Информационные системы и технологии

УДК 004.056

І.О. Розломій

Черкаський національний університет імені Богдана Хмельницького,

бульвар Шевченка, 81, корпус 3, м. Черкаси, 18000, Україна.

Виявлення та нейтралізація загроз безпеки електронних документів на основі аналізу їх життєвого циклу

В даній статті розглянуто принципи та переваги впровадження систем електронного документообігу (СЕД). Досліджено основні властивості електронних документів (ЕД) такі, як конфіденційність, цілісність та достовірність. Сформовано перелік функцій ЕД. Показана схема життєвого циклу ЕД, що дозволяє формалізувати множину загроз на кожному етапі. Розглянуто стандартний набір загроз та порушень безпеки ЕД. Проведено аналіз можливих засобів забезпечення інформаційної безпеки і механізмів захисту ЕД. Розглянуто принцип використання головного реквізиту ЕД, електронного цифрового підпису (ЕЦП). Побудовано схеми створення та перевірки ЕЦП на основі використання хеш-функцій. Запропоновано математичну модель інформаційної безпеки ЕД. Відповідно до отриманих результатів, сформульовано вимоги щодо забезпечення захисту ЕД. Бібл. 5, рис. 3.

Ключові слова: *електронний документ; життєвий цикл; інформаційна безпека; цифровий підпис; хеш-функція; ідентифікація; аутентифікація.*

Вступ

Швидкий розвиток і впровадження сучасних інформаційно-комунікаційних технологій став причиною глобальної трансформації індустріального суспільства в інформаційне. Все більша частина інформації зберігається і передається в електронному вигляді. Проблема необхідності автоматизації управління документообігом давно набула практичного значення.

Більшість організацій впроваджують системи електронного документообігу і вже на власному досвіді змогли оцінити всі переваги нових технологій роботи з документами. Використання електронних документів (ЕД) отримало широке розповсюдження в багатьох сферах людської діяльності. Використання СЕД сприяє ефективній організації всіє управлінської структури, для якої вони призначені, а також дозволяє досягнути великого економічного ефекту [1].

Постановка проблеми

Використання інформаційних технологій в процесі електронного документообігу передбачає створення надійної системи безпеки і захисту інформації. З вдосконаленням програмно-технічних засобів автоматизованої обробки інформаційних потоків в СЕД проблема захисту ЕД стає особливо актуальною. Насамперед, це обумовлено переходом від традиційного документообігу до електронних технологій створення, збереження та обміну даними. Також цьому сприяло створення обчислювальних систем, глобальних мереж і розширення доступу до інформаційних ресурсів.

Аналіз останніх досліджень та публікацій

Даній проблемі присвячені роботи Астахової Т.С., Ярочкина В.І., Панасенка С.П. та інших вчених. Проте, за умов достатньо розвинутих технологій в сфері інформаційних злочинів, проблема захисту потребує ефективних шляхів її вирішення.

Формулювання мети дослідження

Мета роботи – дослідження особливостей впровадження СЕД. Аналіз ЕД, їх головних властивостей, функцій. Визначення можливих загроз порушення інформаційної безпеки (ІБ) документів та засобів їх нейтралізації, зокрема електронного цифрового підпису (ЕЦП) та побудова математичної моделі ІБ електронних документів.

Основний матеріал

В електронному середовищі процес обробки документованої інформації представляє собою складний організаційно-технічний процес, що супроводжується загрозами ІБ. Використання СЕД дозволяє організувати передачу даних, що дозволяє організувати контроль виконання документів.

Системи електронного документообігу – автоматизовані системи, що забезпечують процес

створення, управління доступом і розповсюдження великих обсягів документів у комп'ютерних мережах, а також забезпечують контроль над потоками документів в організації. Головним компонентом СЕД є електронний документ, в якому інформація зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити. ЕД мають специфічні властивості та функції [2].

Основними функціями ЕД в СЕД є:

- забезпечення ефективного керування за рахунок контролю виконання на всіх етапах життєвого циклу ЕД;
- безпечний і швидкий доступ до ЕД в системі;
- підтримка комунікацій, зручний обмін ЕД між організаційними структурами.

ЕД в системі проходять певну послідовність етапів, які складають їх життєвий цикл.

