Глянцева О.І., Кулиняк І.Я.
Національний університет «Львівська політехніка»

МІНІМІЗАЦІЯ КІБЕРАТАК ЯК НАПРЯМ ЗАХИСТУ ІННОВАЦІЙНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

Всеосяжність Інтернету, стрімкий розвиток інформаційно-комунікаційних технологій з однієї сторони дають чимало потенційних можливостей підприємствам і країні загалом. З іншої сторони, інтернатизація усіх сфер життя людини, у тому числі, використання комп'ютерів та інших цифрових пристроїв у всіх бізнес-процесах сприяло розвитку нової загрози – кібератак, під якими розуміють дії в кіберпросторі, спрямовані проти інформаційно-телекомунікаційної системи з метою впливу на неї шляхом порушення її функціонування, отримання контролю над системою, корекції, копіювання, вилучення, пошкодження, впровадження чи знищення даних, створення умов для зміни поведінки її користувачів [1].

Основною метою здійснення кібератак є: розкрадання цінних корпоративних даних, комерційної таємниці або персональних даних співробітників і клієнтів компанії, моніторинг діяльності компанії; знищення даних або блокування роботи інфраструктури; викрадення фінансових коштів через системи дистанційного банківського обслуговування; удар по репутації компанії; сприяння фінансовому збитку через DDoS-атаки, які на кілька днів виводять з ладу зовнішні веб-ресурси компаній [2].

Особливо загрозливою є ситуація, коли під прицілом кіберзлочинців є новітні технологічні розробки підприємства, незапатентована технічна документація, винаходи, промислові зразки, прилади, машини, формули, ресурси, ноу-хау. Така інформація часто зберігається в незашифрованому стані в мережах підприємства у вигляді електронних документів, технічних завдань, звітів, креслень, презентацій, зображень і т.д. і при неефективній системі безпеки можуть стати легкою наживою конкурентів.

При масовому розповсюдженні шкідливих програм жертвою кіберзлочинців може стати будь-яка компанія, комп'ютери якої їм вдасться заразити. Але також спостерігається і цільовість при виборі об'єктів атак. Так, за даними Gemalto у 2014 році число вкрадених записів становило 1023108267, при цьому частки втрат у різних галузях відрізнялися і становили відповідно: торгівля – 55%, фінанси – 20%, технології – 9%, освіта – 5%, уряд – 5%, охорона здоров'я – 3%, інше – 3% [4]. Хоча на галузь технологій і припадає порівняно невелика частка вкрадених записів, їх вартість може бути більшою, через їх унікальність і цінність.

Компанія Symantec в доповіді «Symantec Intelligence Report: November 2012» by Ben Nahorney наводить дані про типи інформації, які найбільш часто піддаються атакам: 55% - справжні імена, 40% - імена користувачів і паролі, 33% - ідентифікаційні номери, 30% - адреси електронних пошт, 28% - дати народжень, 6% - страхова інформація, 13% - фінансова інформація, 14% - телефонні номери, 25% - медична документація, 26% - домашні адреси [4].

Втрати компаній від кібератак є колосальними. Так, за даними компанії HP Enterprise Security втрати від кібератак у шести країнах становили: Австрія – 3,67 та 3,99 млн. дол., Великобританія – 4,72 та 5,93 млн. дол., Франція – 5,19 та 6,38 млн. дол., Японія – 6,73 та 6,91 млн. дол., Німеччина – 7,56 та 8,13 млн. дол. та США – 11,56 та 12,69 млн. дол. відповідно у 2013 та 2014 роках [5].

Вище наведені дані вказують на необхідність застосування ряду превентивних заходів, які б дали можливість комплексно захистити підприємство чи організацію від кібератак, оскільки, такі правомірні заходи захисту конфіденційної інформації, як незалежне відкриття, зворотний технічний аналіз та добросовісне придбання у особи, яка не мала права передавати інформацію [6] є порівняно дорогими та затратними у часі, а нові незаконні способи отримання інформації, такі, як кібератаки є ефективними і досить короткотривалими.

Для ефективної боротьби з кібератаками повинна бути побудована гнучка і настроювана для підвищення ефективності система безпеки, яка дає можливість виявляти шкідливі програми, підозрілі обміни даними, аналізувати міру небезпеки і характеристики атаки та атакуючого, автоматично модифікувати систему відповідно до потреб безпеки та ін. [7].

Важливим кроком для збереження інформації в межах підприємства є жорстке чітке регламентування прав доступу при роботі з інноваційною інформацією конфіденційного характеру, тобто виокремлення посадових осіб, які мають доступ до тої чи іншої інформації в межах своїх функціональних обов'язків і встановлення правил користування нею. Встановлене програмне забезпечення, у тому числі антивірусне має бути із надійних джерел і постійно оновлюватися для гарантування ефективнішої захищеності.

Не обійшли увагою питання захисту інформаційних технологій і стандарти якості ISO, що черговий раз підкреслює їх важливість. Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією було розроблено стандарт ISO / IEC 27001 - міжнародний стандарт з інформаційної безпеки. Він містить вимоги в області інформаційної безпеки для створення, розвитку і підтримки Системи менеджменту інформаційної безпеки.

У стандарті ISO 27001 містяться найкращі світові практики у сфері управління інформаційною безпекою. Він встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення інформаційної безпеки[8] і його впровадження і застосування відіграє важливу роль у цілісному захисті інформації.

Отже, актуальним стає формування ефективної системи кібербезпеки, яка дає можливість захистити інформацію та інтелектуальну власність від втрати і крадіжок. Важливість такого заходу у забезпеченні інноваційного розвитку підприємства є неоціненною, адже усі аспекти діяльності, які охоплюють комерційну таємницю, у тому числі дані щодо розробок, інноваційних рішень, результати досліджень, бази даних та ін. інформація, яка дає можливість створити конкурентні переваги, має значну вартість та знаходиться під прицілом конкурентів є збереженою. Її надійне зберігання дає можливість здійснювати подальшу діяльність в інноваційному спрямуванні без додаткових фінансових та інтелектуальних втрат.

1. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування [Електронний ресурс]: Аналітична доповідь. - Режим доступу: niss.gov.ua/articles/454/.

2. Kaspersky Security Bulletin 2013. Корпоративные угрозы [Електронний ресурс]. – Режим доступу: https://securelist.ru/analysis/ksb/19143/kaspersky-security-bulletin-2013-korporativnye-ugrozy/.

3. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности 2015 г. [Електронний ресурс]. – Режим доступу: book.itep.ru/10/2015.htm.

4. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности 2013 г. [Електронний ресурс]. – Режим доступу: book.itep.ru/10/2013.htm.

5. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности 2014 г. [Електронний ресурс]. – Режим доступу: book.itep.ru/10/2014.htm.

6. Верба І.І. Основи інтелектуальної власності: навчальний посібник/ І.І.Верба, В.О.Коваль; за ред. С.В. Чікін. – 2-ге вид., перероб. і доп. – К.: НТУУ «КПІ», 2013. – 262 с.

7. Информационная безопасность: защита от кибератак [Електронний ресурс]. – Режим доступу: trendmicro.com.ru/technology-innovation/cyber-security/.

8. *Международный стандарт. ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. ИСО/МЭК 2005. Первое издание 2005-10-15. - ЗАО «Технорматив». Перевод на русский язык, 2006. – 48 с.*