УДК 004.056

І. О. Розломій, *аспірантка,*
Г. В. Косенюк, *к.т.н.*
Черкаський національний університет імені Богдана Хмельницького
б-р Шевченка, 81, м. Черкаси, 18000, Україна

ОСНОВНІ МЕХАНІЗМИ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ВІД ФАЛЬСИФІКАЦІЙ

Стаття присвячена проблемі забезпечення інформаційної безпеки електронних документів (ЕД) і захисту інформації в системах електронного документообігу (СЕД). Особлива увага приділяється розгляду таких механізмів захисту інформації, як криптографія, електронний цифровий підпис (ЕЦП), стеганографія та цифровий водяний знак (ЦВЗ). Виконано опис процесу вбудовування ЦВЗ в цифровий документ. Проведено аналіз використання головного реквізиту ЕД – ЕЦП. Розглянуто існуючі підходи до розробки системи захисту ЕД і способи їх прихованої передачі. Запропоновано класифікацію атак та загроз інформаційній безпеці (ІБ) ЕД. Досліджується можливість побудови захищеної СЕД на основі комплексного використання методів криптографії та стеганографії. Отримані результати стануть основою для подальшої розробки та вдосконалення засобів захисту ЕД.

Ключові слова: *електронний документ, достовірність, стеганографія, водяний цифровий знак, електронний цифровий підпис.*

Вступ. Останнім часом спостерігається перехід від традиційної форми представлення документів до електронної. Насамперед, це пов'язано з низкою переваг використання електронного документообігу. Перш за все, електронний документообіг дозволить суттєво спростити роботу з формування, збереження та відправки важливої інформації. Разом з тим, деякі питання, пов'язані з забезпеченням надійного обміну електронними документами (ЕД), протидією розголошення, отримання несанкціонованого доступу (НсД) до ЕД, нині все ще залишаються повністю не вирішеними. Отримані незаконним шляхом конфіденційні дані можуть стати причиною масштабних фінансових втрат організації чи, наприклад, завдати моральної шкоди особистості. У зв'язку із швидкими темпами інформатизації сучасного суспільства і переходу до систем електронного документообігу (СЕД) виникають нові потенційні загрози інформаційній безпеці (ІБ) [1].

Постановка проблеми. На сучасному етапі домінування інформаційних технологій (ІТ), тенденції розвитку обчислювальних машин питання забезпечення ІБ документів при їх створенні, обробці та передачі мережею є актуальними, як ніколи. Разом з прогресом у сфері ІТ спостерігається і розвиток законодавчо-правової бази електронного документообігу, але шлях переходу до ЕД має ряд питань, пов'язаних із забезпеченням їх захисту. Існуючі механізми захисту інформації не можуть повною мірою вирішити ряд завдань, характерних для ЕД. На відміну від паперових документів, шкоди яким можна завдати лише фізичним шляхом і які існують в одному примірнику, ЕД зберігаються на цифрових носіях, передаються мережею, можуть мати декілька копій, тому вони є вразливішими до всякого роду атак. Завдання надійного захисту конфіденційних ЕД від НсД, захисту інтелектуальної власності, авторських прав вирішується вже тривалий час. Проте, деякі питання розробки надійних методів забезпечення ІБ ще потребують вирішення. Проблема захисту ЕД не обмежується лише засобами контролю НсД. Таким чином, стає актуальною і сучасною завдання дослідження можливостей використання методів і моделей захисту ЕД із застосуванням перспективних засобів криптографії та стеганографії. При цьому, варто зауважити, що жоден із зазначених напрямів на цьому етапі свого розвитку не в змозі самостійно вирішити всі завдання, пов'язані з захистом ЕД. Крім того, вирішення більшості специфічних завдань можливе лише за умови комплексного їх використання.

