УДК 35.077.6

Бородкіна І.Л.
Київський національний університет культури і мистецтв

Бородкін Г.О.
Національний університет біоресурсів і природокористування України

МЕТОДИ Й ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Для швидкого та якісного управління в установах різного рівня все більш широко використовуються системи електронного документообігу. Сьогодні існує велика кількість методів і технологій захисту інформації, призначених забезпечити конфіденційність, цілісність і доступність інформації, що циркулює в цих системах. У роботі представлена систематизація та класифікація сучасних методів і технологій захисту інформації в системах електронного документообігу, наведені їх переваги й недоліки. Виконане дослідження спрямоване на полегшення організації системи комплексного та ефективного захисту інформації під час використання систем електронного документообігу.

Ключові слова: *електронний документ, електронний документообіг, система електронного документообігу, захист інформації, шифрування даних.*

Постановка проблеми. Починаючи з останніх десятиріч XX століття спостерігається постійне розширення сфер застосування комп'ютерних мереж, збільшення кількості користувачів як локальними комп'ютерними мережами, так і мережами, підключеними до глобальної комп'ютерної мережі Інтернет. Це призводить до зменшення інформаційної закритості даних, які зберігаються на мережених серверах і клієнтських комп'ютерах організацій та установ.

Однією зі сфер застосування комп'ютерних мереж останніми роками стало впровадження в органи державної влади й управління систем електронного документообігу. За таких умов національна безпека країни істотно залежить від інформаційної безпеки, забезпечення захисту інформації, що зберігається й опрацьовується в системах електронного документообігу органів державної влади та управління. При цьому в ході технічного прогресу ця залежність зростатиме.

Отже, розвиток інформаційних технологій, широке розповсюдження мережі Internet і постійне зростання вартості інформації зумовлюють той факт, що захист даних у системах електронного документообігу сьогодні являє собою одну з найважливіших проблем у сфері інформаційних технологій.

Аналіз останніх досліджень і публікацій. Із 1 січня 2006 року в Україні набрав чинності Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [1]. Відповідно до цього Закону, захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі. Закон визначає, що об'єктами захисту в інформаційній системі є інформація, що обробляється в ній, і програмне забезпечення, яке призначено для обробки цієї інформації.

Більш детально поняття «об'єкт захисту» розглянуто в роботі Т. Нішанбаєва, Ф. Рахімова [5], де під об'єктом захисту розуміється такий структурний компонент системи, в якому знаходиться або може знаходитись інформація, що підлягає захисту. Об'єкт захисту повинен відповідати таким умовам:

– належати до одного й того ж організаційного компонента системи;

– брати участь у здійсненні одних і тих самих функцій, пов'язаних з автоматизованою обробкою інформації в системі;

– бути локалізованим (обмеженим) з погляду територіального розташування системи.

Захисту в комп'ютерній системі підлягає будь-яка документована інформація, неправомірне поводження з якою може завдати збитків її власнику, користувачу або іншій особі. Передусім сюди належать відомості, що являють собою державну таємницю; конфіденційна документована інформація; інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, персональні дані, що зберігаються в інформаційних системах.

Цілями захисту інформації в інформаційно-телекомунікаційних системах є [1; 5]:

1. запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;

2. запобігання загрозам безпеки особистості, суспільства, держави;

3. запобігання несанкціонованим діям щодо знищення, модифікації, спотворення, копіювання, блокування інформації;

4. запобігання іншим формам незаконного втручання в інформаційні системи, забезпечення правового режиму документованої інформації як об'єкта власності;

5. збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;

6. захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, що є в інформаційних системах;

7. забезпечення прав суб'єктів в інформаційних процесах і під час розробки, виробництва й застосування інформаційних систем, технологій і засобів їх забезпечення.

Згідно із Законом [2], захист інформації в інформаційній системі повинен здійснюватись шляхом створення комплексної системи захисту інформації з використанням засобів захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Закон визначає два напрями, у яких повинен здійснюватись захист інформації: технічний і криптографічний.

Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів і/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності й режиму доступу до інформації.

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

У процесі розробки систем захисту інформації до них напрацювалися деякі загальні вимоги, які сформульовані Ж. Солцером та М. Шредером (США) [3; 4]:

1. Простота механізму захисту. Чим краще збігається уявлення користувача про систему захисту з її фактичними можливостями, тим менше помилок виникатиме в процесі роботи.

