищеності і здатний спричинити глобальні катастрофи. Однак альтернативи розвитку інформаційно-телекомунікаційних систем і, як наслідок, систем інформаційної безпеки не існує.

Сьогодні кіберзлочинці мають змогу атакувати організації та приватних осіб за допомогою шкідливих програмних засобів (далі — ШПЗ) і анонімізації, що дозволяє обійти наявні заходи безпеки. Їх атаки стають регулярнішими, складнішими і витонченішими. Дедалі частіше ці атаки виявляють після їх здійснення (якщо взагалі виявляють). Наявні системи виявлення проникнень, бази даних ШПЗ та антивірусні програми не в змозі забезпечити потрібний рівень захисту і занадто швидко втрачають актуальність.

Різним аспектам боротьби з кіберзлочинністю, у тому числі розслідуванню злочинів, пов'язаних з використанням ШПЗ, присвятили свої праці Ю.В. Гаврилін, В.А. Голубєв, С.М. Гусаров, В.О. Вітюк, О.П. Войтович, В.А. Каплун, В.В. Крилов, Л.М. Соловйов, Т.Л. Тропіна, В.С. Цимбалюк та інші вчені. Однак питання визначення понятійного апарату у цій сфері досліджено не повною мірою.

Упровадження методів електронного управління технологічними процесами створює умови для появи принципово нових видів кіберзлочинності — кібердиверсії та кібертероризму, загальна суть яких полягає у несанкціонованому втручанні в роботу компонентів інформаційно-телекомунікаційних мереж, під управлінням яких функціонують критично важливі елементи інфраструктури держави. Спричинена втручанням несанкціонована модифікація комп'ютерних даних може зумовити дезорганізацію роботи зазначених інфраструктурних елементів і цим створити небезпеку загибелі людей, завдання значної майнової шкоди чи спричинення інших суспільно небезпечних наслідків [1].

Актуальність дослідження та вирішення проблеми, про яку йдеться, зумовлені тим, що у разі отримання зловмисниками (а це можуть бути як терористи, так і спецслужби іноземних держав) доступу до комп'ютерних мереж у них з'являється можливість доволі ефективно виводити з ладу системи керування та зв'язку державних установ та організацій, дестабілізувати роботу фінансових ринків і стратегічних об'єктів життєзабезпечення. Сучасні комп'ютерні технології стають ідеальним засобом для вчинення особливо небезпечних кіберзлочинів, які створюють загрозу для всього людства, що виводить питання інформаційної безпеки за національні межі, і воно набуває міжнародного значення.

Одним із найбільш широко відомих прикладів несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем, який більшість спеціалістів з інформаційної безпеки кваліфікують як прояв кібердиверсії, є результат дії вірусу Stuxnet, що у вересні 2010 року успішно вразив значну кількість центрифуг на заводі зі збагачення урану в Натанзі, а також зірвав терміни запуску ядерної АЕС в м. Бушері. Збитки, заподіяні ядерним об'єктам Ірану, фахівці порівнюють зі збитками від атаки ізраїльських військово-повітряних сил [2].

Загроза кібератак є не менш актуальною і для України. Так, 23 грудня 2015 року через стороннє втручання в роботу об'єктів вітчизняної енергосистеми частково без електропостачання залишилася Івано-Франківська область (загалом 80 тис. домогосподарств) [3]. Служба безпеки України повідомила про виявлення шкідливого програмного забезпечення в комп'ютерних мережах окремих обленерго («Прикарпаттяобленерго», «Київобленерго» та «Чернівціобленерго»), звинувативши в його розповсюдженні російські спецслужби [4]. Пізніше до розслідування підключилися експерти урядових установ США (Держдепартамент, Міністерство енергетики, Міністерство національної безпеки та ФБР), які підтвердили причетність РФ до зазначеної інформаційної атаки [5]. Було встановлено, що для атаки застосовували шкідливе програмне забезпечення «BlackEnergy», а саму атаку здійснювала російська хакерська група, відома під назвою «Sandworm». Кібератака складалася з п'яти елементів [6]:

– зараження мереж за допомогою підроблених листів;

– захоплення управління автоматизованою системою диспетчерського управління з вимиканнями на підстанціях;

– виведення з ладу мереж безперебійного живлення, модемів, комутаторів та іншої IT-інфраструктури;

– знищення інформації на серверах і робочих станціях (утилітою «KillDisk»);

– атака на телефонні номери колл-центрів (з російських номерів) з метою відмови від обслуговування знеструмлених абонентів.