Аналіз останніх досліджень та публікацій. Питаннями пошуку шляхів вирішення проблеми забезпечення інформаційного захисту ЕД впродовж багатьох років займалися:

Панасенко С. П., Балакин А. В., Астахова Т. С., Сагайдак Д. А., а також інші науковці, в тому числі й іноземні. Проте, як показує аналіз літературних джерел [4–10], в умовах широкого використання технологій електронного обміну даними використання СЕД дозволяє домогтися значного економічного ефекту при обробці ЕД, але не повністю вирішує ряд проблем, пов'язаних із забезпеченням ІБ документів.

Мета статті – підвищення ефективності захисту ЕД в СЕД. Досягнення поставленої мети передбачає: аналіз можливих атак на інформаційні ресурси СЕД, дослідження сучасних стеганографічних та криптографічних методів забезпечення ІБ, можливість побудови комплексної системи захисту ЕД.

Основний матеріал. Швидкі темпи розвитку СЕД, що спострегіються останнім часом, разом зі своїми перевагами спричинили цілий ряд інформаційних злочинів, пов'язаних з порушенням прав інтелектуальної власності. До таких порушень можна віднести: плагіат, викрадення, розголошення та підробку ЕД. Тому, використання СЕД є неможливим без системи захисту. Для створення і впровадження системи захисту ЕД необхідно реалізувати цілий комплекс стандартних заходів, серед яких можна виділити такі:

1) аналіз основних властивостей і функцій ЕД;

2) класифікація загроз ІБ;

3) дослідження вимог по забезпеченню ІБ;

4) визначення та розробка механізмів захисту інформації.

Цей перелік ще можна продовжити пакетом організаційно-технічних заходів.

Характерними властивостями ЕД є конфіденційність, цілісність та достовірність. Тому, захищена СЕД має передбачувати реалізацію, як мінімум, таких механізмів захисту: забезпечення цілісності документів, безпечного доступу, конфіденційності та достовірності документів. Питання гарантії достовірності ЕД нині піднімається все частіше. Насамперед, це викликано збільшенням обсягів документованої інформації між організаціями, а також розвитком технологій електронного обміну даними. В зв'язку з цим виникає багато методів захисту документів від фальсифікації. Одним і найсуттєвішим із способів порушення властивостей ЕД є отримання НсД. Проблему отримання НсД можна вирішити за допомогою моделі розмежування доступу, наприклад, Take-Grant. Ця модель підтверджує чи компрометує ступінь захисту СЕД і представляє її у вигляді направленого графа, в якому показані правила доступу суб'єктів до електронних документів. Формально описати модель Take-Grant можна таким чином: представимо сукупність об'єктів, тобто ЕД, у вигляді множини $E = (e_1, e_2, \ldots, e_n)$, множину суб'єктів – $S = (s_1, s_2, \ldots, s_n)$. Множину прав доступу представимо у вигляді послідовності $R = (r_1, r_2, ..., r_n) \bigcup (t, g)$. Згідно з класичною інтерпретацією моделі Take-Grant, *t(take)* – право брати «права доступу», *g(grant)* – право давати «права доступу» [6]. Стан системи описується графом. На рис. 1 показаний граф надання прав доступу до ЕД.

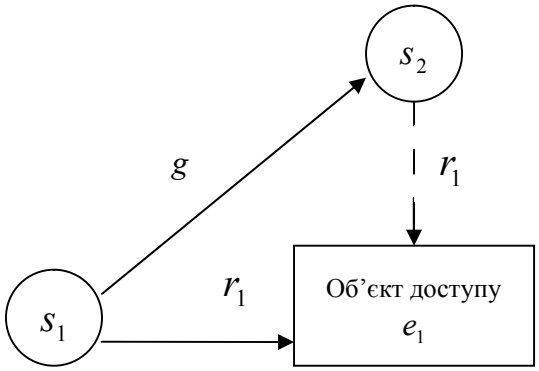

Рис. 1. Модель надання прав доступу Take-Grant

З рис. 1 видно, що об'єкт s_1 дає право доступу r_1 до об'єкта p_1 ЕД, іншому суб'єкту s_2. Аналогічним способом представляється і модель, згідно з якою суб'єкт може брати права доступу. Використовуючи цю модель, можна передбачити стани, в яких буде перебувати СЕД, залежно від розмежування прав доступу [7]. Тобто, модель дає можливість передбачити і проаналізувати можливі загрози інформаційній безпеці для системи.

