УДК 004.451.36:681.5

В. І.Сабат, Українська академія друкарства, м.Львів

СПОСОБИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ ДОКУМЕНТІВ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ДОКУМЕНТООБІГУ

Анотація. У статті проаналізовано можливі атаки та способи захисту авторських прав електронних документів в автоматизованих системах документообігу (АСДО).

Ключові слова: автоматизована система документообігу, атака, цифровий підпис, цифровий водяний знак.

Вступ. Впровадження електронного документообігу та зростання програмно-апаратних засобів зчитування електронної інформації ставить нові вимоги та задачі до захисту інформації, яка міститься в електронних документах. Зокрема це стосується забезпечення авторських прав електронних документів, які, на відміну від паперових носіїв, не мають обмежень в накладі чи у швидкості поширення та тиражуванні. У більшості документів певної виробничої або організаційної предметної області АСДО міститься інформація про управлінські дії, які необхідно здійснити об'єктом на суб'єктами виробничого процесу, тому порушення авторства документа може призвести до непередбачливих наслідків і є реальною загрозою для функціонування таких систем. Отже все-більше стають актуальними проблеми ідентифікації авторства документів і, відповідно, захисту інформації в електронних документах.

Основна частина. До можливих зовнішніх та внутрішніх атак на документи в АСДО можна віднести такі:

— атаки доступу;
— атаки модифікації;
— атаки на відмову в обслуговуванні;
— атаки на відмову від зобов'язань. [1]

Якщо атака доступу здійснюється через несанкіоноване відкриття документа і отримання зловмисником інформації, для перегляду якої у нього немає дозволу, то її можна не враховувати як таку, що порушує авторство документа. Але через несанкціонований доступ зловмисник може здійснити інші види атак, які зможуть знищити чи змінити інформацію в документі на шляху від автора до виконавця.

Як правило автором документів в АСДО є адміністратор організації, а у великих організаціях, з адміністративно-розподіленими повноваженнями, авторами можуть бути керівники підрозділів системи управління. В таких організаціях загроза неадекватних управлінських дій найчастіше з'являється

тоді, коли відбувається збій в системі електронного документообігу. Тому при розробленні політики безпеки організації вкрай важливо, щоб був встановлений основний механізм для аутентифікації користувачів і адміністраторів, а також правильно визначена система надання повноважень службами доступу та ідентифікації.

При здійсненні атаки модифікації порушується цілісність інформації в документі, що руйнує автентичність документа його початковому стану і, відповідно, його авторство. Є три види атаки модифікації: заміна, додавання і видалення інформації в документах. Атака заміни направлена як проти секретної, так і загальнодоступної інформації. Інші види атак — додавання нових даних, або видалення, означає переміщення існуючих даних в документах з метою зміни його управляючих дій.

Модифікувати інформацію, що зберігається в електронних документах, значно легше ніж в паперових. Якщо врахувати те, що зловмисник має доступ до системи, то така операція залишає після себе мінімум доказів. За відсутності санкціонованого доступу до файлів зловмисник спочатку повинен забезпечити собі вхід в систему або видалити файли дозволів. Атаки такого роду використовують вразливі місця систем, наприклад, «проломи» в безпеці сервера, або вразливості в програмному забезпеченні, так звані «експлойти», які дозволяють здійснити контроль над системою.

Атаки на відмову в обслуговуванні (Denial-of-service, DoS) — це атаки, що забороняють легальному користувачеві використання системи, доступу до інформації в електронних документах або можливостей комп'ютерів. В результаті DoS-атаки, направленої проти інформації в документі, вона знищується, спотворюється або переноситься в недоступне місце. Інший вид DoS-атак направлений на програми обробки даних чи програми, які відображають інформацію в документах, або на комп'ютерну систему, в якій ці програми виконуються. У разі успіху подібної атаки вирішення задач, що виконуються за допомогою такої програми, стає неможливим.

DoS-атака не спрямована на порушення авторства документа, а її мета — вивід з ладу комп'ютерної системи, внаслідок чого сама система, встановлені на ній програми і вся збережена інформація стає недоступною.

Атаки на відмову від зобов'язань безпосередньо пов'язані з порушенням авторства документа. Вони виконуються набагато успішніше, якщо інформація представлена в електронному вигляді. Адже електронний документ може створити і відправити будь-хто. Наприклад, у супровідній інформації до документа (його індексації) можна легко змінити відомості про автора, час створення документа тощо (у програмі редактора документів). Це справедливо і для документів, які пересилаються через мережні технології. Система може призначити будь-яку IP-адресу і замаскуватися під іншу систему. В результаті — зловмисник видає себе за іншу людину, використовуючи чужі документи, або навпаки, — сам автор документа заперечує своє авторство, щоб уникнути відповідальності.

