УДК 681.5

ТЕХНІКО-ЕКОНОМІЧНИЙ ПІДХІД ДО ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ У МАЛОМУ БІЗНЕСІ

Усманова М. З.[1], Фурман І. О.[2]

[1]Національний технічний університет "Харківський політехнічний інститут",
[2]Харківський національний технічний університет сільського господарства імені Петра Василенка

У роботі пропонується малобюджетний метод захисту електронної інформації підприємства, що істотно збільшує рівень безпеки зберігання та використання даних.

Постановка проблеми та аналіз стану питання. На даному етапі комп'ютерні технології та системи настільки щільно інтегрувалися в нашу життєдіяльність, що ми вже не уявляємо собі здійснення робочого процесу і прийняття рішень без використання хоча б персонального комп'ютера.

Зростаючий попит призвів до того, що практично вся документація підприємств, вся звітність та супутня інформація зберігаються в електронному вигляді. Саме тому так важливі методи та засоби для створення, використання та безпечного зберігання інформації в комп'ютерах.

На сьогоднішній день в усьому світі витрачаються величезні кошти на захист інформації в комп'ютерах від пошкоджень, створюються потужні системи захисту. Будь-яка компанія намагається захистити свою інформацію, проте ступінь такого захисту істотно залежить від вартості цих даних і платоспроможності компанії. Наприклад, великі корпорації витрачають сотні тисяч доларів на купівлю та утримання таких систем. Але такі статті витрат актуальні для великих концернів і корпорацій, а для представників дрібного бізнесу, що мають невеликий штат працівників і значно менший обсяг інформації, такі масштабні системи недоступні, та й, за великим рахунком, не потрібні.

Головна вимога до системи захисту, щоб її вартість не перевищувала вартість інформації, що захищається. В рамках цієї тези бажано визначити комплекс заходів і дій, витрати на який будуть мінімальні, а ефект у масштабах дрібного бізнесу істотний і достатній.

Під інформаційною безпекою (безпекою інформації) у загальному випадку розуміють рівень захищеності інформації та її носіїв (систем і засобів, що забезпечують отримання, обробку, зберігання, передачу і використання інформації) від різного виду погроз.

Інформаційна безпека - це стан захищеності інформаційного середовища. Захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на зміст інформації, тобто процес, спрямований на досягнення цього стану.

Інформаційна безпека організації - цілеспрямована діяльність її органів і посадових осіб з використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Розрізняють два види джерел загроз, які можуть бути навмисні та ненавмисні. Говорячи про навмисні джерела ми розуміємо такі вчинки, що мають мету незаконного отримання або спотворення інформації.

Під ненавмисними загрозами розуміють дії, які таку мету не ставлять, а можуть виникати через непрофесійну діяльність або через необережне та неналежне використання обладнання. Тому має сенс розробити комплекс заходів із захисту інформації від обох видів загроз.

Мета статті. Запропоновувати методи, що забезпечать захист системи від несанкціонованих і некваліфікованих дій користувачів, а також навмисних мережевих атак і вірусних програм.

Основні матеріали дослідження. Захист електронних даних, перш за все, пов'язаний із забезпеченням безпечних умов експлуатації комп'ютерної техніки. Їм часом приділяється мало уваги, що призводить до необхідності переустановлення систем, а це може привести до втрати інформації з системного диска або всього вінчестера або навіть поломок устаткування, тому:

- необхідно дотримуватися правил входу і виходу з системи, зберігати вручну всі дані після завершення роботи у програмах, не залишати відкритих програм при виході з системи;
- бажано, щоб у комп'ютера був один постійний користувач, але якщо це неможливо, то інші облікові записи повинні бути обмежені в доступі до системного диску, найважливіших папок з даними, можливості та інсталяції ПЗ. Право повного доступу може бути надано лише головному користувачу, тобто адміністратору, обсяг доступу для інших користувачів визначається адміністратором з огляду на необхідність і обставини використання окремо взятого комп’ютера ;
- обліковий запис адміністратора повинен бути захищений надійним паролем, щоб уникнути несанкціонованих дій інших користувачів;

- якщо користувачів декілька і доступ до деяких дисків обмежити не вдається, необхідні папки рекомендується приховати, визначивши цей параметр у властивостях.

