УДК 004.056.5

Роман Михайлович Штонда
Юрій Олександрович Процюк
В'ячеслав Володимирович Овсянніков *(канд. техн. наук)*
Олег Миколайович Маковецький
Ірина Робертівна Мальцева

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

ПІДХОДИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

На фоні подій, що на сьогоднішній день відбуваються в Україні та світі, а також в умовах масового поширення засобів електронно-обчислювальної техніки та можливостей несанкціонованих дій над інформацією виникає необхідність більш ретельного захисту державної, промислової, комерційної та фінансової таємниці. Захист інформації в цілому та захист інформації в автоматизованих системах зокрема, стає усе актуальнішою й складнішою задачею, для вирішення якої необхідно залучати все більше кваліфікованого персоналу та організацій, що спеціалізуються на захисті інформації.

Для швидкого та якісного управління в установах різного рівня все більше впроваджуються системи електронного документообігу, які не в повній мірі захищені від атак зловмисників, що переслідують корисні цілі в заподіяні шкоди тій чи іншій організації. З метою збереження конфіденційності, цілісності та доступності інформації, що циркулює в системах електронного документообігу використовується на даний час ряд методів (засобів) захисту інформації.

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

Вступ

В останні роки в Україні відбувається перехід від традиційних форм відпрацювання документів до їх електронного вигляду. Перехід до електронного документообігу несе цілий ряд переваг, серед яких: суттєве скорочення термінів відпрацювання та проходження документів в установах, спрощення пересилання документів між установами, що в свою чергу, зумовлює відчутну економічну вигоду. На сьогодні в нашій державі вже існує доволі велика кількість нормативно-правових актів, що регулюють відносини у сфері застосування інформаційних систем та захисту інформації в них. Основними нормативно-правовими документами з питань формування потужної бази щодо запровадження електронного документообігу є:

1. Закон України "Про електронні документи та електронний документообіг" [1];

2. Закон України "Про електронний цифровий підпис" [2];

3. Порядок засвідчення наявності електронного документу (електронних даних) на певний момент часу (Постанова Кабінету Міністрів України від 26 травня 2004 р. № 680 "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу") [3];

4. Положення про центральний засвідчувальний орган (Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451 "Про затвердження Положення про центральний засвідчувальний орган") [4];

5. Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1452 "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності") [5].

6. Типовий порядок здійснення електронного документообігу в органах влади (затверджений Постановою Кабінету Міністрів України від 28 жовтня 2004 р. № 1453 "Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади") [6];

7. Порядок обов'язкової передачі документованої інформації (затверджений Постановою Кабінету Міністрів України від 28 жовтня 2004 р. № 1454 "Про затвердження порядку обов'язкової передачі документованої інформації") [7].

З прийняттям вище зазначених нормативно-правових документів електроні документи набули юридичної сили та в повній мірі спроможні замінити традиційні документи.

Постановка проблеми. На сьогоднішній день одним із важливих питань на шляху переходу до електронного документообігу (ЕД) є необхідність захисту інформації в системах електронного документообігу (СЕДО). Загалом, перехід до ЕД

передбачає їх передачу в електронному вигляді по різноманітним каналам зв'язку. Враховуючи сучасний стан, а також перспективи розвитку системи зв'язку та телекомунікації, явним являється широке застосування, для передачі електронних документів, відкритих каналів зв'язку та мережі Інтернет в яких найважливішим питанням є забезпечення захисту інформації, що передається.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень та публікацій з питань розвитку СЕДО та захисту інформації відмічені Г. Асєєв, О. Ганжела, С. Дубова, І. Жукова, О. Калачиков, С. Лимар, О. Матвієнко, І. Ольшанський, О. Орлов, В. Писаренко, А. Порятуй, Д. Птіцин, Д. Сахарук, М. Слободнянюк, О. Целуйко, М. Цивін, О. Шпирка та ін.

Метою статті є аналіз підходів щодо захисту інформації в СЕДО.

Виклад основного матеріалу дослідження

СЕДО є невід'ємною складовою частиною будь-якої установи різного рівня управління (в тому числі і Збройних Сил України). Від успішності функціонування цієї системи, залежить успіх виконання завдання.

