УДК 007.51

В. Б. Дудикевич, Б. М. Березюк
Національний університет "Львівська політехніка,
кафедра захисту інформації

ОСОБЛИВОСТІ ІНЦИДЕНТІВ У СУЧАСНОМУ КІБЕРНЕТИЧНОМУ ПРОСТОРІ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ СУСПІЛЬСТВА

Розглянуто вплив інформаційно-комунікаційних технологій на формування сучасного кіберпростору. Наведено класифікацію кібернетичних втручань за їх видами та проаналізовано найпоширеніші інциденти та методи кіберрозвідки. Сформульовано підходи зменшення впливу на кібербезпеку засобів соціального інжинірингу.

Ключові слова: інформаційно-комунікаційна мережа, кіберпростір, кібербезпека, інцидент, соціальні мережі, соціальний інжиніринг.

The influence of information and communication technologies on the formation of the modern cyberspace. Classification cybernetic interventions by type and analyzed the most common incidents and methods kiberrozvidky. Formulated approaches to reduce the impact of cybersecurity means of social engineering.

Key words: Information and Communications Network, cyberspace, cyber security, incident, social networks, social engineering

Вступ

Поява перших комп'ютерних мереж надала суспільству засіб для оперативного накопичення на електронних носіях різного виду інформації та її опрацювання в режимі реального часу. Новітні ІКМ різного функціонального призначення, об'єднані між собою програмно-технічними та комунікаційними засобами мережі Internet, становлять основу *інформаційного простору* (ІП) сучасного суспільства. Сьогодні всесвітня павутина (World Wide Web, WWW, web) являє собою розміщену на Web-серверах величезну за обсягом інформацію з різних видів людської діяльності, науки, техніки, природи, особистого плану та ін. Спеціальні програмні засоби пошуку та гіперпересилок дають змогу користувачам Internet оперативно отримувати за їхніми запитами потрібну інформацію.

Стрімкий розвиток інформаційних та комунікаційних технологій перетворили мережу Інтернет, яка налічує сотні мільярдів документів і охоплює декілька мільярдів користувачів, на світовий депозитарій людських знань. З часом Інтернет захопили *соціальні мережі*, які наповнили його приватною інформацією та особистими даними і почали впливати на реальне життя суспільства. Інформаційно-комунікаційні технології стали важливою складовою суспільного розвитку, змінивши значною мірою механізми функціонування багатьох суспільних та державних інститутів. Вони істотно впливають на формування сучасного інформаційного середовища і дають змогу оперативно накопичувати різноманітну тематичну інформацію, призначену для використання у системах аналізу та прийняття рішень.

Метою роботи є аналітичний огляд інцидентів у сфері кібернетичного простору та аналіз впливу кібертероризму на безпеку суспільства. Розглянуто основні аспекти використання методів соціального інжинірингу для боротьби з інцидентами, скерованими на втручання в роботу інформаційних систем.

Види інцидентів у сфері кібернетичного простору

Під *кібернетичним простором* розуміють віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та інформаційними об'єктами комунікаційних мереж всіх форм власності, яке використовується для забезпечення інформаційних потреб суспільства [1].

Суспільство, отримавши в результаті зближення інформаційних і комунікаційних технологій необмежені можливості в галузі обміну інформацією, стало надзвичайно вразливим щодо шкідливого кібернетичного впливу та різних видів загроз як на інформаційний простір, так і на свідомість людей. На перший план почали виходити проблеми *кібербезпеки*, тобто захисту кіберпростору від загрозливого втручання (*інцидентів*) у роботу інформаційно-комунікаційних мереж [2, 3].