І така атака не єдина. У січні 2016 року ШПЗ було виявлено в комп'ютерній мережі аеропорту «Бориспіль», до якої входить і управління повітряним рухом аеропорту [7].

Крім того, команда реагування на комп'ютерні надзвичайні події України (CERT-UA) регулярно виявляє цільові атаки як на державні органи влади України, так і на неурядові організації [8], що здійснюють також із застосуванням вже зазначених ШПЗ «BlackEnergy». У зв'язку з цим команда CERT-UA попередила системних адміністраторів про можливу небезпеку [9].

Отже, ШПЗ є одним із дієвих засобів для ефективного втручання в роботу інформаційно-телекомунікаційних систем, а саме кібердиверсії чи кібертероризму. Водночас у Кримінальному кодексі України (далі — КК України) термін «шкідливий програмний засіб» детально не визначено. Стаття 3611 КК України передбачає покарання за «створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». Тому як предмет таких злочинів комп'ютерні програми (програмні засоби) мають бути шкідливими — здатними забезпечити несанкціоноване порушення конфіденційності, доступності, цілісності інформації, яка обробляється автоматизованою системою або передається мережами електрозв'язку [10].

Під час розслідування злочину, передбаченого ст. 3611 КК України, слідчий зазвичай призначає комп'ютерно-технічну експертизу, на вирішення якої ставить питання щодо належності виявлених програм до ШПЗ. Проте відсутність чіткого визначення терміна «шкідливий програмний засіб» має наслідком відсутність єдиного підходу до проведення таких експертиз. У кожному випадку судовий експерт вимушений на власний розсуд, спираючись на власні знання та досвід, визначати, які ознаки програми є суттєвими для віднесення її до ШПЗ, а які такими не можна визнати. Наслідком цього є те, що різні експерти можуть дійти різних висновків щодо тієї самої програми.

З метою визначення більш чітких критеріїв належності програмного забезпечення до шкідливого доцільно створити класифікацію програмних засобів, які можна використовувати для тих чи інших шкідливих цілей, залежно від їх початкового призначення.

До першої класифікаційної групи мають належати програмні засоби, спеціально призначені для несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем. Це, так би мовити, класичні шкідливі програмні засоби: віруси, шпигунські програми, блокувачі комп'ютера чи браузера тощо.

Друга група складається з програм подвійного призначення — програм, створених для проведення тих самих дій, що й ШПЗ, але санкціоновано. Найяскравішим прикладом таких програм є програми для тестів на проникнення (так званих пентестів, від англ. penetration test, pentest) [11].

Тест на проникнення — це докладний аналіз мережі та систем з погляду потенційного зловмисника. Суть тесту полягає в санкціонованій спробі обійти наявний комплекс засобів захисту інформаційної системи. Під час тестування роль зловмисника виконує спеціаліст, який має визначити рівень захищеності інформаційної системи, виявити вразливості, ідентифікувати найбільш ймовірні шляхи зламу і визначити, наскільки добре в установі працюють засоби виявлення та захисту цієї системи від атак зловмисників. Фактично пентест є моделюванням дій зловмисника з проникнення в інформаційну систему, який дозволяє виявити найбільше уразливостей у захисті мережі. Тобто тестування на проникнення дозволяє отримати об'єктивну оцінку того, наскільки легко отримати доступ до ресурсів корпоративної мережі і сайту компанії, в який спосіб і через які вразливі місця. Як правило, тест на проникнення проводять для отримання незалежної оцінки захищеності власної корпоративної мережі установи. Іноді (якщо це можливо і відповідає бажанню замовника) виконують показовий злам захисту системи. Тестування на проникнення можна проводити у межах аудиту на відповідність стандартам і як самостійну роботу. Про проблеми безпеки, виявлені під час тесту на проникнення, доповідають власнику системи. Ефективний тест на проникнення поєднає цю інформацію з точною оцінкою потенційного впливу на установу й окреслить межі технічних і процедурних контрзаходів для зменшення ризиків.

