УДК 004.056

РОЗЛОМІЙ І. О.
Черкаський національний університет імені Богдана Хмельницького

ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЯ ЗАГРОЗ БЕЗПЕКИ ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА ОСНОВІ АНАЛІЗУ ЇХ ЖИТТЄВОГО ЦИКЛУ

Мета. *Підвищення рівня інформаційної безпеки (ІБ) електронних документів (ЕД).*

Методика. *В статті розглянуто особливості впровадження систем електронного документообігу (СЕД). Проведено аналіз ЕД, їх головних властивостей та функцій. Розглянуто стандартний набір загроз з метою побудови математичної моделі ІБ та можливих засобів і механізмів захисту ЕД.*

Результати. *Досліджено основні властивості 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 принцип використання головного реквізиту ЕД, електронного цифрового підпису (ЕЦП). Побудовано схеми створення та перевірки ЕЦП на основі використання хеш-функцій.*

Наукова новизна. *На основі дослідження властивостей ЕД запропоновано математичну модель інформаційної безпеки ЕД.*

Практична значимість. *Відповідно до отриманих результатів, визначено засоби нейтралізації загроз та сформульовано вимоги щодо забезпечення захисту ЕД.*

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

Вступ. Розвиток суспільства визначається рівнем домінування інформаційного середовища. Інформація стала невід'ємною складовою функціонування всіх суспільних установ і життя людини зокрема. 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. Технічний прогрес, обумовлений розвитком інформаційного суспільства передбачає використання технологій електронного обміну даними.

В зв'язку зі збільшенням обсягів інформації, яку доводиться оброблювати, виникає необхідність впровадження систем електронного документообігу (СЕД). Використання електронних документів (ЕД) отримало широке розповсюдження в таких сферах людської діяльності, як освіта, медицина, державних органах управління та інших структурах. Разом з розвитком сучасних інформаційно-технічних можливостей виникають нові ризики та загрози, що призводять до некоректного функціонування системи, зниження надійності, а також значних матеріальних втрат. Тому, використання СЕД обов'язково має супроводжуватися надійною системою захисту.

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

Постановка завдання. Аналіз науково-технічної літератури показує, що за останні роки розроблено багато методів забезпечення безпеки інформаційних ресурсів, зокрема ЕД. Вченими запропоновані різні підходи, щодо способів виявлення загроз, оцінки рівня

захищеності ЕД та засобів захисту. Проте, існує ряд невирішених раніше питань надійного функціонування СЕД. Насамперед, ці питання пов'язані з дослідженням множини загроз на кожному етапі життєвого циклу ЕД в системі, а також способів їх уникнення та нейтралізації.

Мета. Метою роботи є підвищення рівня ІБ електронних документів. Для досягнення мети досліджено особливості впровадження СЕД, проведено аналіз ЕД, їх головних властивостей, функцій. Визначено множину можливих загроз порушення ІБ документів та засобів їх нейтралізації, зокрема електронного цифрового підпису та побудовано математичну модель ІБ електронних документів.

Результати дослідження. 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 контролювати процес виконання документів.

Система електронного документообігу – інформаційна, автоматизована система, яка забезпечує безперервний процес руху ЕД, що відображає діяльність певної структури і контроль її керування. Така система дозволяє керувати документами на протязі всього їх життєвого циклу: від створення до повного видалення. СЕД дає можливість автоматизувати всі процеси обробки електронних даних, що сприяє підвищенню швидкості роботи та зниженню втрат пов'язаних з обміном інформації. Використання СЕД сприяє ефективній організації всієї управлінської структури, для якої вони призначені, а також дозволяє досягнути великого економічного ефекту [1]. Основу будь-якої СЕД складають електронні документи та процеси над ними. ЕД представляє собою аналог паперового документу, створеного на цифровому носії, включаючи обов'язкові реквізити. ЕД мають специфічні властивості та функції.

Основними функціями ЕД в СЕД є:

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

ЕД в системі проходять певну послідовність етапів, які складають їх життєвий цикл, структура якого показана на рис. 1.