2. Дозволи повинні переважати над заборонами. Нормальним режимом роботи вважається відсутність доступу, а механізм захисту повинен бути заснований на умовах, при яких доступ дозволяється. Допуск до інформації надається лише тим користувачам, яким він необхідний.

3. Перевірка повноважень користувача при будь-якому зверненні до будь-якого об'єкта інформації. Це означає, що захист здійснюється на загальносистемному рівні й припускає абсолютно надійне визначення джерела будь-якого звернення до інформації.

4. Розділення повноважень. Надійний захист інформації в системі потребує визначення мінімального круга повноважень для будь-якої програми й будь-якого користувача системи.

5. Трудомісткість проникнення в систему. Чинник трудомісткості залежить від кількості проб, які потрібно зробити для успішного проникнення в систему.

6. Реєстрація проникнень у систему. Іноді вважають, що вигідніше реєструвати випадки проникнення, ніж будувати складні системи захисту.

Отже, під захистом інформації в системах електронного документообігу як різновиді інформаційних систем колективного використання варто розуміти сукупність методів і засобів, що забезпечують цілісність, конфіденційність, достовірність, автентичність і доступність (тобто можливість використання) інформації в умовах дії на неї загроз природного або штучного характеру.

Регулярне застосування засобів і методів захисту інформації допомагає забезпечити потрібну надійність інформації, що зберігається та обробляється з використанням засобів системи електронного документообігу [5; 6]. При цьому під надійністю інформації в системі електронного документообігу розуміється інтегральний показник, який характеризує якість інформації з погляду:

– фізичної цілісності, тобто наявності або відсутності спотворень або знищення елементів цієї інформації;

– довіри до інформації (автентичності), тобто наявності (відсутності) в ній підміни (несанкціонованої модифікації) її елементів при збереженні цілісності;

– безпеки інформації (конфіденційності), тобто наявності (відсутності) несанкціонованого отримання її особами або процесами, які не мають на це відповідних повноважень;

– недопущення несанкціонованого розмноження інформації.

Ефективність захисту інформації в системі електронного документообігу досягається лише в тому випадку, якщо забезпечується її надійність на всіх об'єктах та елементах системи, які можуть бути піддані загрозам з боку дестабілізуючих факторів.

Складність вирішення завдань захисту інформації в системах електронного документообігу зумовлюють такі фактори:

1. високі вимоги до цілісності системного та прикладного програмного забезпечення;

2. високі вимоги до цілісності електронних документів (довідкові, статистичні, звітні документи, інструкції тощо), що зберігаються в системі;

3. перехід на безпаперову технологію вимагає забезпечення юридичної значущості електронних документів;

4. розподілене використання ресурсів системи електронного документообігу вимагає забезпечення безпеки інформації на рівні розмежування доступу до інформації;

5. низка електронних документів вимагає забезпечення безпеки на рівні утаєння змісту документа, а в деяких випадках і недопущення несанкціонованого розмноження.

Отже, всі засоби, призначені для захисту інформації, у той чи інший спосіб регламентують, забороняють або обмежують користувачам можливість доступу до тієї або іншої інформації.

Постановка завдання. Мета статті – проаналізувати й узагальнити інформацію про наявні сьогодні засоби, методи підходи та технології захисту інформації в системах електронного документообігу.

Виклад основного матеріалу дослідження. Виходячи зі структури системи електронного документообігу, до об'єктів захисту в системах електронного документообігу можна зарахувати:

– робочі станції користувачів системи;

– робочі станції адміністраторів (мережі, бази даних, системи захисту тощо);

– сервери (мережеві, баз даних, додатків);

– апаратуру зв'язку (модеми, маршрутизатори);

– канали зв'язку (виділені або комутовані);

– периферійні пристрої колективного використання;

– приміщення, пов'язані з автоматизованою обробкою інформації (місця встановлення обладнання, сховища машинних носіїв інформації тощо).

Найпоширенішими шляхами витоку інформації із системи електронного документообігу, як і з будь-якої інформаційної системи, є:

– викрадення носіїв інформації та документів, які є результатом роботи системи;

– копіювання інформації на ПК;

– несанкціоноване підключення до апаратури та ліній зв'язку;

– перехоплення електромагнітного випромінювання в процесі обробки інформації.