Ще одним типом програм, які можна віднести до другої класифікаційної групи програмних засобів, є програми контролю роботи співробітників. Такі програми забезпечують віддалений контроль дій співробітників, аналіз ефективності їхньої праці та захист інформації від витоків. Зазвичай цього досягають такими шляхами:

– зняття знімків екрану (скриншотів);
– перехоплення натискання клавіш;
– моніторинг запущених процесів;
– контроль корпоративної пошти;
– відслідковування месенджерів (Skype, ICQ, MSN тощо);
– моніторинг веб-сайтів;
– відслідковування пошукових запитів;
– контроль соціальних мереж;
– моніторинг файлів і папок;
– моніторинг буфера обміну;
– моніторинг шифрованого трафіка.

Усю зібрану інформацію надсилають для збереження та обробки або на сервер розробника програми, або на сервер установи, в якій впроваджено програму. Зазвичай співробітники мають бути попереджені про стеження за їх діями за допомогою контролюючої програми. Отже, програми контролю роботи співробітників мають функціонал доволі потужної універсальної шпигунської програми.

Третю класифікаційну групу становлять програми, створені виключно для благонадійних цілей, але які за умови певних налаштувань можна використовувати як ШПЗ. Однією з таких програм є Punto Switcher — програма, яка автоматично переключає розкладку клавіатури. Основне призначення програми — збільшення продуктивності та зручності під час роботи з комп'ютером. Працюючи у фоновому режимі, Punto Switcher проводить статистичний аналіз послідовностей символів, що складають слова, і, якщо поєднання букв виявляється нетиповим для мови, якою

вводяться символи, Punto Switcher перемикає мову введення, стирає надруковане, імітуючи натискання клавіші Backspace, і повторно вводить текст вже з правильною розкладкою клавіатури. За певних налаштувань ця, на перший погляд, зовсім невинна програма стає повноцінним клавіатурним шпигуном [12].

Ще одним прикладом третьої групи програм є утиліта ping, яка за замовченням вбудована майже в усі сучасні операційні системи та є доволі корисною для перевірки мережевого з'єднання у мережах TCP/IP. Вона надсилає запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі та фіксує відповіді (англ. Echo-Reply). Час між надсиланням запиту та одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті та частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв. Налаштування цієї утиліти на максимальне та безперервне надсилання запитів фактично розпочне атаку на відмову в обслуговуванні.

Як свідчить аналіз розглянутих трьох груп програм із суто технічного погляду, чітких критеріїв для їх розмежування немає. Наприклад, застосування програми контролю роботи співробітників передбачає попередження (зазвичай письмове із засвідченням підпису) цих співробітників про те, що за їх діями на комп'ютері ведеться стеження. Але попередження є організаційним моментом і жодним чином не відображається у програмному коді. Отже, якщо цю саму програму застосувати без повідомлення, вона функціонуватиме як звичайний ШПЗ, а саме як шпигунська програма. Мало того, деякі програми контролю роботи співробітників передбачають збереження інформації не на серверах установи, за співробітниками якої проводять спостереження, а у «хмарному» сховищі, тобто на серверах, які не підконтрольні цій установі на всі 100 %. Таким чином, отримана під час спостереження за діями співробітників конфіденційна інформація стає доступною стороннім особам і у разі встановлення такої програми на стратегічному підприємстві немає жодних гарантій, що інформація з обмеженим доступом не стане доступною спецслужбам іноземних держав.

Так само програми для тестів на проникнення кіберзлочинці доволі часто використовують для аналізу (а в окремих випадках і для подолання) системи захисту атакованої інформаційно-телекомунікаційної системи.

За результатами узагальнення судово-експертної практики доцільно розглянути випадок надання на дослідження експертові програмного коду (php-скрипт), під час аналізу якого було встановлено, що він призначений для масової розсилки електронної пошти. Така розсилка може бути цілком благонадійною у випадку, якщо відбуватиметься на замовлення або за згодою її отримувачів (це може бути розсилка певних новин або анонсів певних подій тощо). Проте така розсилка електронної пошти може бути і протизаконною, якщо відбуватиметься всупереч бажанню осіб, які її отримуватимуть (так звана розсилка спаму, від англ. spam), або якщо відбуватиметься масове надсилання листів на певний поштовий сервер з метою його блокування або уповільнення його роботи (це різновид віддаленої атаки на відмову в обслуговуванні). Оскільки зазначені дії залежать від певного способу застосування наданого на дослідження програмного коду, експерт дійшов висновку, що вважати наданий на дослідження php-скрипт ШПЗ чи заперечити його належність до ШПЗ у межах судової комп'ютерно-технічної експертизи неможливо.