Значну увагу потрібно приділити так само програмному забезпеченню, а саме необхідності базового комплекту і заходів безпеки в роботі з ним, у зв'язку з чим:

- необхідно переважно використовувати у роботі ліцензійне програмне забезпечення, особливо щодо системного забезпечення. У самій системі закладено чимало корисних захисних функцій, таких як шифрування або відновлення даних, ці функції можуть бути дуже суттєвими у разі пошкодження інформації або обладнання;
- корисно встановити програму, що очищує і виправляє помилки реєстру. До розряду таких відноситься CCleaner, Error repair і т.д. Їх використання очистить системний диск від різних тимчасових і несанкціоновано створених файлів, які так само можуть нести шкідливу інформацію (наприклад, cookies), збільшить швидкодію системи;
- важлива функція виправлення помилок реєстру, які виникають, у тому числі при неправильній установці і роботі в програмах. Майстер реєстру виправить помилки і забезпечить коректну роботу програми;
- необхідно обов'язково встановити антивірусну програму, бажано з мережевим екраном і mail-агентом. Такі розширені можливості пропонуються наприклад Лабораторією Касперського і MCAfee. Таким чином, будуть ретельно перевірятися не тільки всі програми та файли комп'ютера, але й дані, що надходять на комп'ютер через електронну пошту;
- мережевий екран забезпечить захист комп'ютера від можливих мережевих атак, які так само несуть небезпеку зараження системи вірусом. Без спеціального мережевого екрану виявити атаку для пересічного користувача майже неможливо. Під час атаки важлива інформація може бути викрадена;
- нинішні вірусні програми все більш важко виявляються, тому так само не зайвим буде з певною періодичністю використовувати додатковий антивірусний сканер, що не вимагає інсталяції. До таких належить CureIt від лабораторії Dr.Web;
- обмежити інсталяцію сумнівного програмного забезпечення, яке може містити віруси або виконувати несанкціоновані дії (відправка зібраних даних з комп'ютера, що містять особисту інформацію користувачів);
- важливу інформацію необхідно об'єднувати в тематичні групи й упаковувати в зашифровані архіви (зі створенням пароля для входу доступу до архіву) за допомогою WinRaR, WinZip або 7-Zip.

Висновки. Таким чином, у цій роботі систематизовані основні прийоми для надійного зберігання комп'ютерної інформації.

Дотримання запропонованих рекомендацій допоможе досить ефективно керувати процесом обробки інформації без втрат і пошкоджень, а також, що дуже важливо, значно зекономити витрати на захист даних при розв'язанні економічних задач малого бізнесу, виключаючи необхідність придбання коштовних систем безпеки.

Список використаних джерел

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.
2. Галатенко В. А. Стандарты информационной безопасности. / В. А. Галатенко. М.: Интернет-университет информационных технологий, 2006. – 264 с.
3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. М.: ДМК Пресс, 2008. – 544 с.

Аннотация

ТЕХНИКО-ЭКОНОМИЧЕСКИЙ ПОДХОД К ЗАЩИТЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В МАЛОМ БИЗНЕСЕ

Усманова М. З., Фурман И. А.

В работе предлагается малобюджетный метод защиты электронной информации предприятия, существенно увеличивающий уровень безопасности хранения и использования данных.

Abstract

TECHNICAL AND ECONOMIC APPROACH TO THE PROTECTION OF COMPUTER INFORMATION IN SMALL SCALE BUSINESS

M. Usmanova, I. Furman

A low-budget way to protect electronic information of the companies is offered, which may cause a significant increase of the safety level of data storage.