До найбільш поширених технічних засобів реалізації захисту авторських

прав електронних документів можна віднести шифрування. Але цей метод лише обмежує доступ до документів для несанкціонованих осіб і не дає можливості використовувати інформацію, з дотриманням авторського права, для інших суб'єктів цифрового середовища. Причому, необхідно зазначити, що не всі криптографічні методи забезпечують авторство особи. Так, наприклад, шифрування із секретним ключем дозволяє здійснити криптографічний захист інформації, яка міститься в документах, але не надає інформації про авторство документа, оскільки будь-який суб'єкт може, при наявності закритого секретного ключа, модифікувати електронну інформацію в документі. Проте, шифрування з відкритим ключем дозволяє використовувати два ключі — секретний та відкритий і тим самим забезпечує процедуру цифрового підпису (ЦП) для автора документу. Процедури надання цифрового підпису на сьогодні прописані на законодавчому рівні і цей метод аутентифікації особи, яка створила електронний документ, досить успішно використовується у сучасних АСДО. [2]

Другий метод, який забезпечує авторське право на тиражування та копіювання, електронних видань, за умови дотриманням авторства особи, яка їх створила, і поширюється не лише для санкціонованих осіб, але й для будь-яких суб'єктів цифрового середовища, полягає у створенні ідентифікації електронних видань. Такі ідентифікатори повинні підтверджувати авторство кожного з екземплярів електронного видання. Один з таких способів ідентифікації електронних видань, що реалізуються в цифрових середовищах є цифровий водяний знак (ЦВЗ), який містить інформацію, за допомогою якої можна ідентифікувати авторський екземпляр видання. [3] До основних вимог які повинен забезпечувати ЦВЗ, можна віднести такі:

— ЦВЗ повинен не призводити до спотворення інформації електронного документа або видання, в яке його впроваджено;
— ЦВЗ повинен бути невидимим, при традиційному використанні електронних документів користувачами, чи іншими учасниками процесу захисту авторських прав;
— ЦВЗ повинен бути стійким до можливих перетворень цифрового середовища, пов'язаних із спробами його модифікації, чи спотворення, з метою досягнення можливості несанкціонованого тиражування;
— оскільки для роботи з електронним документом необхідно використовувати відповідні програмно-апаратні засоби, то ЦВЗ повинен бути стійким до можливих стандартних технологічних перетворень;
— ЦВЗ повинен містити всю інформацію, яка є необхідною для ідентифікації електронного документа та підтверджувати його авторські права.

ЦВЗ можна впроваджувати на початку створення документа і не тільки в текстові електронні документи, але й в документи з мультимедійним контентом. Наприклад, якщо документ містить графічні зображення, то за допомогою спеціальних алгоритмів модифікуються певні області піксельного зображення таким чином, щоб забезпечити вищевказані вимоги до ЦВЗ. Також ця технологія захисту авторства документів досить поширена і для

інших електронних видань, наприклад, для відео- та аудіо-інформації.

Висновок. Для АСДО, які використовують електронні документи пріоритетним напрямком є забезпечення захисту інформації в документах від зовнішніх атак. Описаним способам порушення авторства документа від несанкціонованого доступу, модифікації, відмови від зобов'язань чи його знищення можуть протидіяти злагоджені системи захисту і служби безпеки організації, які оснащені усіма технологіями від криптографічного захисту інформації, використання цифрових підписів для документів до цифрових водяних знаків.

Якщо дотримуватись вимог, що визначають ЦВЗ як ідентифікатора електронного документу, то ЦВЗ можна використовувати у якості базового засобу ідентифікації в системі захисту авторських прав для електронних документів, які містять не тільки текстову інформацію, але й мультимедійний контент.

1. *Сабат В. І.* Особливості захисту інформації в автоматизованих системах документообігу / В. І. Сабат. — Збірник наукових праць, випуск 70, ІПМЕ ім. Г. Є. Пухова НАН України. — К., 2014. — С. 119–123.
2. *Золотарьова І. О.* Автоматизація документообігу. Навчальний посібник / І. О. Золотарьова, Р. К. Бутова. — Харків : Вид. ХНЕУ, 2008. — 170 с.
3. *Карпінець В. В.* Методи захисту векторних зображень цифровими водяними знаками : монографія / В. В. Карпінець, Ю. Є. Яремчук. — Вінниця : ВНТУ, 2013. — 156 с.

Поступила 21.9.2015р.

УДК 519.8

Ю.М. Романишин[1),2)], д.т.н., С.Р. Петрицька[1)]
[1)] Національний університет "Львівська політехніка"
[2)] Uniwersytet Warmińsko-Mazurski w Olsztynie

ЕНЕРГЕТИЧНІ ОСОБЛИВОСТІ АКТИВАЦІЇ МОДЕЛЕЙ НЕЙРОНА

Розглянуто енергетичні особливості активації моделі Ходжкіна-Хакслі нейрона. Визначено співвідношення між пороговими значеннями густини струму прямокутного імпульсу активації та його тривалості, обчислено порогове значення енергії вхідного імпульсу, що дало змогу обгрунтувати побудову енергетичної моделі активації нейрона.

Ключові слова: активація нейрона, модель Ходжкіна-Хакслі, енергія

Рассмотрены энергетические особенности активации модели Ходжкина-Хаксли нейрона. Определено соотношение между пороговыми значениями плотности тока прямоугольного импульса активации и его длительности, вычислено пороговое значение энергии входного импульса, что дало