В тих умовах, в яких на сьогоднішній день перебувають Збройні Сили України, успіх виконання поставленого завдання залежить від швидкості передачі тієї чи іншої інформації. Серед інформації, яка циркулюватиме в СЕДО може бути інформація з обмеженим доступом. Тому, щоб запобігти несанкціонованому доступу до цієї інформації, необхідно запровадити надійну систему захисту ЕД. Але слід брати до уваги той факт, що впровадження захисту призводить до ускладнення в роботі системи, зниження її ефективності, тому впровадження системи захисту повинно бути обґрунтованим і доцільним.

Основні загрози інформації, що циркулює в СЕДО можуть бути класифіковані наступним чином [8]:

1. Загроза цілісності – це пошкодження, знищення, або спотворення інформації, що може бути як ненавмисним у випадках помилок і збоїв, так і навмисним.

2. Загроза конфіденційності – це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміна маршрутів слідування і т.д.

3. Загроза працездатності системи – це загроза, реалізація якої призводить до порушення або припинення роботи системи, включаючи навмисні атаки, помилки користувачів, а також збої в обладнані і програмному забезпеченні.

4. Неможливість підтвердження авторства – це загроза, що виражається у тому, що якщо в документообігу не використовується електронний цифровий підпис, то неможливо довести, що саме даний користувач створив даний документ (при цьому неможливо зробити документообіг юридично значимим).

5. Загроза доступності – це загроза, що порушує можливість за допустимий час отримати потрібну інформацію користувачам, що мають право доступу до неї.

Підходами щодо захисту інформації під час передачі по відкритим каналам зв'язку для запобігання вище переліченим загрозам є комбінування методів (засобів) криптографічного та стеганографічного захисту інформації.

Найбільш поширеними і в більшості випадків ефективними є криптографічні методи та засоби захисту інформації – методи шифрування, кодування або іншого перетворення інформації, в результаті якого її вміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. При застосуванні криптографічних методів захисту інформації охороняється безпосередньо сама інформація, а не доступ до неї (наприклад зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Дані методи захисту інформації реалізується у вигляді програмних або апаратно-програмних засобів.

Сучасна криптографія включає чотири розділи:

1. Симетричні криптосистеми. У цих системах використовується для шифрування, і для дешифрування один і той же ключ.

2. Криптосистеми з відкритим ключем. У даних системах використовується два ключі відкритий і закритий, які математично зв'язані один з одним. Інформація шифрується за допомого відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого лише одержувачеві повідомлення.

3. Цифровий електронний підпис. Дана система дозволяє перевірити достовірність повідомлення при одержані його користувачем.

4. Управління ключами. Це процес системи обробки інформації, вмістом яких є складання і розподіл ключів між користувачами.

На ряду з криптографічними методами (засобами) захисту інформації застосовуються методи стеганографічного захисту інформації. На сьогоднішній день існує значна кількість методів, що пов'язані з використанням комп'ютерних форматів в якості контейнера для приховування. Це формати зображення, аудіо та відео. Використання будь-яких з них має свої переваги та недоліки, найширше застосовуються методи що в якості контейнера використовують зображення [9].

1. Методи цифрової стеганографії зображень. Дані методи здатні забезпечити високу робастність та таємність вбудовування, тому ці характеристики необхідно враховувати при забезпеченні стійкості до активних атак в СЕДО.

1.1 Методи приховування даних в частотній області зображення.

1.2 Методи шаблонного вбудовування даних на основі матричного представлення кодів Хеммінга.

2. Методи стеганографічного аналізу частотної області зображень. Найбільш об'єктивні оцінки таємності вбудування даних дозволяють отримати

сучасні методи стеганоаналізу, тому з метою отримання цих оцінок потрібно проаналізувати існуючі методи стеганоаналізу частотної області зображень.

Методи стеганографічного аналізу умовно поділяються на цільові та сліпі. Методи цільового стеганографічного аналізу розробляються з урахуванням особливостей вбудовування. На противагу їм, методи сліпого стеганографічного аналізу не враховують механізм вбудовування. Однак методи сліпого стеганографічного аналізу застосовують широкий набір характеристик натуральних зображень.

Також широко застосовуються методи вбудовування даних у вейвлет-коефіцієнти зображень [9].

