УДК 004.451.36:681.5

В. І.Сабат, УАД, м.Львів

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ДОКУМЕНТООБІГУ

Анотація. У статті проаналізовано особливості захисту інформації та інформаційних ресурсів в автоматизованих системах документообігу на основі опису функцій служб інформаційної безпеки та типів атак, яким вони протистоять.

Ключові слова. Автоматизовані системи документообігу, служби інформаційної безпеки, атаки.

Аннотация. Статья посвящена анализу особенностям защиты информации и информационных ресурсов в автоматизированных системах документооборота на основе описания функций служб информационной безопасности та типов атак, которым они противостоят.

Ключевые слова. Автоматизированные системы документооборота, службы информационной безопасности, атаки.

Актуальність. При вирішенні задач захисту під інформацією розуміють відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання. В залежності від форм представлення інформація може бути розділена на мовну, телекомунікаційну та документовану.

Мовна інформація виникає в процесі розмов між суб'єктами, в роботі систем зв'язку, звукопідсилення і звуковідтворення. Телекомунікаційна інформація циркулює в технічних засобах обробки та зберігання інформації, а також в каналах зв'язку при її передачі. До документованої інформації, або документів, належить інформація, записана на матеріальних або електронних носіях разом з ідентифікуючими її реквізитами. До інформаційних процесів належать процеси збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформації.

Під інформаційною системою документообігу (ІСД) розуміють впорядковані множини чи масиви документів та інформаційні технологій, що реалізують інформаційні процеси. До інформаційних ресурсів в рамках системи документообігу належать документи і масиви документів, існуючі окремо або в складі інформаційних систем.

Інформацію, яка розміщується в електронних документах, поділяють на відкриту і секретну (з обмеженим доступом). Відкрита інформація вільно поширюється в межах системи і доступна усім її суб'єктам. Секретна інформація обмеженого доступу може бути віднесена до державної таємниці або конфіденційної інформації для фізичних чи юридичних осіб. Згідно українського законодавства до конфіденційної інформації належать [1]:

— службова таємниця (лікарська, адвокатська, таємниця суду і слідства тощо);
— комерційна таємниця;

— персональні дані (відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особу).

Отже, інформація є одним із об'єктів цивільного права, в тому числі і права власності, володіння і користування. Власник інформаційних ресурсів, систем і технологій — це суб'єкт з повноваженнями володіння, користування і розпорядження вказаними об'єктами. Під користувачем інформації розуміють суб'єкта, який звертається до інформаційної системи із запитом на отримання необхідної інформації та надання йому прав на користування нею.

В автоматизованих системах документообігу (АСДО) кожен документ може містити такі основні види інформації:

— інструктивну, що містить перелік визначених інструкції, яких повинен дотримуватись суб'єкт АСДО, щодо власних прав і повноважень згідно розробленої політики безпеки у структурі системи в якій він працює;
— інформативну, що реалізується у формі наказів, оголошень та інших дій, пов'язаних з діяльністю підприємства чи його структур;
— виконавчу, що забезпечує можливість здійснювати адекватні дії суб'єктів над об'єктами в межах АСДО;
— адміністративну, яка призначена для контролю за користуванням і виконанням документів;
— управлінську, що забезпечує належну роботу усіх служб, задіяних в функціонуванні системи захисту (СЗ) тощо.

Для успішної роботи системи захисту і убезпечення її від зовнішніх та внутрішніх атак, як відомо, необхідно залучити служби інформаційної безпеки (СІБ). До таких служб належать: служба ідентифікації, служба доступності, служба конфіденційності та служба цілісності. Кожна з цих служб направлена на боротьбу з певним типом атак (рис. 1).