Інциденти, які завдають шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем, згідно із запропонованою Конвенцією Ради Європи класифікацією кібернетичних втручань і загроз, поділяють на такі види [5]:

– несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, здійснений в обхід систем безпеки);

– втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розроблення та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікаційного зв'язку);

– перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних в обхід заходів безпеки);

– незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

При цьому розрізняють внутрішні і зовнішні інциденти. Під внутрішнім інцидентом розуміють подію, джерелом якої є порушник, безпосередньо пов'язаний з постраждалою інформаційною системою. Під зовнішнім інцидентом розуміють подію, джерелом якого є порушник, безпосередньо не пов'язаний з інформаційною системою. До подій такого типу належать вірусні атаки на програмне та технічне забезпечення ІКМ, атаки типу "відмова в обслуговуванні", перехоплення мережевого трафіку, неправомірний доступ до конфіденційної інформації, сканування порталу корпоративної мережі, шахрайство в системах електронного документообігу тощо [4]. Найпоширеніші такі види атак:

Відмова в обслуговуванні (*Denial of Service – DoS*) – атака з метою зробити ресурси ІКМ недоступними для авторизованих користувачів. Здійснюється шляхом провокування надмірного навантаження на ОС, додатки або технічні засоби мережі. До найпоширеніших DoS-атак належать *TCP SYN flood, Flood, ICMP flood, Identification flood та Tribe Flood.*

Розподілена DDoS-атака (*Distributed Denial of Service*) – скоординована DoS-атака відразу з багатьох комп'ютерів. До найпоширеніших DDoS-атак належать *TCP SYN flood , TCP flood, SYN flooding, UDP flood, Smurf* та *ICMP flood.*

Сніфер пакетів (Sniffer) – програма, яка використовує інтерфейсну карту мережі, що працює в нерозбірливому (*promiscuous mode*) режимі прийому і дозволяє перехоплювати всі пакети мережі.

IP-спуфінг (*spoof* – обман) – вид хакерської атаки, що передбачає використання зловмисником, який видає себе за санкціонованого користувача, чужої IP-адреси.

Віруси (Virus) – шкідливий програмий фрагмент, здатний до впровадження в інформаційну систему у тілі переданого користувачем файла в інші файли комп'ютера, зокрема у файли системних і прикладних програм та електронної пошти.

Мережеві хробаки (Worm) – злоякісні програми, здатні до самостійного створення своїх копій і розповсюдження їх по комп'ютерах мережі без участі в цьому процесі користувачів. Водночас хробак збирає інформацію про вузли мережі, їх адреси та інші дані, які цікавлять зловмисника.

Трояни (троянські коні, Trojan horse) – різновид шкідливих програм, які маскуються під корисні додатки але наносять шкоду інформаційній системі: знищують або спотворюють інформацію на диску, викрадають паролі, спотворюють імена файлів і т.п.

Логічні бомби (Logic bombs) – спеціально сконструйовані коди, які за певною ознакою спричиняють деструктивну роботу програми, що виконується, зокрема, повне припинення її виконання.

Спам (Spam) – вид атаки засобами електронної пошти. Велика кількість листів, яка надсилається зловмисником на адресу електронної пошти, унеможливлює роботу поштових скриньок, а іноді і поштових серверів.

Ін'єкції (Exploit tools) – вид атаки шляхом впровадження шкідливих команд або даних в працюючу систему з метою впливу на її роботу так, щоб отримати доступ до комп'ютера чи даних, або дестабілізувати роботу системи загалом. Прикладом такого виду атаки є *SQL-ін'єкції*, які зловмисники використовують для зміни параметрів запитів до бази даних (сховища).

Бекдор (*back door*) – злоякісна програма, яка забезпечує зловмиснику доступ до конфіденційної інформації, розміщеної на віддаленому комп'ютері. Завдяки бекдору зловмисник може витягнути з інфікованої LAN назву та ЄДРПОУ корпорації, пароль проксі-сервера, ім'я поштового сервера, паролі та email-адреси клієнтів.

За висновками фахівців у сфері IT-технологій, мережа Інтернет стала ідеальним середовищем для діяльності терористів, в якому частота і складність кібер-атак постійно зростає [6]. Сьогодення характеризується появою нових злоякісних програм та широким використанням таких видів атак, як кібер-шантаж, розсилання фальшивих електронних листів, фішинг, SMS-шахрайство, використання бот-мереж для організації атак на приватні сайти. Для викрадення інформації часто застосовують *програми-шпигуни* та *програми-кіберрозвідники* – вид шкідливих програм, які таємно встановлює зловмисник на комп'ютери мережі з метою збирання секретної інформації про будову та принципи функціонування мережі, виявлення брандмауерів, перехоплення й аналізу даних. Найпоширенішими видами шпіонських програм є *сканери портів, клавіатурні та екранні шпигуни і модемні та мережеві кіберрозвідники*.

