ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

В. О. Ольховський, *к. т. н., доцент;*
В. В. Карцева, *к. е. н., доцент*
Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі»

Сьогодні будь-яка організація використовує електронні документи. Такі документи можуть містити відомості від загальнодоступних до відомостей з обмеженим доступом. Технологічні, виробничі та комерційні дані підприємств і організацій часто мають високу вартість, а їх втрата або витік може привести до фінансових втрат.

Актуальність проблем безпеки підвищується при використанні електронного документообігу. Для вирішення цих завдань необхідні різні організаційно-технічні заходи, які забезпечать захист електронних документів від несанкціонованого прочитання, втрати, випадкової або навмисної модифікації. Реалізація загроз безпеки може настати внаслідок дій зловмисників, помилок персоналу або стихійних факторів. Ці загрози ділять на три основні категорії:

- загрози конфіденційності інформації;
- загрози цілісності інформації;
- загрози доступності інформації.

Для протидії загрозам цілісності та доступності існують спеціальні методи. Для забезпечення інформаційної безпеки використовуються програмні засоби та технічні, організаційні, правові, фізичні методи. Традиційним засобом забезпечення конфіденційності інформації є шифрування – оборотне перетворення відкритих даних в засекречені за певним криптографічним алгоритмом. Шифрування крім конфіденційності забезпечує цілісність і засвідчення джерела інформації.

Криптографічний алгоритм характеризується криптостійкістю. Для збереження конфіденційності є доцільним, щоб за час, витрачений на злом шифрованої інформації, вона безнадійно застаріла або кошти, витрачені на її злом, перевищили вартість самої інформації.

Найпростішим способом шифрування електронних документів є використання функцій захисту MicrosoftOffice – захист на відкриття і захист на зміну документа. Захист на відкриття документа забезпечується завданням пароля. Переглянути захищений документ можна тільки після введення пароля. Захист на зміну дозволяє перегляд документа, редагувати документ можна тільки після введення пароля. Захист від змін дозволяє скопіювати і зберегти документ під іншим ім’ям. Можна заново набрати текст захищеного документа або зберегти копію екрану. Варіантом захисту від змін можна вважати електронний цифровий підпис від MicrosoftOffice – зміна документа призведе до видалення цифрового підпису. Але цифровий підпис від MicrosoftOffice несумісний між версіями. Так, цифровий підпис документу Word 2010 не відображається програмою Word 2007 або Word 2003 і навпаки. Для створення сумісного цифрового підпису існують програми різних розробників.

Використання функцій захисту MicrosoftOffice не користу-ється популярністю у досвідчених користувачів. Через експортні обмеження США в багато країн поставляються версії з обмеженою довжиною ключа шифрування – незалежно від довжини ключа користувача програма формує ключ всього з 5 символів. У старих версіях MicrosoftOffice ключ шифрування зберігався явно в самому файлі і методи його пошуку відомі. У версіях від 2007 і вище система захисту документів значно поліпшена, застосовані стійкі алгоритми шифрування. Тим не менш, існує ряд програм підбору ключів до документів Office, в тому числі і від компанії Microsoft.

Функцію захисту файлів мають архіватори. У зашифрованому архіві виключений перегляд і самого файлу і зміст архіву. Архіватор WinRAR 5 використовує шифрування з довжиною ключа 256 біт. Підбір пароля вимагатиме величезних часових і обчислювальних витрат. Старі версії використовують шифрування AES-128.

Для вирішення завдання захисту електронних документів існує безліч криптографічних програм різних розробників. Фахівці звертають увагу на закритість коду таких програм, тому що немає гарантій у відсутності «закладок» від розробників. Відомою безкоштовною програмою шифрування з відкритим кодом є TrueCrypt. У програмі використані стійкі алгоритми, складні для злому навіть для державних спецслужб. Надійною вважається версія 7.1 – для неї проведено незалежний успішний аудит коду, потім виникли підозри в тиску спецслужб на розробників і проект був закритий.

Програма з файлу-контейнера створює на комп’ютері спеціальну захищену область, яку операційна система сприймає як логічний диск. TrueCrypt шифрує дані при зверненні до цього диску практично непомітно для користувача, і тим самим забезпечує надійний захист без

спеціальних маніпуляцій з файлами. Файл-контейнер може мати будь-який розмір і тип, в папках комп’ютера він може відображатися як фільм або картинка. TrueCrypt має можливість створення на зашифрованому диску в невикористаному просторі прихованого тому. Файл-контейнер TrueCrypt неможливо відрізнити від набору випадкових даних, тобто файл не можна пов’язати з TrueCrypt ні в якій формі і рамках.

Знання програм захисту електронних конфіденційних документів дозволить випускникам забезпечувати безпеку документообігу на підприємствах та в установах.