УДК 004.451.36:681.5:002

О. А. ХЛОБИСТОВА, Кандидат технічних наук, доцент кафедри інформаційних систем, Національний університет харчових технологій, вул. Володимирська, 68, Київ, Україна, 01601

М. В. ГЛАДКА, асистент кафедри інформаційних систем, Національний університет харчових технологій, вул. Володимирська, 68, Київ, Україна, 01601

ВИБІР МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ДОКУМЕНТООБІГУ

Використання новітніх методик у виробництві – основне питання у час зростання конкуренції за частку ринку та споживача. Безпека інформаційного захисту дозволяє забезпечити збереження та захист інформації на різних рівнях доступу. Використання методів захисту завжди залежить від цінності інформації, яку необхідно захистити та зберегти.

Ключові слова: документ, інформація, ключ, захист, шифрування, електронний цифровий підпис.

Вступ

Розвиток нових інформаційних технологій і всесвітня комп’ютеризація привели до того, що безпека інформації не тільки обов’язкова, вона також є однією з характеристик інформаційної системи. Під безпекою інформаційної системи розуміють захищеність системи від випадкового, або зловмисного втручання в процес її функціонування, від намагання викрадення, модифікації або знищення інформації.

Інформаційна безпека підкреслює важливість інформації в сучасному суспільстві – розуміння того, що інформація – це цінний ресурс, щось більше, ніж окремі елементи даних. Інформаційною безпекою називають заходи по захисту інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і вільному доступі. Інформаційна безпека включає заходи по захисту процесів створення даних, їх введення, обробки і виводу.

Метою інформаційної безпеки є забезпечити цілість системи, захистити і гарантувати точність та повноту інформації, мінімізувати можливі руйнування, якщо інформація буде модифікована або пошкоджена. Інформаційна безпека вимагає обліку всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється.

Мета роботи

Метою роботи являється дослідження методів захисту інформації та їх практичне використання у системах документообігу.

Викладення основного матеріалу

Системи документообігу є невід`ємною складовою частиною будь-якого підприємства. Від успішності функціонування цієї системи залежить керованість підприємства.

Документи, які циркулюють на підприємстві, можна умовно згрупувати таким чином:

- прогнози збуту, виробнича програма, виробничий план, оперативні плани-графіки;
- виробничі потужності, запаси сировини, напівфабрикатів і готових виробів;
- рецептура, конструкторська документація, опис технології виробництва;

- договори на постачання сировини і комплектуючих;
- договори на виготовлення і збут продукції;
- фінансові документи;
- кадрова документація.

Всі документи, які функціонують на підприємстві, можна умовно розділити на дві категорії:

- зовнішнього зв`язку,
- внутрішнього зв`язку.

До першої категорії відносяться документи, які надходять на підприємство зовні, або розробляються для передачі від підприємства іншій організації.

До другої категорії відносяться документи, за допомогою яких відбувається керування підприємством.

Серед документів як першої, так і другої категорії присутня значна кількість таких, що містять конфіденційну і навіть секретну інформацію. Тому, щоб запобігти несанкціонованому доступу до цієї інформації, необхідно запровадити надійну систему захисту документообігу. При цьому слід брати до уваги той факт, що впровадження системи захисту завжди призводить до ускладнень в роботі, отже впровадження системи захисту повинно бути економічно обґрунтованим і доцільним.

Система документообігу будь-якого підприємства містить документи на паперових носіях і електронні документи, які надходять на підприємство або створюються в результаті його функціонування. Оскільки захисту потребують всі види документів, то перейдемо до розгляду основних видів атак на системи документообігу і засобів їм протидії.

Можна виділити такі напрями захисту інформації на підприємстві:

- правові;
- організаційні;
- технічні.

Правова основа захисту інформації на підприємствах базується на нормативних документах [1-3].

Організаційно-правові методи захисту інформації полягають у обмеженні доступу як сторонніх осіб, так і працівників підприємства до об`єктів, де міститься секретна або конфіденційна інформація. Головна задача цих методів захисту – перешкоджати несанкціонованому доступу (НСД). Атака цього виду може здійснюватися як пасивним методом (зчитування секретної інформації), так і активним (пошкодження інформації). Для попередження НСД здійснюють наступне:

- при роботі з зовнішніми документами, що містять секретну інформацію, слід дотримуватися визначених правил (передавати документи з кур`єром, забезпечити їх зберігання і охорону тощо);
- в разі безпаперової передачі документів слід забезпечити ідентифікацію, як автора документа, так і його змісту.