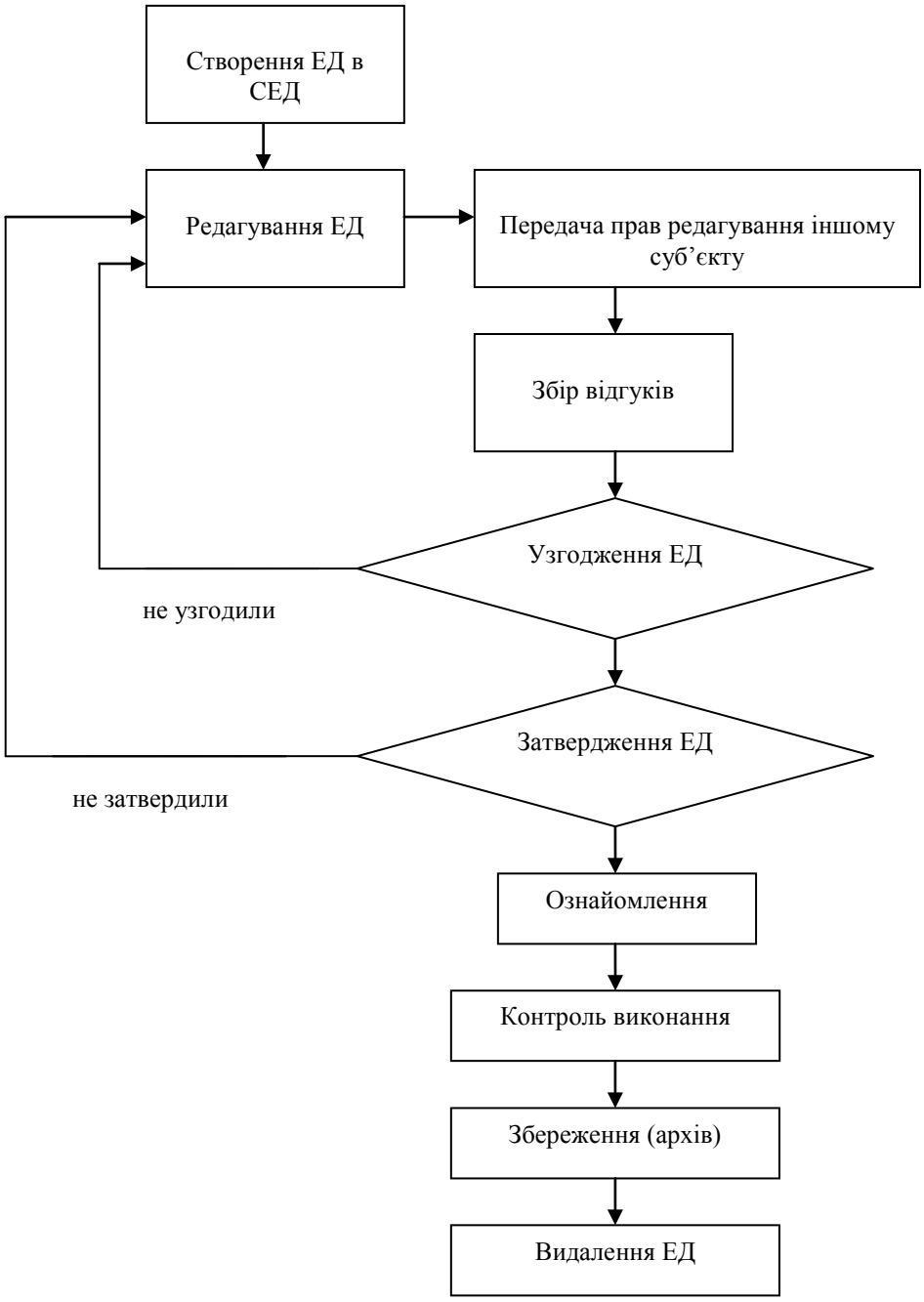

Рис.1. **Структура життєвого циклу ЕД в СЕД**

Аналіз життєвого циклу ЕД є важливим чинником при розробці механізмів захисту, оскільки чітке розуміння життєвого циклу ЕД в СЕД дозволяє виявити можливі загрози безпеці на кожному етапі. Для забезпечення стабільності функціонування СЕД потрібно ужити заходів захисту ЕД при його створенні, передачі, обробці, збереженні, виконанні, а також за умов впливу зовнішніх чинників.

