Міністерство освіти і науки України
Полтавський національний технічний університет імені Юрія Кондратюка
Науково-навчальний інститут фінансів, економіки та менеджменту
Кафедра фінансів і банківської справи

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IV Всеукраїнської науково-практичної Інтернет-конференції з міжнародною участю

15 грудня 2017 р. – 25 січня 2018 р.

Полтава
2018

УДК 330.336
Е45

Е45 **Економічна безпека: держава, регіон, підприємство:** Матеріали IV Всеукраїнської науково-практичної Інтернет-конференції з міжнародною участю, 15 грудня 2017 р. – 25 січня 2018 р. – Полтава: ПолтНТУ, 2018. – 195 с.

ISBN 978-966-616-177-5

У збірнику матеріалів IV Всеукраїнської науково-практичної Інтернет-конференції з міжнародною участю представлено результати розвитку теорії економічної безпекології, теоретичні та методологічні аспекти системотворення економічної безпеки держави, регіону та підприємства, забезпечення економічної безпеки держави, регіону, підприємства (концепції, напрями дій, способи та алгоритми), оцінювання економічної безпеки держави, регіону, підприємства.

Участь у конференції взяли науковці та практики з м. Київ, Львів, Харків, Одеса, Запоріжжя, Сєвєродонецьк, Хмельницький, Дніпро, Миколаїв, Лисичанськ, Кривий Ріг, Миколаїв, Суми, Полтава.

Призначений для фахівців з економічної безпеки, науковців, викладачів, аспірантів, докторантів та студентів.

УДК 330.336

ISBN 978-966-616-177-5

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТА ПІДПРИЄМНИЦТВА

Л.О. Птащенко, *доктор економічних наук, професор*
Полтавський національний технічний
університет імені Юрія Кондратюка

Інформаційна система сучасної організації чи підприємства є складним утворенням, побудованим у багаторівневій архітектурі клієнт-сервер, яке користується численними зовнішніми серверами, а також надає доступ до зовнішніх серверів.

Розвиток нових інформаційних технологій і загальна комп'ютеризація привели до того, що інформаційна безпека не тільки стає обов'язковою, вона є важливим елементом загальної системи безпеки суб'єкта підприємництва.

Високі темпи розвитку інформаційних технологій актуалізують проблему захисту інформації, її користувачів, інформаційних ресурсів та каналів передачі даних, а також вимагають постійного вдосконалення механізмів захисту.

В процесі управління інформаційною безпекою слід ураховувати загрози, котрі класифікують як випадкові (ненавмисні) й навмисні.

Серед випадкових загроз найбільш частими й найнебезпечнішими (з точки зору розміру збитку) є "людський фактор" – ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. За опублікованими даними, до 65% інформації безслідно зникає саме через ці фактори.

Важкопередбачуваними джерелами загроз інформації є аварії та стихійні лиха. На безпеку інформаційних систем істотно впливає той факт, що безпомилкових програм в принципі не існує [1]. Це стосується не тільки окремих програм, а й цілої низки програмних продуктів корпорацій, відомих у всьому світі, наприклад, Microsoft. За даними інформаційно-аналітичного сайту, щодня виявляються в середньому 5-10 нових уразливостей в операційних системах і додатках.

До навмисних загроз належать такі:

несанкціонований доступ до інформації та мережевих ресурсів;

розкриття та модифікація даних і програм, їх копіювання;

розкриття, модифікація або підміна трафіку обчислювальної мережі;

розроблення та розповсюдження комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;

крадіжка магнітних носіїв та технічної документації;

руйнування архівної інформації або умисне її знищення;

фальсифікація повідомлень, відмова від факту отримання інформації або зміна часу її отримання;

перехоплення та ознайомлення з інформацією, що передається по каналах зв'язку;

незаконне використання привілеїв;

несанкціоноване використання інформаційних ресурсів.

До найбільш поширених видів навмисних загроз належить несанкціонований доступ [2]. Зазвичай метою зловмисника є порушення конфіденційності даних. При цьому найскладнішим виявляється визначити, хто і до яких даних може мати доступ, а хто – ні. Найчастіше застосовуються такі шляхи несанкціонованого доступу до інформації:

застосування підслуховуючих пристроїв (закладок);

перехоплення електронних випромінювань;

дистанційне фотографування;

перехоплення акустичних випромінювань і відновлення тексту принтера;

читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

копіювання носіїв інформації з подоланням заходів захисту;

маскування під зареєстрованого користувача;

маскування під запити системи;

використання програмних пасток;

використання недоліків у мові програмування;

незаконне підключення до апаратури та ліній зв'язку спеціально розроблених апаратних засобів, котрі забезпечують доступ до інформації;

зловмисне виведення з ладу механізмів захисту;

інформаційні віруси.

Перераховані шляхи несанкціонованого доступу вимагають спеціальних технічних знань і відповідних апаратних та програмних розробок. Однак є й досить примітивні шляхи несанкціонованого доступу, зокрема:

розкрадання носіїв інформації та документальних відходів;

схиляння до співпраці з боку зловмисників;

підслуховування,

спостереження тощо.