Найбільш поширеним алгоритмом ідентифікації є використання цифрового підпису (ЕЦП). В схемах ЕЦП замість документа розглядається його хеш-функція h(x), основна властивість якої – практична неможливість створення двох різних документів з однаковим значенням хеш-функції. Перевірка правдивості документу полягає у контролі співвідношення, що пов`язує хеш-функцію документа, підпис під ним і відкритий ключ автора документу.

Внутрішня система документообігу в основному вразлива з боку співробітників підприємства. Доведено, що причиною 80% всіх викрадень або спотворень інформації є зловмисні вчинки працівників фірми. Єдиний засіб запобігти цьому – відповідна кадрова політика підприємства, спрямована на підвищенні зацікавленості працівників в успішній роботі, вихованні почуття відповідальності за свою справу.

Крім використання правових і організаційно-правових методів для перешкоджання НСД слід встановити фізичні перешкоди на шляху потрапляння зловмисника до інформації, що захищається, у тому числі

спробам з використанням технічних засобів знімання інформації і впливу на неї.

Управління доступом – метод захисту інформації за рахунок регулювання використання всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);
- ідентифікацію об'єкта або суб'єкта за пред'явленим ідентифікатором;
- перевірку повноважень (перевірка відповідності встановленому регламенту дня тижня, часу доби, залучених ресурсів і процедур);
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію (протоколювання) звернень до ресурсів, що захищаються;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Методи захисту інформації на практиці реалізуються із застосуванням засобів захисту.

Засоби захисту інформації можна розділити на:

1. Засоби захисту інформації, які знаходяться в одному приміщенні з захищеною системою, але не використовуються для безпосередньої обробки, зберігання, накопичення і передачі інформації. Вони поділяються на:

- пасивні – фізичні (інженерні) засоби, технічні засоби виявлення, прилади контролю радіоефіру, ліній зв'язку і т.п.;

- активні – джерела безперебійного живлення, шумогенератори, скремблери, пристрої відключення лінії зв'язку, програмно-апаратні засоби маскування інформації і ін.

2. Засоби, призначені для безпосередньої обробки, зберігання, накопичення і передачі інформації, що захищається, виготовлені в захищеному виконанні.

3. Засоби, призначені для контролю ефективності захисту інформації.

Для запобігання просочування мовної інформації по акустичному і віброакустичному каналах здійснюються заходи щодо виявлення каналів витоку. В більшості випадків для несанкціонованого знімання інформації у приміщенні зловмисник застосовує відповідні зчитувальні пристрої.

Можна так класифікувати потенційні погрози, проти яких направлені технічні заходи захисту інформації:

1. Втрати інформації через збої устаткування:

- перебої електроживлення;
- збої дискових систем;
- збої роботи серверів, робочих станцій, мережевих карт і так далі.

2. Втрати інформації через некоректну роботу програм:

- втрата або зміна даних при помилках ПЗ;
- втрати при зараженні системи комп'ютерними вірусами;

3. Втрати, пов'язані з несанкціонованим доступом:

- несанкціоноване копіювання, знищення або підробка інформації;
- ознайомлення з конфіденційною інформацією.

4. Помилки обслуговуючого персоналу і користувачів:

- випадкове знищення або зміна даних;
- некоректне використання програмного і апаратного забезпечення, що веде до знищення або зміни даних.

Самі технічні заходи захисту можна розділити на:

- засоби апаратного захисту, що включають засоби захисту кабельної системи, систем електроживлення, і так далі.
- програмні засоби захисту, у тому числі: криптографія, антивірусні програми, системи розмежування повноважень, засоби контролю доступу і так далі.

Програмні засоби захисту інформації мають бути реалізовані як додаткові модулі системи документообігу.

Програмними називаються засоби захисту даних, що функціонують у складі програмного забезпечення. Серед них можна виділити наступні:

- засоби архівації даних;
- антивірусні програми;
- криптографічні засоби;
- засоби ідентифікації і аутентифікації користувачів;
- засоби управління доступом;
- протоколювання і аудит.

Найбільш поширеними і в більшості випадків ефективними є криптографічні методи захисту інформації – спеціальні методи шифрування[1], кодування або іншого перетворення інформації, в результаті якого її вміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту, безумовно, найнадійніший метод захисту, оскільки охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм. Сучасна криптографія включає чотири розділи:

[1] Шифрування – процес перетворення: вихідний текст, який носить також назву відкритого тексту, замінюється шифрованим текстом, дешифровка - зворотний шифруванню процес. На основі ключа шифрований текст перетвориться в початковий.