Характерними властивостями ЕД є конфіденційність, цілісність та достовірність. Цілісність ЕД гарантує незмінність, достовірність, повноту інформації, що містять ЕД, тобто така їх властивість, яка гарантує чітко визначену структуру ЕД [2]. Порушення цілісності –

це загрози, при реалізації яких інформація втрачає значимість, юридичну силу. Порушення цілісності інформації може мати випадковий і навмисний характер [3]. Порушення конфіденційності виникає внаслідок отримання несанкціонованого доступу (НсД) до даних. НсД можна отримати шляхом перехоплення інформації, зміни маршрутів руху ЕД та іншими способами шахрайства. Загрози порушення конфіденційності спрямовані на розголошення конфіденційної чи секретної інформації. В разі реалізації цих загроз інформація стає відомою для суб'єктів, які не мають до неї доступу. 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 до ЕД, отримання суб'єктом прав доступу, на які він не має дозволу. Порушення ІБ – сукупність умов і факторів (явищ, подій, процесів), що компрометують один чи декілька аспектів ІБ. Загрози становлять потенційну небезпеку, що призводить до непередбачуваних фактів таких, як витік, 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 однією з переваг 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. Закон України «Про електронний цифровий підпис» регулює відносини, що виникають в процесі використання ЕЦП [5]. 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]. Алгоритм формування ЕЦП показаний на рис. 2.

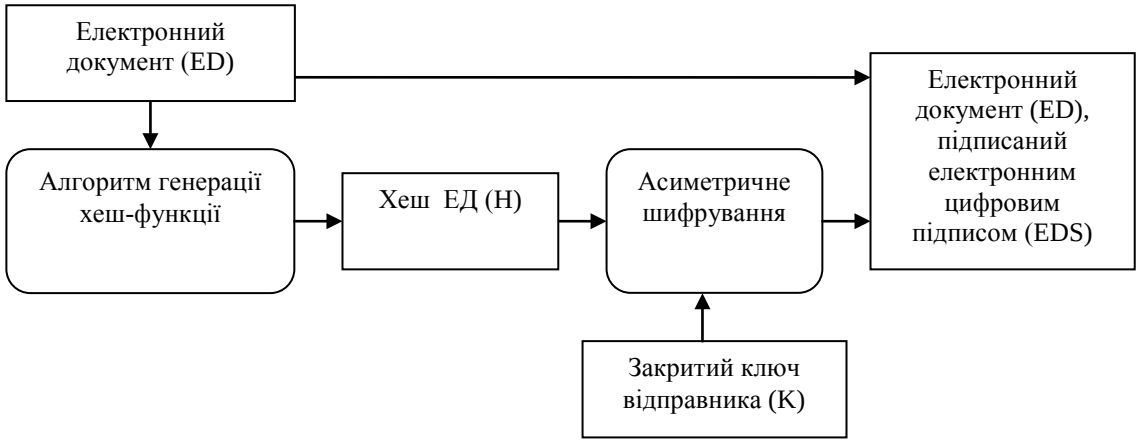

Рис. 2. **Алгоритм формування ЕЦП**

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 [7].

При перевірці ЕЦП отримувач ЕД розшифровує прийнятий хеш (H) відкритим ключем відправника. Крім того, отримувач самостійно за допомогою хеш-функції (H) обчислює хеш (h) отриманого ЕД і порівнює його з розшифрованим [8]. Якщо (H) і (h) співпадають, то ЕЦП – вірний. В іншому випадку – ЕЦП фальсифікований, або змінено вміст ЕД. Співпадання (H) і (h) є критерієм цілісності ЕД і підтвердженням його авторства. Алгоритм перевірки ЕЦП показаний на рис. 3.