Проте, за умов неможливості забезпечення абсолютного контролю доступу до інформаційної системи і недопущення отримання НсД, для захисту ЕД можуть бути використані засоби криптографії та стеганографії. Одним із напрямів захисту ЕД при збереженні, передачі комп'ютерною мережею є цифрова стеганографія [2]. Стеганографія – метод організації зв'язку, який приховує факт

його існування [3]. Для засобів стеганографії характерним є те, що приховане повідомлення вбудовується в деякий об'єкт, який потім відкрито пересилається мережею. На відміну від криптографії, де є очевидним для зловмисника факт зашифрування ЕД, методи стеганографії дозволяють вбудовувати повідомлення в ЕД таким чином, щоб неможливо було запідозрити про його наявність [4]. Стеганографія в інформаційних системах зв'язку – слабо розвинений напрям, а існуючі методи мало пристосовані до завдань захисту ЕД. Це пов'язано з властивими їй недоліками, такими як невисока надійність і стійкість. Проте, разом з цим, застосування стеганографічних систем у СЕД дозволить вирішити ряд важливих завдань, серед яких варто відзначити забезпечення прихованого збереження і передачі ЕД, перетворення комунікацій між відправником та отримувачем повідомлень на непомітні, виявлення каналів витоку ЕД, а також внесення прихованого ЕЦП [5].

Зазвичай у документованій інформації з метою захисту авторських прав використовують цифрові водяні знаки (ЦВЗ). ЦВЗ – цифрові мітки, які впроваджуються в ЕД за допомогою спеціальних стеганографічних перетворень [6]. Практичне застосування характеризується такими аспектами, як захист авторських прав, отримання цифрового відбитка, приховування факту обміну інформацією. На сьогоднішній день існує багато систем впровадження ЦВЗ у мультимедійну інформацію, поліграфічну продукцію. Стосовно ЕД, захист документів за допомогою вбудовування ЦВЗ наразі є недостатньо вивченим та опрацьованим. У джерелах [2–4] описані можливі способи впровадження ЦВЗ в ЕД та фізичні документи.

Стенографічні системи виконують завдання захисту авторських прав на ЕД за умов різного роду спроб порушення та атак. Системи ЦВЗ забезпечують ідентифікацію автора ЕД. Аналогічне завдання також може бути вирішене за допомогою ЕЦП. На відміну від стегосистеми ЦВЗ, ЕЦП не може забезпечити захист ЕД за умови неправомірної модифікації документа, тобто підробки. Стеганографічна система дозволяє вбудувати цифрові дані одного об'єкта в інший і вилучати приховану інформацію [7].

Для того щоб представити структуру стегосистеми, необхідно ввести такі позначення: нехай *C* – цифрове зображення, ЦВЗ, *I* – цифровий документ, в стенографії зображення, в яке вбудовується ЦВЗ, називають контейнером, *K* – заповнений контейнер. Процеси *E, T, D* – відповідно процес вбудовування ЦВЗ в документ, перетворення заповненого контейнера і вилучення ЦВЗ. Стандартну схему стеганографічної системи можна показати наступним чином (рис. 2).