Останнім часом хакери доволі часто використовують *бот-мережі* (*botnet, зомбі-мережі*), до складу яких може входити велика кількість інфікованих комп'ютерів зі встановленими зловмисником шкідливими програмами. До отримання команди від зловмисника бот-мережа знаходиться в "сплячому" режимі. Отримавши команду, botnet починає виконувати закладені в неї функції, наносячи шкоду ресурсам атакованої мережі (розкриття IP-адрес та паролю доступу до інформаційних ресурсів, розповсюдження спаму, здійснення атак на сервери з метою спровокувати відмову в обслуговуванні клієнтів тощо). Керувати ботом зловмисник може як посиланням відповідного коду на адресу одного з комп'ютерів, так і через веб-сайти за допомогою наперед сформованої URL-адреси та використанням p2p-мереж. Найчастіше бот-мережі використовують для організації DDoS-атак.

В останні роки для кіберрозвідки почали активно застосовувати методи моніторингу відкритих і відносно відкритих джерел *(МВВВД)* та соціальної інженерії *(СІ)*, які, за оцінками вітчизняних і західних фахівців, забезпечують отримання від 30 % до 90 % розвідувальних даних [1, 7].

Моніторинг відкритих і відносно відкритих джерел – це процес збирання широкого спектра інформації про об'єкт розвідки, супроводжуваний її опрацюванням та підготовкою оперативних дій. Соціальна інженерія – це комплекс заходів, спрямованих на отримання зловмисником доступу до конфіденційної інформації завдяки зовнішньому впливу на працівників об'єкта атаки з подальшим провокуванням внутрішнього інциденту.

Для підготовки атаки агенти соціальної інженерії користуються переважно такими засобами, як фішинг, претекстинг і бейтинг. *Фішинг* (phishing, риболовля) – використання зловмисником фальшивих *e-mail* та розсилка через соціальні мережі шахрайських повідомлень та різних типів вірусних програм з метою отримання доступу до конфіденційної інформації. *Бейтинг* – запуск злоякісних програм засобами електронної пошти при відповіді атакованого на запит зловмисника.

Претекстинг – дії, за яких зловмисник, використовуючи *Skype* або телефон і згадуючи імена реальних людей, входить в довіру до жертви і отримує від неї інформацію, яка його цікавить. Разом з тим, засоби соціальної інженерії передбачають використання різних вкладок (пристроїв підслуховування, відео- та аудіоспостереження, перехоплення електромагнітних сигналів та запис різнотипних випромінювань тощо), замаскованих під предмети побуту, аксесуари індивідуального користування, іграшки тощо.

Вплив кібертероризму на безпеку суспільства

Якщо у двадцятому столітті питання безпеки в Інтернеті зводилося переважно до захисту банківської та особистої інформації, то з появою *кібертероризму* на передній план вийшли проблеми захисту як приватних, так і публічних ІКМ [2]. У процесі проникнення інформаційних технологій до усіх сфер діяльності людини залежність кожного індивіда від інформаційних систем і мереж та його вразливість щодо стороннього кібернетичного впливу постійно зростають. Мережа Інтернет надала злочинним елементам ефективні засоби впливу на громадську думку та привела до появи нових видів злочинності. Сучасний кібертероризм вийшов за рамки викрадення секретної інформації та отримання фінансової вигоди від проведення хакерської атаки. Розміщення невірогідної (фейкової) інформації на спеціально створених сайтах (*consumer opinion sites*), а також поширення небезпечного контенту через форуми, блоги, e-mail може не тільки спровокувати соціальні заворушення та паніку серед населення, а й запустити незворотні процеси в державних масштабах (зруйнувати банківську та фінансову системи держави, вплинути на роботу об'єктів критичної інфраструктури тощо).