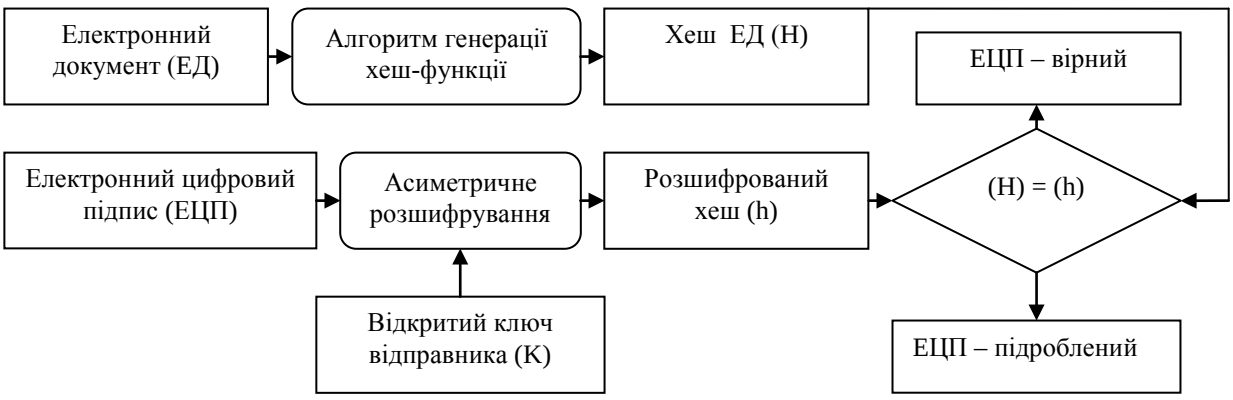

Рис. 3. **Алгоритм перевірки ЕЦП**

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

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

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 і-ї загрози. Дані про ймовірність порушення можна отримати на основі експертних оцінок.

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

Висновки. В висновку зазначимо, що активне використання технологій електронного обміну суттєво підвищило вразливість інформації, що циркулює в сучасних інформаційних системах. Описані в статті принципи впровадження СЕД демонструють необхідність створення надійної системи безпеки і захисту ЕД. Побудована структура життєвого циклу ЕД в системі дозволяє виявити можливі загрози ІБ на всіх етапах – починаючи від створення документу до остаточного його видалення. Досліджено механізми формування та перевірки головного реквізиту електронного документа – ЕЦП. На основі дослідження властивостей та загроз ЕД запропоновано математичну модель інформаційної безпеки ЕД. Відповідно до отриманих результатів, визначено засоби нейтралізації загроз та сформульовано вимоги щодо забезпечення захисту ЕД.

Список використаних джерел

1. Астахова Л.В., Лужнов В.С. Проблемы организации защищенного документооборота с использованием электронной подписи на предприятиях малого бизнеса// Вестник ЮФУ. Компьютерные технологии, управление, радиоэлектроника. – Выпуск №3 (13). –2013. –72– 79 с.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – «Гелиос АРВ». – 2002. – 480 с.

3. Линник О.В. Виявлення підробки електронного цифрового підпису для встановлення змін у документі// Юридичний науковий електронний журнал. Випуск № 2. – 2015. – 209– 211 с.

4. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота// Вестник АГТУ. Компьютерное обеспечение и вычислительная техника. Серия: управление, вычислительная техника и информатика. Выпуск №2. –2009. – 140– 143 с.

5. Закон України «Про електронний цифровий підпис»// Відомості Верховної Ради України (ВВР) №36. – 2003. – 18 с.

6. Королев И.Д. Анализ безопасности информации при применении модели отнесения документов автоматизированной системы к информационным областям ответственности исполнителей// Политематический сетевой электронный научный журнал КГАУ. Автоматика. Вычислительная техника. № 93. – 2013. – 1–11 с.

7. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей святи от экспертных данных при расчетах с

использованием модели нечетких множеств// Вопросы кибербезопасности. Кибернетика. – Выпуск №2(3). – 2014. – 33– 39 с.