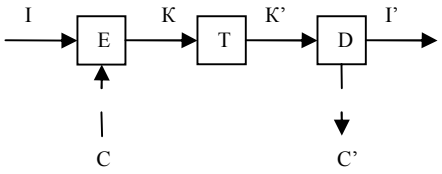

Рис. 2 Схема стеганографічної системи

Перетворення *T* заповненого контейнера *K*" можуть включати процеси: передача по мережі, різного роду атаки на ЕД, друк та інші [8]. Основною властивістю стеганосистеми є близькість значень порожнього і заповненого контейнера $I \approx K$. Насамперед, ця умова має виконуватися для того, щоб візуально був непомітним вбудований ЦВЗ в ЕД. Математичну модель стеганографічної системи можна представити у вигляді формул (1)–(3). Спочатку виконується генерація ЦВЗ:

$$Z = F(R, K, I) \ , \qquad (1)$$

де *Z* – множина можливих ЦВЗ, *R* – ключі, *K* – контейнери, *I* – приховані дані, ЕД.

Процес вбудовування ЦВЗ *Z(m,n)* у вихідний цифровий документ *I(m,n)*:

$$I'(m,n) = I(m,n) \oplus L(m,n)Z(m,n)p(m,n) \quad (2)$$

де *L(m,n)* – маска вбудовування ЦВЗ, що враховує властивості зору людини з метою зробити непомітним використання ЦВЗ, *p(m,n)* – проектувальна функція, яка залежить від ключа і відповідає за розподіл ЦВЗ по площині цифрового документа.

Операція детектування *D* – виявлення ЦВЗ в документі –представлена формулою:

$$D(I', Z) = (I', F(I, R)) = \begin{Bmatrix} 1, \textit{якщо } Z \in \\ 0, \textit{якщо } Z \textit{ немає} \end{Bmatrix}. \quad (3)$$

Можливості криптографії вже відомі, вона давно пройшла шлях свого становлення й існуючі методи можуть бути легко адаптовані до задач СЕД. Сучасна криптографія включає такі основні розділи: асиметричні системи, симетричні системи шифрування, системи ЕЦП та керування ключами [9]. Досить часто для захисту ЕД використовують

симетричні системи, до яких можна віднести підстановки, перестановки, гамування й блочні шифри. Основні напрями використання криптографічних методів: передача конфіденційної інформації в каналах зв'язку, встановлення дійсності переданих повідомлень, збереження інформації на носіях у зашифрованому вигляді. Криптографія дає можливість перетворити інформацію таким чином, що її прочитання можливе тільки при знанні ключа.

Головним реквізитом ЕД є ЕЦП – атрибут, який дозволяє на основі криптографічних методів встановити авторство і цілісність ЕД [10]. Використання ЕЦП дає можливість забезпечити:

1) контроль цілісності ЕД за умови будь-якого випадкового чи навмисного спотворення документа, оскільки підпис стане недійсним, тому що він створений на основі первинного стану документа і відповідає лише йому;

2) захист від редагування (фальсифікації) ЕД;

3) гарантування авторства і неможливість відмови від нього; створити конкретний електронний підпис можна, лише володіючи закритим ключем, який відомий тільки власникові [11].

Система ЕЦП включає процедуру формування і перевірки підпису. ЕЦП може створюватися за симетричною або за асиметричною схемами. Крім цього, існують також й інші різновиди цифрового підпису, які є модифікаціями двох основних схем. 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 у 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. Принциповим моментом у системі ЕЦП є неможливість підробки ЕЦП користувача без володіння секретним ключем підпису. Тому важливо тримати ключ в таємниці і забезпечити надійний захист від НсД [12].

Безпека інформації при її передачі відкритими каналами зв'язку може забезпечуватися методами як криптографії, так і стеганографії. Проте, враховуючи, що жоден із цих напрямів на даному етапі свого розвитку не може самостійно вирішити всі питання, пов'язані з захистом інформації в СЕД, забезпечення ІБ електронного документообігу можливе лише в умовах комплексного використання криптографічних і стеганографічних засобів захисту.