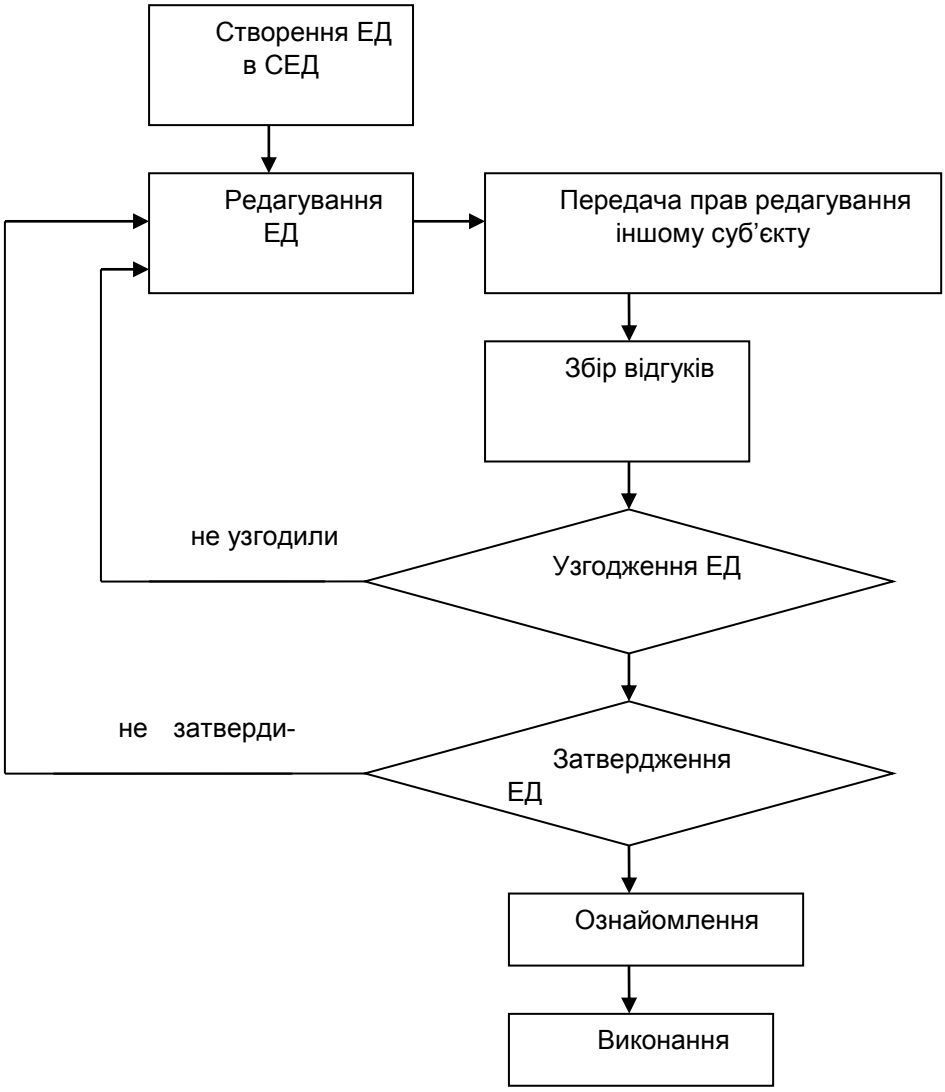

Рис. 1. Блок схема життєвого циклу ЕД в СЕД

Чітке розуміння життєвого циклу ЕД в СЕД дозволяє виявити можливі загрози безпеці на кожному етапі.

Характерними властивостями ЕД є конфіденційність, цілісність та достовірність. Цілісність ЕД – характеризує їх незмінність, достовірність, повноту інформації, що містять ЕД, тобто така їх властивість, яка гарантує чітко визначену структуру ЕД [3]. Порушення цілісності – це загрози, при реалізації яких інформація втрачає значимість, юридичну силу. Загрози цілісності інформації, що зберігається в СЕД чи передається по каналах зв'язку, які спрямовані на її редагування чи спотворення, що призводять до порушення якості чи повного знищення. Порушення цілісності інформації може мати випадковий і навмисний характер[3].

Порушення конфіденційності може виникнути, як наслідок крадіжки, перехоплення інформації, зміни маршрутів руху ЕД. Загрози порушення конфіденційності спрямовані на розголошення конфіденційної чи секретної інформа-

ції. В разі реалізації цих загроз інформація стає відомою для суб'єктів, які не мають до неї доступу.

Доступність – це властивість ЕД, яка передбачає відсутність перешкод доступу до них і правомірному їх використанню власником чи уповноваженими суб'єктами. Доступність характеризує можливість несанкціонованого доступу до документів, що зберігаються в СЕД в будь-який момент часу [4].