Висновки й перспективи подальших досліджень

В сучасному світі комп'ютерних технологій прослідковується тенденція зростання впровадження в процеси управління установами - СЕДО. Але жодна СЕДО не може існувати без надійних засобів захисту інформації, які ґрунтуються на сучасних методах (засобах) захисту інформації. Виходячи з цього захист інформації – нагальна потреба сучасного функціонування будь-якої СЕДО. Вибір конкретних методів (засобів) захисту інформації буде залежати від цінності інформації, яка обробляється. Чим складніші методи (засоби) захисту інформації в СЕДО (комбінація методів та засобів криптографічного та стеганографічного захисту інформації), тим вони будуть дорожчі. Але в будь-якому випадку для забезпечення захисту інформації, що циркулює в СЕДО повинні бути спочатку впроваджені хоч б елементарні, найдешевші засоби.

Література

1. Закон України Про електронні документи та електронний документообіг : Закон від 22.05.2003 № 851-IV / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon4.rada.gov.ua/laws/show/851-15. – Назва з екрану. **2. Закон України** Про електронний цифровий підпис : Закон від 22.05.2003 № 852-IV. / [Електронний ресурс] // Верховна Рада України – Режим доступу: http://zakon4.rada.gov.ua/laws/show/852-15. – Назва з екрану. **3. Постанова Кабінету Міністрів України** Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу : Постанова від 26.05.2004 № 680. / [Електронний ресурс] // Кабінет Міністрів України – Режим доступу: http:// zakon1.rada.gov.ua/laws/show/680-2004-%D0%BF. – Назва з екрану. **4. Постанова Кабінету Міністрів України** Про затвердження Положення про центральний засвідчувальний орган : Постанова від 28.10.2004 № 1451. / [Електронний ресурс] // Кабінет Міністрів України – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1451-2004-%D0%BF. – Назва з екрану. **5. Постанова Кабінету Міністрів України** Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : Постанова від 28.10.2004 № 1452. / [Електронний ресурс] // Кабінет Міністрів України – Режим доступу:http://zakon4.rada.gov.ua/laws/show/1452-2004-%D0%BF. – Назва з екрану. **6. Постанова Кабінету Міністрів України** Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади: Постанова від 28.10.2004 № 1453. / [Електронний ресурс] // Кабінет Міністрів України – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1453-2004-%D0%BF. – Назва з екрану. **7. Постанова Кабінету Міністрів України** Про затвердження порядку обов'язкової передачі документованої інформації : Постанова від 28.10.2004 № 1454. / [Електронний ресурс] // Кабінет Міністрів України – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1454-2004-%D0%BF. – Назва з екрану. **8. Досмухамедов Б.Р.** Анализ угроз информации систем электронного документооборота / Б.Р. Досмухамедов // Компьютерное обеспечение и вычислительная техника. – 2009. - № 6. – с.140-143. **9. Лукічов В.В.** Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень / Лукічов В.В., Лужецький В.А., Васюра А.С. – В.: ВНТУ, 2014. с. 19-105.

ПОДХОДЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Роман Михайлович Штонда
Юрий Александрович Процюк
Вячеслав Владимирович Овсянников *(канд. техн. наук)*
Олег Николаевич Маковецкий
Ирина Робертовна Мальцева

Военный институт телекоммуникаций и информатизации, Киев, Украина

На фоне событий, на сегодняшний день происходят в Украине и мире, а также в условиях массового распространения средств электронно-вычислительной техники и возможностей несанкционированных действий над информацией возникает необходимость более тщательной защиты государственной, промышленной, коммерческой и финансовой тайны. Защита информации в целом и защите информации в автоматизированных системах в частности, становится все более актуальной и сложной задачей, для решения которой необходимо привлекать все больше квалифицированного персонала и организаций, специализирующихся на защите информации.

Для быстрого и качественного управления в учреждениях различного уровня все больше внедряются системы электронного документооборота, которые не в полной мере защищены от атак злоумышленников, преследуют полезные цели в причиненные ущерб той или иной организации. С целью сохранения конфиденциальности, целостности и доступности информации, циркулирующей в системах электронного документооборота используется в настоящее время ряд методов (средств) защиты информации.