Висновки. У висновку можна зазначити, що проблема ІБ в СЕД постійно зростала, стимулюючи при цьому пошук нових методів захисту ЕД. Забезпечення достовірності і гарантії авторства ЕД є необхідною умовою якісного функціонування соціальних структур. Основною причиною порушення ІБ у системах вже довгий час залишається отримання НсД до інформаційних ресурсів. Як один із варіантів контролю прав доступу до СЕД запропонована модель розмежування доступу Take-Grant. Оскільки абсолютний контроль доступу в більшості випадків є неможливим, то вирішення проблеми безпеки ЕД має додатково забезпечуватися засобами захисту інформації.

Особлива увага зосереджена на таких напрямах захисту, як стеганографія та криптографія. Для захисту авторських прав, забезпечення цілісності та достовірності ЕД використовуються ЦВЗ та ЕЦП. Проте, дослідження доводить, що на сучасному етапі свого розвитку ефективного захисту ЕД можна домогтися лише за умови комплексного використання засобів криптографії та стеганографії. Поступово вже виникають нові, гібридні системи захисту інформації.

Список літератури

1. Розломій І. О. Організація і оцінка ефективності системи захищеного документообігу / І. О. Розломій // Вісник Кременчуцького національного університету ім. Михайла Остроградського. – 2015. – № 6 (95). – С. 119–124.
2. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-пресс. Изд. : Пандора-1, 2002. – 261 с.
3. Коханович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Кохано-

вич, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
4. Стеганография, цифровые водяные знаки и стегоанализ / Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. – М. : Вузовская книга, 2009. – 220 с.
5. Digital watermarking and steganography / I. J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco : Morgan Kaufmann Publishing, 2008. – 624 p.
6. Балакин А. В. Использование стеганографических методов для защиты текстовой информации / А. В. Балакин, А. С. Елисеев // Технологии информационного общества ФГНУ НИИ «Спецвузавтоматика». – 2009. – С. 183–184. – (Спецвыпуск).
7. Сагайдак Д. А. Способ формирования цифрового водяного знака для физических и электронных документов / Д. А. Сагайдак, Р. Т. Файзуллин // Компьютерная оптика. – 2014. – № 1 (38). – С. 94–104.
8. Очнев Д. В. Цифровые водяные знаки как метод защиты текстовых печатных документов / Д. В. Очнев, Е. С. Чиркин // Гаудеамус : психолого-педагог. журн. – 2012. – № 2 (20). – С. 148–149.
9. Основы криптографии / Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. – Гелиос АРВ, 2002. – 480 с.
10. Астахова Т. С. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа / Т. С. Астахова, Е. П. Чадаева // Известия Томского политехнического университета. – 2012. – № 6. – С. 55–61.
11. Розломій І. О. Електронний цифровий підпис як засіб забезпечення цілісності та достовірності електронного документа / І. О. Розломій // Сучасна наука: теорія і практика. – Запоріжжя : ІОПМ, 2015.
12. Рябко Б. Я. Основы современной криптографии / Б. Я. Рябко, А. Н. Фионов. – Научный Мир, 2004. – 173 с.