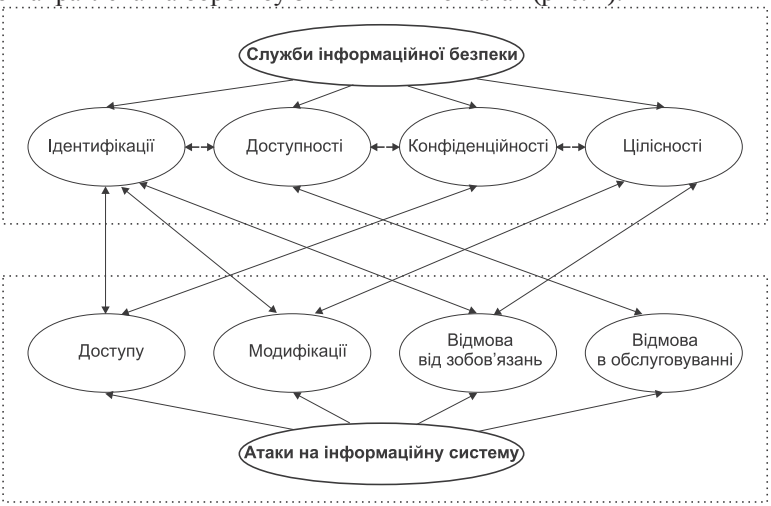

Рис. 1. Служби інформаційної безпеки та типи атак на ІС

Особливості використання служб інформаційної безпеки в рамках окремої організації залежать від рівня оцінки ризику в цій організації і планування системи безпеки [2].

До атак в АСДО слід віднести такі зовнішні та внутрішні дії, які порушують безпеку електронних документів в ІС: атака доступу до інформації, атака модифікації інформації, відмова від прийнятих в ІС зобов'язань та відмова в обслуговуванні.

Захист інформації в електронних документах можливий лише при злагодженій роботі усіх служб інформаційної безпеки а також у постійному моніторингу ІС на наявність можливих небезпек, що можуть призвести до зовнішніх чи внутрішніх атак на АСДО.

Як видно з рис. 1, важливе місце в роботі системи захисту належить службі ідентифікації суб'єктів, які з тих чи інших мотивів здійснюють спроби впливу на ІС з метою доступу до інформації, що міститься в електронних документах чи їх модифікації. Також до функцій системи ідентифікації відноситься аутентифікація користувачів, яка базується на трьох факторах: те що ви знаєте, те що ви маєте, те ким ви є. У більшості систем захисту документів використовується двохфакторна аутентифікація, але для підвищення надійності систем захисту в АСДО може бути введена трьохфакторна система аутентифікації, яка включає в себе також засоби біометричного контролю. Щодо протистоянь атакам на відмову від зобов'язань прийнятих в електронних документах найкраще використовувати цифровий підпис, що також забезпечує ідентичність особи, яка завіряє електронний документ на відповідність самому документу.

Основна функція служби доступності полягає в забезпеченні вільного доступу до апаратно-програмного забезпечення та інформаційних ресурсів АСДО для санкціонованих користувачів. Зрозуміло, що така доступність забезпечується при достовірній ідентифікації усіх суб'єктів ІС і при відповідній підтримці служби ідентифікації. Окрім забезпечення надійної роботи усіх програмних та технічних засобів, служба доступності також протидіє зовнішнім DoS-атакам через т.зв. мережі заражених шкідливим кодом персональних комп'ютерів (ботнетів) і відновленням робочого стану АСДО після таких атак.

До атак доступу також слід віднести ненавмисні дії, які можуть виникнути з тих чи інших причин (помилки користувачів, форс-мажорні обставини тощо), тому в арсеналі служби доступності повинні бути резервні копії дисків та описані процедури реагування на випадок швидкого відновлення функціонування ІС. Під ефективністю захисту інформації в цьому випадку вважається ступінь відповідності результатів захисту інформації до поставленої мети, яка задовольняє певний рівень безпеки системи. Отже об'єктом захисту може бути не лише інформація, яка міститься в документі, але й її носій чи інформаційний процес.

Протидією від несанкціонованого витоку інформації в АСДО, при спробі несанкціонованих і ненавмисних атак доступу до неї займається служба

конфіденційності. Конфіденційність є суб'єктивною характеристикою інформації, пов'язаної з об'єктивною необхідністю захисту законних інтересів одних суб'єктів від інших. При підтримці служби ідентифікації, служба конфіденційності надає права доступу до інформації для усіх користувачів ІС і суб'єктів які працюють з електронними документами в межах системи. На основі розроблених процедур надання доступу до інформації, згідно прийнятої політики безпеки в організації, визначається рівень таємності документа, який може поширюватись разом з ним у вигляді супровідної службової інформації. Служба конфіденційності для кожного суб'єкта ІС визначає рівень доступу до інформації і узгоджує його з рівнем таємності для кожного документа в АСДО. Цей рівень таємності може видозмінюватись з часом, коли інформація втрачає свою актуальність, і документ може перейти в статус вільно доступного, або навпаки — зростати з часом до більш таємного [3].