Крім того, користувачі системи можуть припускатися різних помилок і бути предметом зловживань.

Запобігання витоку інформації із системи переліченими вище шляхами здійснюється як технічними, так і криптографічними методами захисту інформації. На жаль, фізичний доступ сторонніх до конфіденційної інформації, що зберігається на жорстких дисках комп'ютерів робочих станцій або серверів, не завжди можна виключити за допомогою організаційних заходів і технічних методів захисту (відомі приклади, коли, незважаючи на всі запобіжні засоби, особливо цінна інформація просто викрадалася шляхом вилучення носія, на якому ця інформація зберігалась). Для убезпечення даних на випадок вилучення носіїв необхідно застосовувати процедури криптографічного перетворення інформації, які посідають особливе місце в будь-якій інформаційній системі, в тому числі й у системі електронного документообігу, оскільки саме вони захищають безпосередньо документи. У результаті перетворення інформації вміст документів стає недоступним без застосування відповідного ключа та зворотного перетворення. Залежно від способу використання натепер існують симетрична та асиметрична криптографічні системи. Симетричні криптосистеми для шифрування й дешифрування використовують один ключ. Недоліком таких систем варто вважати складність передачі ключа. Існує проблема пошуку надійного способу обміну ключами.

В асиметричних криптографічних системах для шифрування й дешифрування використовуються різні ключі. Ключ шифрування є відкритим, а таємність ключа дешифрування зберігається. При цьому відкритий ключ шифрування складений так, що він не дає змоги обчислити секретний ключ дешифрування. Математичний взаємозв'язок між закритим і відкритим ключами робить кожну пару ключів унікальною.

Принципи асиметричної криптографії покладено в основу механізму захисту документів з

використанням електронного цифрового підпису, який набуває все більшого розповсюдження в системах електронного документообігу. У таких системах також використовуються закритий і відкритий ключі електронного цифрового підпису. Відкритий ключ відомий усім користувачам системи й призначений для перевірки електронного цифрового підпису. Він допомагає визначити автора підпису та достовірність електронного документа, не даючи змоги обчислити секретний ключ.

Застосування криптографічних методів захисту інформації допомагає захищати безпосередньо інформацію, а не доступ до неї. Завдяки цим методам убезпечуються дані безпосередньо в першоджерелі системи електронного документообігу – в базі даних, сховищі, на сервері. Однак постійне шифрування й дешифрування інформації призводить до суттєвого зниження продуктивності бази даних і, відповідно, системи загалом.

Проблему можна вирішити шляхом побудови відповідної стратегії захисту інформації, тобто раціонального використання комбінації різних рівнів захисту – від апаратного рівня до рівня програмних додатків.

Крім криптографічних методів захисту інформації, застосовуються методи стеганографічного захисту інформації, тобто методи, які приховують сам факт існування повідомлення й не дають змоги сторонній особі дізнатися про його існування. Сьогодні існує багато методів стеганографічного захисту інформації, які базуються на фізичних, хімічних, голографічних та інших підходах [7].

Цифрова стеганографія базується на приховуванні або вбудовуванні додаткової інформації в цифрові (як правило, мультимедійні) об'єкти, викликаючи при цьому деякі їх спотворення без утрати функціональності. Методи стеганографії допомагають замінити несуттєві частки даних на конфіденційну інформацію, оскільки можливості людини розрізняти дрібні зміни кольору або звуку обмежені. До переваг класичної стеганографії можна зарахувати доступність засобів реалізації, а основними недоліками є складність практичної реалізації та можливість випадкового вияву повідомлення. Стеганографія зазвичай використовується спільно з методами криптографії, доповнюючи її.

Новим і дуже перспективним напрямом у технологіях захисту інформації є поєднання USB-брелків або смарт-карток і спеціального програмного забезпечення, призначеного для шифрування даних. Така технологія одержала назву Secret Disk. Вона заснована на принципі шифрування даних на жорсткому диску, при цьому доступ до них можна отримати тільки за допомогою допоміжного ключа, який зберігається на зовнішньому пристрої (USB-брелці або смарт-картці). Перевага такого рішення полягає в тому, що захист даних забезпечується за допомогою алгоритму переміщення даних, а для того, щоб дістати доступ до зашифрованих даних, потрібні спеціальний пристрій (USB-брелок або смарт-картка) і введений із клавіатури пароль.

