УДК 004

Т.А.Дмитренко, к.т.н., доцент,
Т.М. Деркач,к.т.н., доцент,
Н.П. Воронюк, магістрантка, 501-ГД,
Полтавський національний технічний університет імені Юрія Кондратюка

ВПРОВАДЖЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЯК ЗАСІБ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Нині всі підприємства та організації особливу увагу починають приділяти питанню збереження інформації, зокрема відомостей, що становлять комерційну або державну таємницю. Адже діяльність установ безпосередньо залежить від уміння керувати інформацією, котра потрібна ринку, але невідома йому. Саме така інформація фіксується, передається та зберігається у вигляді документів. У зв'язку з цим є доцільним оптимізувати захист саме документної інформації.

Як один зі способів обмеження доступу до конфіденційних матеріалів більшість підприємств використовують системи електронного документообігу. Така система передбачає сукупність заходів, котрі значною мірою зменшують ризик несанкціонованого доступу до даних. Серед них:

1. Обмеження прав фізичного доступу до об'єктів системи документообігу;
2. Розмежування прав доступу до файлів;
3. Підтвердження авторства електронного документа;
4. Контроль цілісності електронного документа;
5. Конфіденційність електронного документа;
6. Забезпечення юридичної сили електронного документа;
7. Забезпечення надійності функціонування технічних засобів;
8. Забезпечення резервування каналів зв'язку;
9. Резервне дублювання інформації;
10. Захист від вірусів;
11. Захист від «злому» мереж [4].

Жодна система електронного документообігу не може існувати без розмежування прав доступу. Це потрібно для того, щоб кожен користувач системи мав доступ тільки до тієї частини інформації, котра йому необхідна для виконання своїх посадових обов'язків. Сучасні учені виділяють три моделі розмежування доступу:

1. Рольова модель.
2. Модель Бела і ЛаПадула.
3. Модель Біби [1, с. 98].

Сутність рольової моделі (Role-Based Access Control – RBAC) полягає у тому, що керування доступом стає можливим на основі прав доступу до ролей. Важливими є також самі правила, що регулюють призначення цих ролей, які бувають як індивідуальними, так і груповими.

Модель Белла і ЛаПадули заснована на так званій мандатній моделі керування доступом і регулюванні рівнів доступу.

На думку спеціалістів, модель Біби є своєрідною прямою інверсією попередньої моделі. В її основу покладено групування рівних цілісностей об'єктів і суб'єктів.

Для підтвердження авторства електронного документа та забезпечення його юридичної сили в системах електронного документообігу використовують електронний підпис та електронний цифровий підпис.

Електронний підпис у системі електронного документообігу виглядає як підпис людини на паперових документах. Такий підпис можна отримати на різноманітних сервісах, зокрема на найпоширенішому МЕДок. Даний підпис виступає підтвердженням авторства документа.

Електронний цифровий підпис представлений у вигляді зашифрованих даних, при цьому шифрування відбувається асиметричним способом, який складається з закритого ключа та відкритого. Закритий ключ – це набір виняткових символів відомих тільки автору підпису, за допомогою яких відбувається криптографічне перетворення даних (шифрування). Відкритий ключ передбачає дешифрування отриманої інформації, тобто підтвердження достовірності підпису. Відкритий ключ створюється на основі закритого ключа і може надаватися будь-якому користувачу системи електронного документообігу для перевірки автентичності підпису. Електронний цифровий підпис не тільки підтверджує авторство документа, а й виступає гарантом того, що документ є цілісним і не був видозмінений після його підписання та надає документу юридичну силу.

На відміну від електронного підпису, електронний цифровий підпис можна отримати тільки у спеціалізованих установах. На даний момент на території України діє 24 центри, котрі уповноважені надавати такі підписи, серед них найпопулярнішими є Акредитований центр сертифікації ключів при Держаній фіскальній службі та Центр сертифікації ключів «Україна».

Отже, на основі проведеного аналізу можна зробити висновок, що впровадження системи електронного документообігу на підприємстві значно зменшує ризик несанкціонованого доступу до конфіденційної інформації. Такий результат досягається за допомогою використання комплексу заходів безпеки, серед яких розмежуванню прав доступу та використання електронного цифрового підпису для підтвердження авторства документа та надання йому юридичної сили.

Література

1. Девянин П.Н. Модели безопасности компьютерных систем / П.Н.Девянин. – М.: Академия, 2005. – 144 с.

2. Климов В. О. Информатика и информационные технологии: навч. посіб.. / В. О. Климов, М. В. Гаврилов. – М.: Юрайт, 2015. – 384 с.

3. Про електронний цифровий підпис (зі змінами та доповненнями). Закон України від 22 травня 2003 р. // ВВР. – 2003. – № 36. – Ст. 276.

4. *Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. – 2010. – № 7. – С. 62–64.*