На свідомість людей та життя суспільства загалом останнім часом почали активно впливати *соціальні мережі*, які можуть використовувати різні способи маніпулювання громадською думкою. В них часто виникають інциденти, що несуть загрозу як різним сферам суспільного життя, так і кібернетичному простору всієї держави. Соціальні мережі нерідко використовують для розповсюдження різних видів вірусів, проведення антидержавної та націоналістичної пропаганди, закликів до повалення влади, вербування людей для участі в терористичних актах. Моніторингом соціальних мереж займаються спеціальні підрозділи органів державної безпеки, які проводять спостереження, аналіз та прогнозування ймовірності виникнення нових видів інцидентів [8].

Кібертеротисти в пошуках об'єкта атаки часто беруть до уваги психологічний стан осіб, причетних до роботи з інформацією. Потенційними жертвами та джерелом витоку інформації з обмеженим доступом можуть стати як адміністративний персонал і фахівці у сфері IT-технологій, так і будь-який працівник фірми. За даними проведених досліджень кібербезпека організації на 80 % залежить від правильного добору працівників, а легітимний користувач стає найслабшою ланкою в системі інформаційної безпеки мережі. Відомий випадок, коли зловмисник, використовуючи претекстинг, за допомогою телефонного дзвінка вивідав у працівника енергетичної компанії інформацію, яка дала змогу організувати успішну атаку на мережу цієї компанії [1].

Політика сучасної кібернетичної безпеки передбачає вивчення працівниками корпорації основ соціального інжинірингу. Методи соціального інжинірингу для боротьби з інцидентами передбачають використання механізму оповіщення інтернет-користувачів про злоякісні веб-сайти, які спеціально створюються зловмисниками для збирання конфіденційних даних. Так, антифішинг реалізується введенням до популярних браузерів (Microsoft Internet Explorer, Firefox та ін.) спеціальних фільтрів (плагінів), що попереджають користувачів у випадку їх звертання до підроблених або підозрілих сайтів. Співробітники як державних, так і приватних компаній повинні орієнтуватися в методах і засобах соціальної інженерії, проявляти пильність у разі виявлення вкладень з незнайомих джерел та усвідомлювати, що більшість кібератак здійснюється через фальшиві веб-сайти та електронну пошту. Неналежна увага керівництва до потреб підлеглих, а також до формування у співробітників почуття відповідальності та сумлінного ставлення до виконання своїх обов'язків може спровокувати негативні прояви людського фактора в системі забезпечення комплексної безпеки корпорації.

Діяльність терористів у сфері інформаційних технологій характеризується відсутністю національних кордонів, а їхні дії можуть бути спрямовані як на приватні, так і на урядові об'єкти. У міжнародних стосунках на заміну воєнним діям із застосуванням армійських підрозділів все частіше приходять інформаційні та гібридні війни, в яких активно використовують кібершпіонаж та кібератаки на об'єкти критичної інфраструктури. Хакери спрямовують свої атаки на урядові сервери, сервери політичних партій, громадських організацій, виборчих комісій та ін.

Наймасовіша атака в історії сучасного кіберпростору відбулася у травні 2017 року, коли вірус WannaCry атакував сотні тисяч комп'ютерів у 150 країнах на всіх континентах земної кулі. Кібератака була спрямована на комп'ютери як приватних користувачів, так і корпорацій та державних організацій. Вірус, що самостійно поширювався через електронну пошту, блокував файли атакованих комп'ютерів і вимагав викупу для розблокування зашифрованих даних. Більшість фахівців з кібербезпеки вважають, що збагачення зловмисників не було ціллю атаки, а деякі характерні ознаки WannaCry свідчать про можливість причетності до створення цієї злоякісної програми північнокорейської хакерської організації Lazarus Group.

Наймасовішу кібератаку на мережі фінансових установ, органів влади, об'єктів критичної інфраструктури, засобів масової інформації та інших державних і приватних компаній України було здійснено 27 червня 2017 року. Злоякісна руйнівна програма Nyetya (або Petya), яка поширювалася через електронну пошту, шифрувала файли та дані на жорстких дисках інфікованих комп'ютерів без можливості їх дешифрування і маскувалася при цьому під здирника грошей. За даними кіберполіції, постраждали понад 2 тисячі як вітчизняних, так і міжнародних компаній, які вели свій бізнес в Україні. В результаті детального розслідування цього інциденту за участі міжнародних фахівців у галузі кібербезпеки виявилося, що при поширенні вірусу Nyetya всі інсталяції було отримано через систему оновлення бухгалтерського програмного забезпечення M.E.Doc, яке використовується для взаємодії з українськими податковими системами. За висновками фахівців Cisco і розробника антивірусів ESET, до недостатньо захищеного програмного забезпечення M.E.Doc хакери у 2017 р. внесли злоякісну програму типу *бекдор*, яка давала змогу перехоплювати конфіденційні дані клієнтів, що зверталися до сервера оновлення бухгалтерського програмного забезпечення.