8. 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.

References

1. Astakhova L.V. and Luzhnov V.S. (2013), "Problems of organization of protected electronic document circulation using electronic digital signature at the small businesses enterprises", Bulletin of SFU. Computer technology, management, electronics, no. 3, 72– 79 p. [in Russian]

2. Alferov A.P., Zubov A.U., Kuzmin A.S. and Cheremushkin A.V. (2002), "Principles of cryptography ", 480 p. [in Russian]

3. Linnik O.V. (2015) "Identifying fake electronic digital signature to establish changes in the document", Law Journal, no. 2, 209– 211 p. [in Ukrainian]

4. Dosmukhamedov B.R. (2009), "The analysis of threats of the information of systems of electronic document circulation", no. 2, 140– 143 p. [in Russian]

5. The Law of Ukraine (2003), "On electronic digital signature", Supreme Council of Ukraine, no. 36, 18 p. [in Ukrainian]

6. Korolev I.D. (2013), "The safety information analysis in applying of documental reference model of the automated system in the informational areas of the actor's liability", Multidisciplinary network electronic scientific journal of the KSAU. Automation. Computer Engineering, no. 93, 1– 11 p. [in Russian]

7. Belfer R.A., Kaluzshnyi D.A. and Tarasova D.V. (2014), "Analysis of dependence of risk level of safety of communication networks of expert data during calculations with the use of a model of the illegible sets", Questions cyber security. Cybernetics, no. 2, 31– 39 p. [in Russian]

8. Black J., Rogaway P. and 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. [in English]

Рекомендовано до публікації д.т.н, проф. Рудницьким В. М.

ВЫЯВЛЕНИЕ И НЕЙТРАЛИЗАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ НА ОСНОВЕ АНАЛИЗА ИХ ЖИЗНЕННОГО ЦИКЛА

РОЗЛОМИЙ И. А.

Черкасский национальный университет имени Богдана Хмельницкого

Цель. Повышение уровня информационной безопасности (ИБ) электронных документов (ЭД).

Методика. В статье рассмотрены особенности внедрения систем электронного документооборота (СЭД). Проведен анализ ЭД, их основных свойств и функций. Рассмотрен стандартный набор угроз с целью построения математической модели ИБ и возможных средств и механизмов защиты ЭД.

Результаты. Исследованы основные свойства ЭД такие, как конфиденциальность, целостность и достоверность. Сформирован перечень функций ЭД. Показана схема жизненного цикла ЭД, которая позволяет формализовать множество угроз на каждом этапе. Рассмотрен принцип использования главного реквизита ЭД, электронной цифровой подписи (ЭЦП). Построены схемы создания и проверки ЭЦП на основе использования хэш-функций.

Научная новизна. На основе исследования свойств ЭД предложена математическая модель информационной безопасности ЭД.

Практическая значимость. Согласно полученным результатам, определены средства нейтрализации угроз и сформулированы требования по обеспечению защиты ЭД.

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

DETECTION AND NEUTRALIZATION OF THREATS TO THE SECURITY OF ELECTRONIC DOCUMENTS BY ANALYZING THEIR LIFE CYCLE

ROZLOMII I. A.
Cherkassy Bogdan Khmelnytckyi National University

Purpose. Increased information security of electronic documents.

Methodology. The aspects of deployment and functioning of the Document Management System (DMS) were considered in article. The main properties and functions of electronic document has been analyzed. A standard set of threats has been considered for creating mathematical model information security and possible tools of electronic protection.

Findings. The main properties of electronic documents, such as confidentiality, integrity, certainty were researched. The list of functions of electronic documents was created. The scheme lifecycle of electronic document has been shown which allows formalized set of threats at each stage. The principle of using of the main props of electronic documents, such as electronic digital signature has been considered. The schemes of creation and verification electronic digital signature based on the using hash-functions has been constructed.

Originality. The mathematical model of information security of electronic documents was offered based on the researching properties of electronic documents.

Practical value. According to the achieved results, identified means of neutralization of threats and formulated requirements of electronic documents protection.

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