Будь-які способи витоку конфіденційної інформації можуть призвести до загроз безпеці, значного матеріального і морального збитку як для суб'єкта підприємництва, так і для його контрагентів. Більшість з перерахованих шляхів несанкціонованого доступу піддаються надійному блокуванню при правильно розробленій і реалізованій на практиці системі забезпечення безпеки.

Аналізуючи можливі загрози з точки зору найбільшої небезпеки, витонченості й руйнівності, слід виділити шкідливе програмне забезпечення, тобто будь-яку програму, котра створена з метою нанесення шкоди або для використання ресурсів атакованого комп'ютера. Про шкідливе програмне забезпечення відомо більше, ніж про будь-які інші небезпеки й пошкодження комп'ютерної техніки. Його можна розділити на три групи: комп'ютерні віруси, хакерське програмне забезпечення і спам.

Найновіші сімейства шкідливих програм вражають комп'ютери під управлінням сімейства ОС Microsoft Windows. Перші представники, виявлені в 2016 році, були звичайними зразками здирницьких вірусів. Останній найвідоміший вірус – Petya виявлений у березні 2016 року. Компанія Check Point тоді зазначила, що хоча вірусу вдалося заразити менше комп'ютерів, ніж іншим програмам-здирникам початку 2016 року, таким як CryptoWall, поведінка нового вірусу помітно відрізняється, завдяки чому він негайно був відмічений як наступний крок в еволюції програм-вимагачів. За відновлення доступу до файлів програма вимагала від користувача 0,9 біткоїнів, що, станом на березень 2016 року становило близько $380.

Наприкінці червня 2017 року відбулася масштабна атака останнім представником сімейства, який запозичив деякі модулі з попередніх зразків, але, можливо, створений іншими розробниками та вже розглядався фахівцями як вірус-винищувач даних, замаскований під програму-вимагача.

Програма шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує й шифрує головний завантажувальний запис (MBR) – дані, необхідні для завантаження операційної системи. В результаті всі файли, що зберігаються на комп'ютері, стають недоступними. Потім програма вимагає грошовий викуп у біткоїнах за розшифровку та відновлення доступу до файлів. При цьому перша версія вірусу шифрувала не самі файли, а MFT-таблицю – базу даних з інформацією про файли, що зберігаються на диску.

Станом на 28 червня 2017 року вірусом вражено 12 500 ПК у 64 країнах світу. Атака в основному була спрямована проти України, на яку припало 75 % усіх постраждалих від вірусу комп'ютерів. Зокрема, атаці піддались енергетичні компанії, українські банки, Харківський аеропорт, Чорнобильська АЕС, урядові сайти, Київський метрополітен [3].

Таким чином, зі зростанням ролі інформації та інформаційних систем у сучасному світі загострюються й загрози їх нормальному функціонуванню. Для протидії загрозам розвиваються методи й засоби захисту інформації та інформаційних систем.

Більшість великих антивірусних компаній стверджують, що їхнє програмне забезпечення оновлено, щоб активно виявляти й захищати від проникнення вірусу. Наприклад, продукти компанії Symantec використовують сигнатури оновленої версії 20170627.009. Крім того, актуальні оновлення Windows виправляють вразливість EternalBlue, що дозволяє зупинити один з основних способів зараження, а також захистити користувачів від майбутніх атак з різного роду корисними навантаженнями.

Системи захисту інформації, що пропонуються науковцями та практиками, не відображають повною мірою вирішення завдань та виконання функцій, які стоять перед захистом інформації в системі інформаційної безпеки, інформаційного забезпечення та безпеки суб'єкта підприємництва в цілому.

Завданнями системи захисту інформації та інформаційних систем є:

організація особливого діловодства та контролю за секретними документами;

виявлення, попередження та присікання каналів витоку інформації;

розроблення посадових інструкцій, а також положень, пам'яток, методичних вказівок для роботи з відомостями, що складають комерційну таємницю;

захист інформації при використанні комп'ютерної техніки та інших технічних засобів оброблення та передавання даних;

виявлення необхідності, обґрунтування та організація встановлення необхідних технічних засобів забезпечення збереження інформації;

захист у судових та інших державних органах інтересів суб'єкта підприємництва щодо комерційної таємниці;

розроблення нормативної документації щодо комерційної таємниці суб'єкта підприємництва;

навчання правилам інформаційної безпеки працівників [4].

Оскільки система захисту інформації становить найбільш вагому частку в інформаційній безпеці, отже, й більшість складових в системі інформаційної безпеки (технічна, організаційна та правова) становлять саме елементи захисту інформації. Крім того, дуже важлива попереджувальна складова в контексті передбачення, виявлення та перекриття каналів витоку інформації.

Література

1. Безпека інформаційних систем : сайт. URL: http://bukvar.su.

2. Види умисних загроз безпеці інформації : сайт. URL: http://ymi.underref.ru/001489649.html