Ключевые слова: *электронный документ; электронный документооборот; система электронного документооборота; защита информации; шифрования.*

THE APPROACHES TO THE INFORMATION PROTECTION IN ELECTRONIC DOCUMENT FLOW SYSTEMS

Roman M. Shtonda
Yurii O. Protsiuk
Viacheslav V. Ovsiannikov *(Candidate of Technical Sciences)*
Oleh M. Makovetskyi
Iryna R. Maltseva

Military Institute of Telecommunications and Information, Kyiv, Ukraine

Against the background of events that today in Ukraine and the world, as well as in mass distribution of electronic computer engineering and unauthorized actions on information it is necessary to more thoroughly protect the public, industrial, commercial and financial secrecy. Information security in general and protection of information in automated systems in particular, becomes more urgent and complex problem, whose solution must involve more skilled personnel and organizations specializing in the protection of information.

For a quick and good governance in the institutions of different levels are increasingly introducing electronic document management systems that are not fully protected from malicious attacks plaguing useful purpose in the damage caused by a particular organization. In order to preserve the confidentiality, integrity and availability of information circulating in electronic document systems currently used by a number of methods and means of information protection.

Keywords: *electronic document; electronic document; electronic document management system; Data Protection; encryption.*

References

1. The Law of Ukraine (2003), On electronic documents and electronic document. [*Pro elektronni dokumenty ta elektronnyy dokumentoobih*], The Verkhovna Rada of Ukraine, http://zakon4.rada.gov.ua/laws/show/851-15. **2. Law of Ukraine** (2003), On electronic digital signature. [*Pro elektronnyy tsyfrovyy pidpys*], The Verkhovna Rada of Ukraine, http://zakon4.rada.gov.ua/laws/show/852-15. **3. The Cabinet** of Ministers of Ukraine № 680 (2004), On approval of the testimony of the presence of an electronic document (electronic data) for a certain time. [*Pro zatverdzhennya Poryadku zasvidchennya nayavnosti elektronnoho dokumenta (elektronnykh danykh) na pevnyy moment chasu*], The Cabinet of Ministers of Ukraine, http: // zakon1. rada. gov.ua/laws/show/680-2004-%D0%BF. **4. The Cabinet** of Ministers of Ukraine № 1451 (2004), On approval of the central certification body. [*Pro zatverdzhennya Polozhennya pro tsentral'nyy zasvidchuval'nyy orhan*], The Cabinet of Ministers of Ukraine http://zakon4.rada.gov.ua/laws/show/1451-2004-%D0%BF. **5. The Cabinet of** Ministers of Ukraine № 1452 (2004), On approval of the use of digital signature public authorities, local governments, enterprises, institutions and organizations of state ownership. [*Pro zatverdzhennya Poryadku zastosuvannya elektronnoho tsyfrovoho pidpysu orhanamy derzhavnoyi vlady, orhanamy mistsevoho samovryaduvannya, pidpryyemstvamy, ustanovamy ta orhanizatsiyamy derzhavnoyi formy vlasnosti*], http://zakon4.rada.gov.ua/laws/show/1452-2004-%D0%BF. **6. The Cabinet** of Ministers of Ukraine № 1453 (2004), On Approval of Standard Order of electronic document circulation in executive authorities. [*Pro zatverdzhennya Typovoho poryadku zdiysnennya elektronnoho dokumentoobihu v orhanakh vykonavchoyi vlady*], The Cabinet of Ministers of Ukraine, http://zakon0.rada.gov.ua/laws/show/1453-2004-%D0%BF. **7. The Cabinet** of Ministers of Ukraine № 1454 (2004) On adoption of obligatory transfer of documented information. [*Pro zatverdzhennya poryadku obov"yazkovoyi peredachi dokumentovanoyi informatsiyi*], The Cabinet of Ministers of Ukraine, http://zakon3.rada. gov.ua/laws/show/ 1454-2004-%D0%BF. **8. Dosmuhamedov B.R.** (2009), Analysis of information systems threats Electronic document circulation. [*Analyz uhroz ynformatsyy system elektronnoho dokumentooborota*], Provision of computer and vыchyslytelnaya technology, № 6, pp.140-143. **9. Lukichov V.V.** (2014), Steganographic methods and means of information protection based on wavelet transformation. [*Metody ta zasoby stehanohrafichnoho zakhystu informatsiyi na osnovi veyvlet-peretvoren*], NTB, pp. 19-105.

Отримано: 18.10.2015 р.