References

1. Rozlomii, I. O. (2015) Organization and evaluation of the effectiveness of secure document management system. *Visnyk Kremenchutskoho natsionalnoho universytety im. Mykhaila Ostrohradskoho*, 6 (95), pp. 119–124 [in Ukrainian].
2. Gribunin, V. G., Okov, I. N. and Turintsev, I. V. (2002) Digital steganography. Moscow: Solon-press. Publisher: Pandora-1, 261 p. [in Russian].
3. Kokhanovich, G. F. and Puzyrenko, A. Yu. (2006) Computer steganography. Theory and practice. Kiev : MK-Press, 288 p. [in Russian].
4. Agranovskiy, A. V., Balakin, A. V., Gribunin, V. G. and Sapozhnikov, S. A. (2009) Steganography, digital watermarking and steganalyst. Moscow: Vuzovskaya kniga, 220 p. [in Russian].
5. Cox, I. J., Miller, M., Bloom, J. and Fridrich, J. (2008) Digital watermarking and steganography. San Francisco: Morgan Kaufmann Publishing, 624 p.
6. Balakin, A. V. and Eliseev, A. S (2009) The use of steganographic techniques to protect textual information. *Technologiyi informatsionnogo obschestva FGNU NII "Spetsvuzavtomatika"*. Special edition, pp. 183–184 [in Russian].
7. Sagaidak, D. A. and Faizullin, R. T. (2014) A method of forming a digital watermark for physical and electronic documents. *Compjuternaya optika*, 1 (38), pp. 94–104 [in Russian].
8. Ochnev, D. V. and Chirkin, E. S. (2012). Digital watermarks as a method of protection of text printed documents. *Gaudeamus: psychopedagogical journal*, 2 (20), pp. 148–149 [in Russian].
9. Alferov, A. P., Zubov, A. U., Kuzmin, A. S. and Cheremushkin, A. V. (2002). Basics of cryptography. Helios ARV, 480 p. [in Russian].
10. Astakhova,T. S. and Chadaeva, E. P. (2012). Electronic digital signature as a factor in preserving the integrity and authenticity of the document. *Izvestiya Tomskogo politehnicheskogo universiteta*, (6), pp. 55–61 [in Russian].
11. Rozlomii, I. O. (2015) Electronic digital signature as a means of electronic document's integrity and authenticity. *Suchasna nauka: teoriya i praktyka.* Zaporizhzhya, pp. 150–153 [in Ukrainian].
12. Ryabko, B. Ja. and Fionov, A. N. (2004) The foundations of modern cryptography. Nauchnyy Mir, 173 p. [in Russian].

I. O. Rozlomii, *postgraduate student,*
G. V. Kosenuk, *Ph.D.*
Cherkasy Bogdan Khmelnytskyi national university
Schevchenko blvd, 81, Cherkasy, 18000, Ukraine

THE MAIN PROPERTIES OF ELECTRONIC DOCUMENT PROTECTION FROM FALSIFICATIONS

In connection with the development of information technologies and computer data networks the systems of electronic document management become widely implemented. However, an important obstacle to the introduction of electronic documents has a number of issues related to the security of information systems of electronic documents.

The tools of information protection in order to enhance the protection of electronic documents have been researched. Achieving of this goal involves: the analysis of possible attacks on information resources of electronic documents, the study of modern steganographic and cryptographic methods of information security, the possibility of building of a comprehensive system of electronic documents protection.

The existing mechanisms of information security can not fully solve a number of problems specific to electronic documents. Thus, it becomes relevant and contemporary task of research opportunities by means of methods and models for electronic documents protection, using advanced cryptography and steganography tools.

The development of the system of electronic documents protection provides the following basic steps:

1) the analysis of the basic properties and functions of electronic documents;
2) the classification of threats to information security;
3) the research of requirements for information security;
4) the identification and development of mechanisms to protect information.

Most attacks on information are carried out by means of unauthorized access to information resources. In the article the model of access Take-Grant, whose rules allow to control the access to electronic documents, is considered. Since absolute control of the access to system resources is not possible, the protection of electronic documents can be used by means of cryptography and steganography. Digital watermarks are used in documented information in order to copyright protection. By means of cryptography one can protect the information through encryption or electronic digital signature. Electronic digital signature ensures the integrity of the document, the protection against forgery and guarantees authorship.

The safety of information during its transfer by open channels of communication can be provided by the methods of cryptography and steganography. However, given that none of these areas at this stage of the development can not solve all issues related to the protection of information in the systems of electronic document management, the providing of information security of electronic documents is possible only in the conditions of complex use of cryptography and steganography remedies. The practical value of the study is the ability to use the results for further development of new and improvement of existing systems of electronic documents protection.

Keywords: *electronic document, authenticity, steganography, digital watermark, electronic digital signature.*

Рецензенти: В.М. Рудницький, д.т.н., професор,
С. В. Голуб, д.т.н., професор