Для забезпечення високого рівня безпеки ЕД, надійного функціонування СЕД необхідно створити умови захисту системи від існуючих загроз. Система захисту ЕД – комплекс програмно-технічних засобів, спрямованих на виявлення і усунення можливих загроз ІБ. Для створення системи захисту необхідно деталізувати множину можливих загроз, провести аналіз вразливостей СЕД, ризику здійснення загроз і можливих збитків, що можуть виникнути у разі порушення безпеки. Одним з таких порушень є несанкціонований доступ (НсД) до ЕД, отримання суб'єктом прав доступу, на які він не має дозволу. Порушення правил розмежування доступу може стати причиною порушення цілісності, достовірності та конфіденційності ЕД. Порушення ІБ – сукупність умов і факторів (явищ, дій, процесів), що спричинюють потенційну небезпеку, що призводить до непередбачуваних фактів таких, як витік інформації, модифікація та знищення інформації.

Основу гарантування інформаційної безпеки в інформаційно-телекомунікаційних системах становлять криптографічні методи та засоби захисту інформації. Беручи до уваги те, що швидкісні криптографічні перетворення даних є найефективнішим засобом забезпечення таких характеристик безпеки інформаційних ресурсів, як конфіденційність і цілісність, то, безумовно, перспективним напрямком досліджень є розробка методів підвищення продуктивності криптографічних систем.

Особливе місце в електронному документообігу займає задача ідентифікації користувачів, вирішити яку покликаний електронний цифровий підпис (ЕЦП) – найбільш зручний сучасний інструмент для здійснення угод у віддаленому режимі та обміну юридично значимої документацією/ ЕЦП гарантує достовірність, забезпечує цілісність, дозволяє створювати корпоративну систему обміну електронними документами. Так само одним з головних достоїнств підпису є можливість удосконалити контроль за обігом, використанням та зберіганням електронної документації на підприємстві.

Правовий статус ЕД забезпечується використанням ЕЦП, який ідентифікує автора підписаного документа. Відповідно до закону України «Про електронний цифровий підпис», ЕЦП – реквізит ЕД, отриманий в результаті криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувала [5]. Цей Закон визначає правовий статус ЕЦП та регулює відносини, що виникають при його використанні.

Оскільки ЕД можуть бути достатньо великими, то часто ЕЦП накладається не на сам документ, а на його хеш. Хеш обчислюють за допомогою криптографічних хеш-функцій, що гарантує виявлення змін в документі при перевірці підпису.

Технологія використання ЕЦП передбачає електронний обмін даними між абонентами мережі. Для відправника і отримувача генерується пара ключів: відкритий і закритий. Закритий ключ зберігається у відправника в таємниці і використовується ним з метою формування ЕЦП. Відкритий ключ відомий отримувачеві і призначений для перевірки ЕЦП підписаного ЕД. Система ЕЦП включає процедуру формування підпису та його перевірку.

Процедура формування ЕЦП використовує закритий ключ відправника, а процес перевірки підпису – відкритий ключ відправника. Спочатку відправник генерує пару ключів і повідомляє відкритий ключ отримувачеві для подальшої перевірки підпису. Потім відправник обчислює значення хеш-функції електронного документу[6].

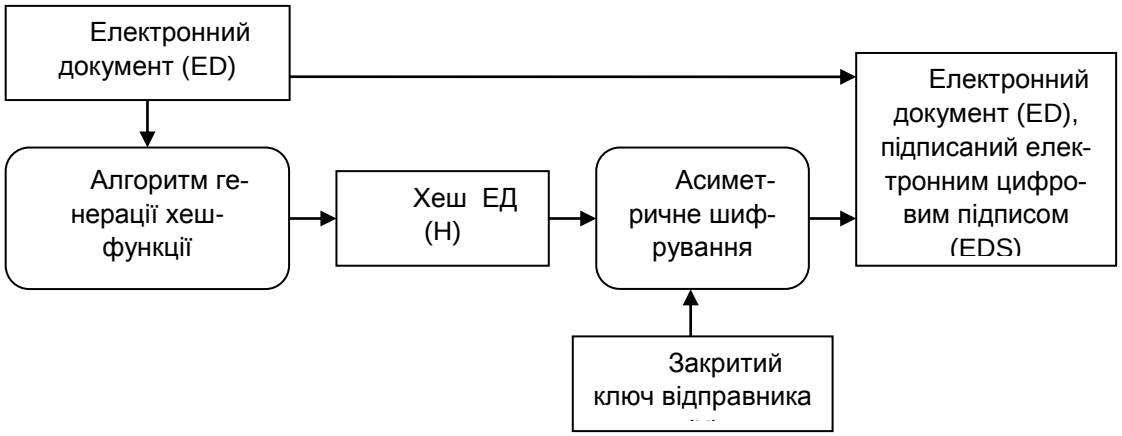

Рис. 2. Схематичне зображення формування ЕЦП

Хеш-фунція служить для обчислення хешу ЕД (H) – фіксована кількість бітів, що характеризує повністю документ. Відправник шифрує хеш за допомогою свого секретного ключа, отримана в результаті пара чисел представляє собою ЕЦП даного ЕД. Потім підписаний ЕД надходить до отримувача. Використання хеш-функцій дозволяє формувати криптостійкі контрольні суми ЕД.