На превеликий жаль, у науковій літературі також не існує єдиного підходу до визначення ШПЗ і критеріїв віднесення програм до шкідливих. Аналізуючи різні

погляди вчених, можна дійти висновку, що вони доволі часто застосовують термін «шкідливий програмний засіб», не розкриваючи його змісту, чи надають визначення окремих різновидів ШПЗ, уникаючи загального визначення цього терміна. За результатами проведеного дослідження можна надати таке визначення ШПЗ: це програма або комплекс програм, призначених для несанкціонованої (з порушенням встановленої політики безпеки) зміни режиму роботи атакованої інформаційно-телекомунікаційної системи, спрямованої на порушення порядку обробки інформації або спричинення їй збитків. Це визначення також не позбавлене недоліків з позиції застосування його в судово-експертній практиці, оскільки містить таку суттєву ознаку, як несанкціонованість. А встановлення факту несанкціонованості як правового питання заборонено експертам ст. 242 Кримінального процесуального кодексу України.

З огляду на зазначене можна констатувати, що наразі вкрай складно встановити чіткі критерії віднесення програми до ШПЗ, які були б достатніми для використання експертами під час проведення експертиз. Експерт може дослідити функціональність програмного засобу та за певних умов вказати ті з них, які характерні для ШПЗ. Остаточне ж рішення щодо належності програмного засобу до шкідливого прийматиме суд.

Підбиваючи підсумки, слід зазначити, що діяльність з протидії кібертероризму в Україні повинна мати системний і комплексний характер — ця робота має будуватися на чіткій взаємодії всіх правоохоронних органів, у тому числі й судових експертів, з упровадженням ефективних методів профілактики, виявлення та розкриття таких злочинів. Розвитку цієї діяльності сприятиме проведення відповідних наукових досліджень понятійного апарату з подальшим коригуванням законодавчих та інших нормативно-правових актів.

Список використаної літератури

1. *Голубєв В.* Кібертероризм — загроза національній безпеці та інтересам України [Електронний ресурс] / В. Голубєв // Юридичний журнал. — 2004. — № 1. — С. 132—134. — Режим доступу : http://www.justinian.com.ua/article.php?id=1002.

2. *Гольд Р.* Stuxnet: война 2.0 [Электронный ресурс] / Р. Гольд. — Режим доступа : http://habrahabr.ru/post/105964/.

3. *Після* кібератаки на «Прикарпаттяобленерго» в США переглянуть захист енергомереж [Електронний ресурс]. — Режим доступу: http://www.dw.com/uk/після-кібератаки-на-прикарпаттяобленерго-в-сша-переглянуть-захист-енергомереж/a-18964517?maca=ukr-rss-ukrnet-ukr-all-3816-xml.

4. *СБУ* попередила спробу російських спецслужб вивести з ладу об'єкти енергетики України [Електронний ресурс]. — Режим доступу : http://www.ssu.gov.ua/sbu/control/uk/publish/article?-art_id=170951&cat_id=169080.

5. *U.S. official* blames Russia for power grid attack in Ukraine [Електронний ресурс]. — Режим доступу : http://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html.

6. *В Минэнерго* рассказали подробности кибератаки РФ [Электронный ресурс]. — Режим доступа : https://inforesist.org/v-minenergo-rasskazali-podrobnosti-kiberataki-rf.

7. *Ukraine* says to review cyber defenses after airport targeted from Russia [Електронний ресурс]. — Режим доступу : http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0.

8. *Продолжаются* целевые вирусные атаки с помощью электронной почты на госорганы Украины [Электронный ресурс]. — Режим доступа : http://cert.gov.ua/?p=2357.

9. *До уваги* системних адміністраторів щодо можливих атак BlackEnergy [Електронний ресурс]. — Режим доступу : http://cert.gov.ua/?p=2464.

10. *Судова* практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс] / Офіційний веб-сайт Верховного Суду України. — Режим доступу : http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(print)/AFB1E90622E4446FC2257B7C00499C02.

11. *Тест* на проникновение (Пентест) [Электронный ресурс]. — Режим доступа : http://pentest.com.ua/.

12. *Клавиатурный* шпион или как приручить Punto Switcher! [Электронный ресурс]. — Режим доступа : http://pikabu.ru/story/klaviaturnyiy_shpion_ili_kak_priruchit_punto_switcher_1520617.