Принцип захисту даних за допомогою системи Secret Disk полягає в створенні на комп'ютері користувача (або сервері компанії) захищеного ресурсу – секретного диску, призначеного для безпечного зберігання конфіденційної інформації. У разі збереження дані в захищених ресурсах шифруються. Доступ до цієї інформації та її розшифровка здійснюються тільки після приєднання до USB-порту комп'ютера електронного ключа. Отже, інформація, захищена системою, доступна тільки її власникам. Проте, якщо інформація, яка зберігається на цьому захищеному ресурсі, необхідна декільком його колегам, власник може дати їм право цією інформацією користуватися. Для цього їм необхідно тільки мати власний електронний ключ. Інші користувачі не бачитимуть захищений ресурс, для них він буде недоступним. Вони можуть навіть і не здогадуватись про його наявність.

Висновки. Сучасний розвиток комп'ютерних технологій створив необхідні умови для впровадження в процеси управління установами систем електронного документообігу. При цьому актуальності набула проблема забезпечення інформаційної безпеки на всіх рівнях упровадження та експлуатації таких систем. Виникла потреба створення комплексної системи захисту інформації, що охоплюватиме весь життєвий цикл систем електронного документообігу – від розробки до утилізації – і весь технологічний ланцюжок збирання, передавання, зберігання, обробки й видачі інформації. Проаналізувавши всі можливі способи захисту та утаємнення інформації в системах електронного документообігу, можна резюмувати, що лише комплексне застосування всіх відомих на теперішній час організаційних, апаратних і програмних засобів у змозі забезпечити необхідний рівень таємності інформації.

Список літератури:

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. Відомості Верховної Ради України (ВВР). 1994. № 31. С. 286.
2. Про інформацію: Закон України. Відомості Верховної Ради України (ВВР). 1992. № 48. С. 650.
3. Боровікова Н. Способи захисту конфіденційної інформації. URL: http://www.aladdin.ru/press/archive/article282.php.
4. Домарев В.В. Безопасность информационных технологий. Системный подход. Киев; Москва; Санкт-Петербург: Торгово-издательский дом «DiaSoft», 2004. 975с.
5. Нішанбаєв Т., Рахімов Ф. Основи системного захисту даних в розподілених інформаційних системах. URL: http://ru.infocom.uz/more.php?id=A747_0_1_0_M.
6. Захист інформації в процесі зберігання. URL: http://www.securit.ru/solutions/store/.
7. Сучасні стеганографічні методи захисту інформації / О. Стасюк, С. Гнатюк, Н. Довгич, М. Літош. Захист інформації. 2011. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/1994.doi:10.18372/2410-7840.13.1994.

МЕТОДЫ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Для быстрого и качественного управления в учреждениях различного уровня все более широко используются системы электронного документооборота. На сегодняшний день существует большое количество методов и технологий защиты информации, предназначенных обеспечить конфиденциальность, целостность и доступность информации, циркулирующей в этих системах. В работе представлена систематизация и классификация современных методов и технологий защиты информации в системах электронного документооборота, описаны их преимущества и недостатки. Проведенное исследование направлено на облегчение организации системы комплексной и эффективной защиты информации при использовании систем электронного документооборота.

Ключевые слова: *электронный документ, электронный документооборот, система электронного документооборота, защита информации, шифрование данных.*

METHODS AND TECHNOLOGIES OF INFORMATION SECURITY IN ELECTRONIC MANAGEMENT SYSTEMS

Electronic document management systems are increasingly used for fast and high-quality management in institutions of various levels. Today, there are many methods and technologies for protecting information designed to ensure the confidentiality, integrity and availability of information circulating in these systems. The paper presents the systematization and classification of modern methods and technologies of information security in electronic document circulation systems, their advantages and disadvantages are presented. The research is aimed at facilitating the organization of the system of integrated and effective information protection in the use of electronic document management systems.

Key words: *electronic document, electronic document management, electronic document management system, data protection, data encryption.*