До надійних засобів захисту електронних документів від несанкціонованого доступу належить шифрування. Шифруванням інформації називають процес її перетворення, при якому зміст інформації стає незрозумілим для несанкціонованих суб'єктів. Результат шифрування інформації називають криптограмою. Зворотний процес відновлення інформації — її розшифровуванням. Алгоритми, використовувані при шифруванні і розшифровуванні інформації, зазвичай не є конфіденційними, але конфіденційність забезпечується використанням при шифруванні додаткового параметра, який називається ключем шифрування. Знання ключа шифрування дозволяє виконати правильне розшифрування інформації [4].

Служба цілісності інформації в електронних документах забезпечує її незмінність в умовах випадкового і (або) навмисного спотворення чи руйнування. Цілісність є частиною більш широкої характеристики інформації — її достовірності, що включає крім цілісності ще й повноту і точність відображення предметної області. Отже служба цілісності інформації забезпечує її важливий показник — якість інформації. Хоча під якістю інформації розуміють більш ширше поняття — сукупність властивостей, що обумовлюють придатність інформації задовольняти визначені потреби її користувачів відповідно до призначення інформації. Проте, одним із показників якості інформації є її захищеність — підтримання на заданому рівні тих параметрів інформації, які характеризують установ¬ленний статус її зберігання, обробки та використання.

Згідно визначення основних функцій служби цілісності інформації випливає, що основна її мета — це протидія будь-яким атакам модифікації інформації від несанкціонованих суб'єктів ІС і визначення достовірності (авторства) документа, тобто протидії атакам відмови від зобов'язань.

Висновок. При правильному підході до розроблення політики безпеки АСДО, а саме: затвердженні документованих норм, правил і практичних прийомів, що регулюють управління, захист і розподіл інформації в електронних документах, а також при активній співпраці усіх служб

інформаційної безпеки, які в сукупності протидіють зовнішнім та внутрішнім атакам на ІС, можна досягти оптимального рівня захисту для будь-якої організації, що займається виготовленням, поширенням, користуванням і архівуванням електронних документів. На етапі проектування таких систем документообігу необхідно також визначити вразливості і загрози для ІС, що дозволить оцінити усі ризики і можливі затрати на розробку системи захисту для конкретної організації.

1. Закон України «Про захист інформації в автоматизованих системах».
2. Искусство защиты и взлома информации / Д. Скляров. — СПб, 2004. — 288 с.
3. Дурняк Б. В. Загальна організація використання інформаційних засобів для створення системи управління повноваженнями / Б. В. Дурняк, Л. Є. Шведова, В. І. Сабат // Збірник наукових праць. [ІПМЕ ім. Г. Є. Пухова НАН України]. — К., 2011. — Вип. 59. — С. 200–207.
4. *Бабаш Шанкин*. Криптография. Аспекты защиты / Шанкин Бабаш. — М., 2002. — 384 с.

Поступила 10.02.2014р.

УДК 655.28.022.2

Б.М.Гавриш, УАД, м.Львів

РОЗДІЛЬНА ЗДАТНІСТЬ ПРИСТРОЇВ ВИВЕДЕННЯ І МЕТОДИ МАСШТАБУВАННЯ РАСТРОВИХ ЗОБРАЖЕНЬ

Анотація. Проаналізований вплив роздільної здатності на якість растрових зображень, відтворюваних поліграфічними методами. Досліджено особливості масштабування при виведенні векторних і растрових малюнків.

Ключові слова. Роздільна здатність, друкарське зображення, піксель, масштабування.

Abstract. The influence of the resolution on the quality raster images reproduced polygraph methods. The features of the derivation of the scaling vector and bitmap drawings.

Keywords. The resolution, printing image, pixel, scaling.

Вступ

Для друку растрових зображень, які складаються з точок, особливу важливість має поняття роздільної здатності. При цьому слід розрізняти: роздільну здатність оригіналу; роздільну здатність екранного зображення; роздільну здатність друкарського зображення [1-4].

Роздільна здатність – це рівень деталізації бітового зображення. Розміри у пікселях відповідають загальній кількості пікселів вздовж ширини або висоти цифрового зображення. Вона вимірюється у пікселях на дюйм (pixel