Експерти та фахівці у сфері інформаційної безпеки схиляються до висновку, що метою цієї атаки могла бути демонстрація зловмисниками своїх можливостей та перевірка здатності атакованої держави до швидкого та ефективного реагування на кібернетичну загрозу, своєрідне тестування свого шкідливого ПЗ перед проведенням серйозніших кібератак на об'єкти критичної міжнародної інфраструктури.

В Україні боротьбою з кібертероризмом займаються спеціалізовані підрозділи національної поліції, СБУ та Держспецзв'язку, які тісно співпрацюють з міжнародними підрозділами боротьби з кіберзлочинністю та провідними міжнародними компаніями в галузі IT і кібербезпеки. Активну позицію в боротьбі з кібертероризмом займає НАТО. Це проявляється в активізації його роботи з країнами-партнерами та створенні трастового фонду з кібербезпеки. Тісний контакт з правоохоронними органами європейських країн та партнерами в галузі кібернетичної безпеки підтримує Європол.

Однак, уникнути інцидентів у кібернетичному просторі неможливо. Оперативна реакція на прояви міжнародного кібертероризму та інтенсивність дослідження нових та очікуваних інцидентів з метою їх врахування у політиці безпеки залежать від наявності належних інвестицій та об'єднання зусиль світових організацій і компаній, які спеціалізуються у сфері кібернетичної безпеки.

Висновки

Сучасне суспільство, отримавши в результаті розвитку інформаційних і комунікаційних технологій небачені досі можливості в галузі обміну інформацією, стало надзвичайно вразливим щодо стороннього шкідливого кібернетичного впливу та різних видів загроз.

Загрозу кібернетичній безпеці становлять як зовнішні, так і внутрішні інциденти. Безпека інформаційної системи значною мірою залежить від правильного добору кадрів, вивчення ними основ соціального інжинірингу та неухильного дотримання вимог політики безпеки.

Соціальні мережі, які наповнили Інтернет приватною інформацією та особистими даними, впливають на інформаційний простір, свідомість людей та реальне життя суспільства. Вони знаходяться під постійною увагою соціального інжинірингу та моніторингу з боку спеціальних як державних, так і міжнародних структур.

Мережа Інтернет надала міжнародним терористам зручне для злочинної діяльності середовище, в якому частота і складність кібератак постійно зростають, а кібертероризм починає використовуватися у міждержавних стосунках та світовій політиці.

Міжнародний кібертероризм неможливий без підтримки і координації дій з боку агресивних держав. Кібератаки здійснюються здебільшого під керівництвом спецорганів недружніх держав і спроможні без використання традиційних видів озброєння нанести атакованій державі безповоротних втрат.

Ефективність боротьби з новими видами інцидентів у сфері міжнародної кібербезпеки залежить від залучення світовою спільнотою належних інвестицій та тісної співпраці національних і міжнародних правоохоронних органів з провідними компаніями у галузі інформаційних технологій та кібербезпеки.

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с. 2. Грищук Р. В. Основи кібернетичної безпеки: монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕ, 2016. – 636 с.: іл. 3. GAO-10-606. CYBER SPASE United States Faces Challenges in Addressing Global Cyber security and Governance, Washington, July 2010 [Електронний ресурс]. – Режим доступу: http://web.ebscohost.com. *4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с. 5. Конвенція про кіберзлочинність / Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 р. [Електрон. ресурс]. – Режим доступу:* http://zakon4.rada.gov.ua/laws/show/994_575. *6. Довгань О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 49–53. 7. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації. – 2012. – № 4(57). – С. 5–12. 8. Гавриш С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії [Електронний ресурс] / С. Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – Режим доступу:* http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm.