УДК 681.3

МАЗНИЧЕНКО Н.І.

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА ОСНОВІ СИСТЕМ ІДЕНТИФІКАЦІЇ

У багатьох сферах діяльності широке розповсюдження одержало використання електронних документів. Використання систем електронного документообігу (СЕД) дозволяє досягти величезного економічного ефекту. Але, упроваджуючи СЕД не можна забувати про безпеку системи. Однією з найважливіших вимог до будь-якої СЕД є забезпечення безпеки електронного обміну документами.

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.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно чітко оцінювати можливі загрози і ризики СЕД і можливі втрати від реалізованих загроз.

Традиційний підхід до захисту інформації заснований на попередньому аналізі загроз і зіставленні їм сукупності механізмів захисту.

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.

Система ідентифікації і аутентифікації користувачів є невід'ємним і важливим

елементом системи захищеного електронного документообігу.

Можна констатувати, що загальними задачами для організації ЗЕД на основі систем ідентифікації і аутентифікації є:

- жорстка ідентифікація і аутентифікація користувачів для організації доступу до інформаційно важливих ресурсів, що захищаються;
- обмеження доступу до конфіденційної інформації і персональних даних;
- блокування несанкціонованого доступу;
- забезпечення доступності публічної інформації.

Тут необхідно загострити увагу на методах ідентифікації і аутентифікації користувачів комп'ютерних систем. Найпоширеніший з них, звичайно, парольний. Головна перевага парольної ідентифікації - це простота реалізації й використання. Основні проблеми, які сильно знижують надійність даного способу - це людський чинник. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

Апаратний (електронний) принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні [3]. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. Але серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані.

Максимально надійний спосіб ідентифікації і аутентифікації - біометричний, при якому користувач ідентифікується за своїми біометричними даними (це може бути відбиток пальця, сканування сітківки ока, голос і т.д.) [4]. Проте в цьому випадку вартість рішення вища, а сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов.

Ще один важливий параметр ідентифікації і аутентифікації - кількість факторів, що враховуються. Тобто, цей процес може бути однофакторним або багатофакторним, коли для визначення особи користувача застосовується відразу кілька параметрів [5]. Також можливе комбінування різних методів: парольного, апаратного і біометричного. Втім, сьогодні найчастіше використається тільки одна пара: парольний захист і токен. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим суттєво підвищує рівень безпеки і захисту систем електронного документообігу.

ЛІТЕРАТУРА

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. Джхунян, В.Л. Электронная идентификация / В.Л. Джхунян, В.Ф. Шаньгин. – М.: NT Press, 2004. – 695 с.

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

5. Шрамко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. - 2004. - №45.

МАЗНИЧЕНКО Наталя Іванівна – старший викладач кафедри інформатики і обчислювальної техніки Національного юридичного університету імені Ярослава Мудрого.

Наукові інтереси:

– *інформаційна безпека, ідентифікація користувачів комп'ютерних систем, біометрія.*