- Симетричні криптосистеми. У симетричних криптосистемах і для шифрування, і для дешифровки використовується один і той же ключ.
- Криптосистеми з відкритим ключем[2]. У системах з відкритим ключем використовуються два ключі – відкритий і закритий, які математично зв'язані один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого лише одержувачеві повідомлення.
- Електронний підпис. Системою електронного підпису називається приєднуване до тексту його криптографічне перетворення, яке дозволяє при отриманні тексту іншим користувачем перевірити авторство і достовірність повідомлення.
- Управління ключами. Це процес системи обробки інформації, вмістом яких є складання і розподіл ключів між користувачами. Основні напрями використання криптографічних методів – передача конфіденційної інформації по каналах зв'язку (наприклад, електронна пошта), встановлення достовірності передачі повідомлень, зберігання інформації (документів, баз даних) на носіях в зашифрованому вигляді.

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, проте їй властиві і переваги: висока продуктивність, простота, захищеність і так далі Програмна реалізація більш практична, допускає відому гнучкість у використанні. Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

- зашифроване повідомлення повинне піддаватися читанню лише за наявності ключа;

[2] Ключ – інформація, необхідна для безперешкодного шифрування і дешифровки текстів.

- число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритому тексту, має бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровки інформації шляхом перебору всіляких ключів повинно мати строгу нижню оцінку і не виходити за межі можливостей сучасних комп'ютерів (з врахуванням можливості мережевих обчислень);
- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення навіть при використанні одного і того ж ключа;
- структурні елементи алгоритму шифрування мають бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, має бути повністю і надійно приховані в шифрованому тексті;
- довжина шифрованого тексту має бути рівною довжині вихідного тексту;
- не повинно бути простих і легко встановлюваних залежностей між ключами, що послідовно використовуються в процесі шифрування;
- будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Висновки

Захист інформації в системах документообігу – нагальна потреба сучасного функціонування будь-якого підприємства. Вибір конкретних засобів захисту залежить від цінності інформації, яка оберігається. Тому при виборі засобів захисту слід оцінити реальні втрати від розголошення або спотворення інформації і співставити з вартістю засобів охорони. Але в будь-якому випадку повинні бути впроваджені елементарні, найдешевші і від цього не менш ефективні засоби – вхід до системи документообігу повинен здійснюватися за системою паролів з розмежованим рівнем доступу. Фізичний доступ в приміщення, де встановлена система керування документообігом, повинен здійснюватися за правилами внутрішнього розпорядку і бути обмеженим для сторонніх осіб.

Список літератури:

1. Закон України «Про захист інформації в автоматизованих системах»

2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації від несанкціонованого доступу

3. НД ТЗІ Класифікація автоматизованих систем і стандартні профілі захищеності опрацьованої інформації від несанкціонованого доступу.

4. *В. Задирака, О. Олексюк*. Методи захисту фінансової інформації .К.: «Вища школа», 2000 С.456..

5. *Широчин В. П., Широчин С. В., Мухін В. Є*. Основи безпеки комп`ютерних систем. К.: «Корнійчук». 2009 С.285.

УДК 004.451.36:681.5:002

ВИБІР МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ДОКУМЕНТООБІГУ

О. А. Хлобистова, М. В. Гладка

Использование новых методик – основой вопрос во времена роста конкуренции за часть рынка и потребителя. Безопасность информационной защиты позволяет обеспечить сохранность и защиту информации на различных уровнях доступа. Использование методов защиты всегда зависит от ценности информации, которую требуется защитить и сохранить.

Ключевые слова: документ, информация, ключ, защита, шифрование, электронная цифровая подпись.

UDC 004.451.36:681.5:002

CHOICE OF METHODS OF INFORMATION SECURITY IN WORKFLOW SYSTEM

O. A. Khlobystova, M. V. Gladka

Use of the newest techniques the main issue in a competition for significant market share. Security information security ensures the preservation and protection of information at different levels of access. Use protection methods always depend on the value of information that must be protected and maintained.

Key words: document, information, key, security, encryption, digital signature.

Розміщено:

Вісник Національного технічного університету "Харківський політехнічний інститут". Збірник наукових праць. Тематичний випуск: Системний аналіз, управління та інформаційні технології. – Харків: НТУ "ХПІ". – 2013.