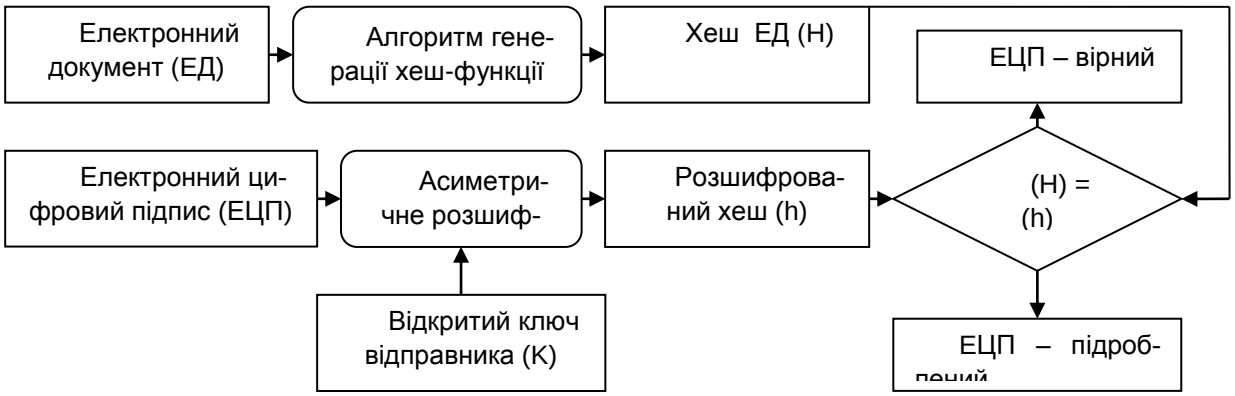

Рис. 3. Схематичне зображення перевірки ЕЦП

При перевірці ЕЦП отримувач ЕД розшифровує прийнятий хеш (H) відкритим ключем відправника. Крім того, отримувач самостійно за допомогою хеш-функції (H) вираховує хеш (h) отриманого ЕД і порівнює його з розшифрованим. Якщо (H) і (h) співпадають, то ЕЦП – вірний. В іншому випадку або ЕЦП фальсифікований, або змінено вміст ЕД. Співпадання (H) і (h) є критерієм цілісності ЕД і підтвердження його авторства.

Враховуючи основні властивості електронних документів, математичну модель інформаційної безпеки ЕД можна представити в вигляді задачі (1).

$$\sum_{i}^{n} f(C_i, K_i, D_i) \to \max л \qquad (1)$$

де $f(C_i, K_i, D_i)$ – значення функції ІБ для *i-ї* загрози безпеці, n – кількість загроз безпеці ЕД, C_i, K_i, D_i – ймовірності порушення цілісності, конфіденційності та достовірності ЕД для *i-ї* загрози.

Таким чином, захищена СЕД має передбачувати реалізацію, як мінімум таких механізмів захисту: забезпечення цілісності, безпечного доступу, конфіденційності та достовірності документів.

Висновки

Забезпечення захисту ЕД на сьогоднішній день є дуже масштабною і актуальною темою, оскільки зараз практично всі галузі діяльності базуються на інформаційних технологіях. ЕД має свій життєвий цикл, функції, властивості та вимоги. Для забезпечення автентичності та цілісності документа використовується ЕЦП, який є його обов'язковим реквізитом, створюється і перевіряється за допомогою механізмів закритого і відкритого ключів з відповідними вимогами щодо їх створення та розподілу. Таким чином, ЕЦП є основним, і практично єдиним з запропонованих, рішенням для забезпечення достовірності документа, який дозволяє, на основі криптографічних методів, встановити авторство і цілісність ЕД. Враховуючи швидкі темпи розвитку сучасних комп'ютерних систем і математичних методів крипто аналізу, практична схема ЕЦП повинна вдосконалюватися, щоб гарантувати достатній рівень захисту на декілька років вперед.

