Мосіюк А.П.
студентка,
Науковий керівник: **Гулак Г.М.**
кандидат технічних наук, доцент,
Навчально-науковий інститут інформаційної безпеки

ЗАХИЩЕНИЙ ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ НА ОСНОВІ СИСТЕМИ ІДЕНТИФІКАЦІЇ

Вплив глобальних процесів інформатизації на суспільне життя зумовлює появу нової сфери відносин, предметом яких є електронний обмін інформацією. У цьому процесі беруть участь органи державної влади, комерційні та некомерційні організації, а також громадяни у своїх офіційних і особистих стосунках. Перед суспільством ставляться нові завдання, вирішити які можна лише застосовуючи сучасні засоби, впроваджуючи нові інформаційні технології. Одним із пріоритетних напрямів розвитку інформатизації суспільства є широке впровадження електронного документообігу.

У даний час все більшого поширення набувають системи захищеного електронного документообігу (ЗЕДО). Це пов'язано із збільшенням кількості конфіденційних документів в органах державної влади і організаціях різної форми власності і активним переходом систем документообігу до електронного вигляду.

Базовий елемент будь СЕД – документ, всередині системи це може бути файл, а може бути запис в базі даних. Говорячи про захищеному документообіг, часто мають на увазі саме захист документів, захист тієї інформації, яку вони в собі несуть. У цьому випадку все зводиться до вже банальною (хоча і не простий) завданню захисту даних від несанкціонованого доступу.

Тут є велика помилка, адже мова йде саме про захист системи, а не тільки про захист даних усередині неї. Це означає, що потрібно захистити також її працездатність, забезпечити швидке відновлення після ушкоджень, збоїв і навіть після знищення. Система – це як живий організм, не достатньо захистити тільки вміст його клітин, необхідно захистити також зв'язку між ними і їх працездатність. Тому до захисту системи електронного документообігу необхідний комплексний підхід, який має на увазі захист на всіх рівнях СЕД. Починаючи від захисту фізичних носіїв інформації, даних на них, і закінчуючи організаційними заходами.

Таким чином, необхідно захищати, по-перше, апаратні елементи системи. Це комп'ютери, сервери, елементи комп'ютерної мережі та мережеве обладнання (як активне – маршрутизатори, switch'i і т.д., так і пасивне – кабелі, розетки і т.д.). Необхідно передбачити такі загрози, як поломка обладнання, доступ зловмисника до обладнання, відключення живлення і т.д.

По-друге, захист необхідна файлів системи. Це файли програмного забезпечення та бази даних, рівень між апаратними пристроями системи і логічними елементами системи та фізичними складовими. В іншому випадку з'являється можливість впливу зловмисником або зовнішніми обставинами на

файли СЕД, не проникаючи в систему, тобто як би зовні. Наприклад, файли бази можуть бути скопійовані зловмисником або пошкоджені в результаті збою операційної системи або обладнання. По-третє, само собою, необхідно захищати документи та інформацію, що знаходяться усередині системи.

Використовуючи такий підхід, можна побудувати систему, захищену на всіх рівнях, і рубежі оборони від загроз на кожному рівні. Можливо, виглядає трохи параноїдально, та й вартість такого захисту може зрівнятися з вартістю самої СЕД, тому завжди потрібно шукати розумний баланс між безпекою і вартістю.

Основні загрози для систем електронного документообігу можуть бути класифіковані таким чином [1]:

– загроза цілісності – це пошкодження, знищення або спотворення інформації, що може бути як ненавмисним у випадках помилок і збоїв, так і зловмисним;

– загроза конфіденційності – це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміна маршрутів слідування і т.д.;

– загроза працездатності системи – це загроза, реалізація якої призводить до порушення або припинення роботи системи, включаючи навмисні атаки, помилки користувачів, а також збої в обладнанні і програмному забезпеченні;

– неможливість доказу авторства – це загроза, що виражається у тому, що якщо в документообігу не використовується електронний цифровий підпис, то неможливо доказати, що саме даний користувач створив даний документ (при цьому неможливо зробити документообіг юридично значимим);

– загроза доступності – це загроза, що порушує можливість за допустимий час отримати потрібну інформацію користувачам, що мають право доступу до неї.

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. Відповідно, в комплекс захисту електронної документації повинні входити наступні заходи [2]:

- обмеження прав фізичного доступу до об’єктів системи документообігу;
- розмежування прав доступу до файлів і папок;
- підтвердження авторства електронного документу;
- контроль цілісності електронного документу;
- конфіденційність електронного документу;
- забезпечення юридичної сили електронного документу;
- забезпечення надійності функціонування технічних засобів;
- забезпечення резервування каналів зв’язку;
- резервне дублювання інформації;
- захист від вірусів;
- захист від «злому» мереж.

У основі реалізації захисту даних методом управління доступом лежать поняття ідентифікації і аутентифікації: ідентифікація користувача – це привласнення йому унікальних параметрів; аутентифікація – встановлення достовірності суб'єкта.

Для спрощення будемо називати процеси встановлення особи користувача і процеси підтвердження легітимності користувача на ту чи іншу дію або інформацію одним терміном – аутентифікацією, розуміючи під ним весь комплекс заходів, що проводяться як на вході користувача в систему, так і постійно протягом його подальшої роботи.

Тут необхідно загострити увагу на методах аутентифікації. Найпоширеніший з них, звичайно, парольний. Основні проблеми, які сильно знижують надійність даного способу – це людський фактор. Навіть якщо змусити користувача використати правильно згенерований пароль, в більшості випадків його можна легко знайти на папірці в столі або під клавіатурою, а особливо «талановиті» зазвичай прикріплюють її прямо на монітор.

Найстаріший з відомих світу способів аутентифікації – майновий. Свого часу повноваження власника скрині підтверджувалися ключами, сьогодні прогрес пішов далеко вперед, і повноваження користувача підтверджуються спеціальним носієм інформації. Існує безліч рішень для майнової аутентифікації користувача: це всілякі USB-ключі, смарт-карти, «пігулки» магнітні картки, в тому числі використовуються і дискети, і CD. Тут також не виключений людський фактор, але зловмисникові необхідно також отримати сам ключ і дізнатися PIN-код.

Максимально надійний для проведення ідентифікації та подальшої аутентифікації спосіб – біометричний, при якому користувач ідентифікується за своїми біометричних даних (це може бути відбиток пальця, сканування сітківки ока, голос) [3]. Однак у цьому випадку вартість рішення вище, а сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов.

Ще один важливий параметр аутентифікації – кількість врахованих факторів. Процес аутентифікації може бути однофакторний, двохфакторний і т.д [4]. Також можливе комбінування різних методів: парольного, майнового і біометричного. Так, наприклад, аутентифікація може проходити за допомогою пароля і відбитка пальця (двохфакторний спосіб).

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно тверезо оцінювати можливі загрози і ризики СЕД і величину можливих втрат від реалізованих загроз. Як вже говорилося, захисту СЕД не зводиться лише до захисту документів і розмежування доступу до них. Залишаються питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв; захисту мережевої середовища, в якій функціонує система, захист каналів передачі даних і мережевого устаткування, можливо виділення СЕД в особливий сегмент мережі. Комплекс організаційних заходів грають роль на кожному рівні захисту, але їм, на жаль, часто нехтують. Але ж тут і інструктаж, і підготовка звичайного персоналу до роботи з конфіденційною інформацією. Погана організація може звести до нуля всі технічні заходи, наскільки досконалі вони б не були.

Список використаних джерел:

1. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника. – 2009. – № 6. – С. 140–143.

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

3. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.

4. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. – 2004. – №45.