Список використаних джерел

1. *Black J., Rogaway P., Shrimpton T*. Black-box analysis of the block-cipher-based hash-function constructions from PGV. Advances in Cryptology, CRYPTO'02, Lecture Notes in Computer Science, Springer-Verlag, 2002.
2. *Астахова Л.В., Лужнов В.С.* Проблемы организации защищенного документооборота с использованием электронной подписи на предприятиях малого бизнеса// Вестник ЮФУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2013. – 7с.
3. *Астахова Т.С., Чадаева Е.П.* Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа// Известия Томского политехнического университета, Хабаровск.– 2012. – №6.–5 с.
4. *Елисеев Н.И*. Модель угроз безопасности информации при ее обработке в системе защищенного документооборота// Известия ЮФУ. Технические науки Тематический выпуск. – 2013. – 7 с.
5. Закон України «Про електронний цифровий підпис»*//* Відомості Верховної Ради України (ВВР). – 2003. – №36. – 18 с.
6. *Панасенко С.П.* Защита электронных документов: целостность и конфиденциальность// Информационные технологии. – 2000. – № 3. – 8 с.

Поступила в редакцию 21 ноября 2015 г.

УДК 004.056

И.А. Розломий

Черкасский национальный университет имени Богдана Хмельницкого,

бульвар Шевченка, 81, корпус 3, г. Черкассы, 18000, Украина.

Выявление и нейтрализация угроз безопасности электронных документов на основе анализа их жизненного цикла

В данной статье рассмотрены принципы и преимущества внедрения систем электронного документооборота (СЭД). Исследованы основные свойства электронных документов (ЭД) такие, как конфиденциальность, целостность и достоверность. Сформирован перечень функций ЭД. Показана схема жизненного цикла ЭД, позволяет формализовать множество угроз на каждом этапе. Рассмотрены стандартный набор угроз и нарушений безопасности ЭД. Проведен анализ возможных средств обеспечению информационной безопасности и механизмов защиты ЭД. Рассмотрены принцип использования главного реквизита ЭД, электронной цифровой подписи (ЭЦП). Построены схемы создания и проверки ЭЦП на основе использования хэш-функций. Предложена математическая модель информационной безопасности ЭД. Согласно полученным результатам, сформулированы требования по обеспечению защиты ЭД. Библ. 5, рис. 3.

Ключневые слова: *электронный документ; жизненный цикл; информационная безопасность; цифровая подпись; хэш-функция; идентификация; аутентификация.*

UDC 004.056

I. Rozlomii

Cherkassy Bogdan Khmelnitsky National University,

boulevard Shevchenko, 81, Chercassy, 18000, Ukraine.

Detection and neutralization of threats to the security of electronic documents by analyzing their life cycle

The principles and benefits of implementing electronic document management systems (EMDS) have been researched in the article. The basic properties of electronic documents (ED) such as confidentiality, integrity and authenticity have been discovered. The list of main functions of electronic dokuments was formed. The life cycle ED, that allowing formalized set of threats at each stage has been shown. The standard set of threats and security breaches of ED has been considered. The possible means of ensuring information security and protection mechanisms of ED has been analyzed. The principle of using the main props of ED, electronic digital signature (EDS) has been considered. A scheme to create and verify electronic signature through the use of hash functions has been constructed. The mathematical model of information security units has been proposed. According to the results, we have come up with the list of suggestions regarding the development of protection of ED. Referense 5, Figures 3.

Keywords: *electronic document; lifecycle; information security; digital signature; hash function; identification; authentication.*

Reference

1. *Black, J., Rogaway, P., Shrimpton, T.* (2002). Black-box analysis of the block-cipher-based hash-function constructions from PGV. Advances in Cryptology, CRYPTO'02, Lecture Notes in Computer Science, Springer-Verlag, P. 76.
2. *Astakhova, T. S. and Chadaeva, E. P.* (2012). Using Digital Signature for Ensuring Integrity and Authenticity of the Document. Bulletin of the Tomsk Polytechnic University, Habarovsk, no. 6, P.5. (Rus)
3. *Astakhova, L. V. and Luzhnov, V. S.* (2013). Problems of the organization of secure document using the electronic signature in small businesses. Bulletin of South Federation University, A series of "Computer technology, management, electronics", P. 7. (Rus)
4. *Eleseev, N. A.* (2013). Threat Model for the Secure Document. Engineering Special Issue, P.7. (Rus)
5. *Panasenko, S. P.* (2000). Securing Digital Documents. Integrity and Confidentiality in Information Technology, no. 3, P. 8. (Ukr)
6. The Law of Ukraine (2003). On electronic digital signature. Supreme Council of Ukraine, no. 36, P.18. (Ukr)