УДК 003.26:004.056.55

ОРГАНІЗАЦІЯ І ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИЩЕНОГО ДОКУМЕНТООБІГУ

І. О. Розломій
Черкаський національний університет імені Богдана Хмельницького
б-р Шевченка, 81, м. Черкаси, 18031, Україна. E-mail: innulichka-best@inbox.ru

Стаття присвячена розгляду проблем впровадження та функціонування систем електронного документообігу. В статті проаналізовано основні властивості електронних документів. Розглянуто стандартний набір загроз та факторів негативного впливу на електронний документообіг. Показано детальну класифікацію загроз безпеки електронного документообігу за певними ознаками, що дає змогу формалізувати завдання опису повної множини загроз. Показано основні форми витоку інформації. Проведено аналіз можливих методів забезпечення інформаційної безпеки. Побудовано модель захищеної системи електронного документообігу, яка демонструє механізм доступу до електронних документів. Досліджено базові механізми захисту електронного документообігу. Показано перелік можливих критеріїв оцінки ефективності засобів захисту. Запропоновано підхід до вибору системи захисту електронного документообігу на основі визначення і розрахунку показника її ефективності. Відповідно до отриманих результатів запропоновані способи та рекомендації щодо розробки системи захисту електронного документообігу.

Ключові слова*:* конфіденційність, цілісність, доступність, ідентифікація, аутентифікація.

ОРГАНИЗАЦИЯ И ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА

И. А. Розломий
Черкасский национальный университет имени Богдана Хмельницкого
б-р Шевченка, 81, г. Черкассы, 18031, Украина. E-mail: innulichka-best@inbox.ru

Статья посвящена рассмотрению проблем внедрения и функционирования систем электронного документооборота. В статье проанализированы основные свойства электронных документов. Рассмотрен стандартный набор угроз и факторов негативного воздействия на электронные документы. Показана подробная классификация угроз безопасности электронных документов по определенным признакам, которая позволяет формализовать задачу описания полного множества угроз. Показаны основные формы утечки информации. Проведен анализ возможных методов обеспечения информационной безопасности. Построена модель защищенной системы электронного документооборота, которая демонстрирует механизм доступа к электронным документам. Исследованы базовые механизмы защиты электронного документооборота. Показан перечень возможных критериев оценки эффективности средств защиты. Предложен подход к выбору системы защиты электронного документооборота, который основан на определении и расчете показателя ее эффективности. Согласно полученным результатам предложены способы и рекомендации по разработке системы защиты электронного документооборота.

Ключевые слова: конфиденциальность, целостность, доступность, идентификация, аутентификация.

АКТУАЛЬНІСТЬ РОБОТИ. Сучасний етап розвитку інформаційних технологій характеризується тенденцією домінування електронних документів (ЕД) над традиційними паперовими. У зв'язку з цим, важливим є забезпечення захисту ЕД. Сьогодні велика кількість організацій прагнуть до електронного обміну даними, а це можливо лише з використанням надійних систем захисту. Проблема гарантування достовірності ЕД є першочерговим завданням в процесі електронного документообігу.

ЕД вразливі до ряду негативних чинників та неправомірних дій різного характеру впливу та походження. Поряд з розгортанням переліку загроз ЕД, розвивається і ринок можливих засобів їх нейтралізації. Проте швидкість здійснення кібератак вражаюча, а розробка надійних засобів захисту інформації вимагає розумових, часових і матеріальних ресурсів. Вибір методів захисту, які б забезпечували безпеку від множини загроз і при цьому мали б мінімальну собівартість є складною проблемою.

Останнім часом спостерігається неабиякий інтерес до електронних документів, особливостей її використання і захисту від фальсифікацій. Вченими С.П. Панасенком, К.Ю. Воронiним, Б.В. Глазуновим запропоновані методики надійного захисту, проте, в зв'язку з підвищенням рівня вимог до захищеності електронних документів, зростанням злочинів в інформаційній сфері, є питання, що потребують вирішення.

Існує велика кількість підходів до забезпечення безпеки систем електронного документообігу (СЕД) і електронних документів зокрема. Вибір того чи іншого засобу захисту інформації визначається багатьма факторами, такими як сумісність з системою, надійність, функціональність. Виникає необхідність вибору методів захисту, які б дозволили отримати найраціональнішу структуру системи захисту електронного документообігу (СЗЕД) і сформувати оптимальний набір засобів, що забезпечуватимуть нейтралізацію виявлених загроз з високою ефективністю.

Мета роботи – дослідження особливостей функціонування СЕД, вплив негативних чинників на СЕД, визначення та характеристика множини можливих загроз. Аналіз засобів нейтралізації негативного впливу на СЕД, визначення, на основі розрахунку показника ефективності, оптимальних засобів захисту електронних документів.

МАТЕРІАЛ І РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ. Інформаційна безпека – один з найголовніших напрямків СЕД, що розвивається у відповідності з за-

конодавчо установленими стандартами. Безпека і захист електронних документів є невід'ємною частиною функціонування СЕД.

Від якісного формування ЕД повністю залежить ефективність управління всією організаційною структурою, для якої вони призначені. Контроль якісного формування, виконання, пошуку, використання, а також надійного зберігання та захисту є складовими продуманого документообігу. Потреба в ефективному управлінні ЕД стала причиною створення СЕД. СЕД – організаційно-технічні системи, що забезпечують процес створення, керування доступом та розповсюдження електронних документів по комп'ютерною мережею.

В електронному середовищі обробка документованої інформації представляє собою складний організаційно-технічний процес, що супроводжується низкою загроз безпеці інформації, реалізація яких може привести до втрати документом своєї юридичної значимості і як наслідок до збитку [1].

Під безпекою електронного документообігу розуміють захищеність інформації від перетворення і знищення, неможливість отримання суб'єктами непередбачених прав доступу [2]. Захищеність інформаційних ресурсів від впливу, направленого на порушення їх конфіденційності, цілісності та достовірності.

Розробка системи захисту потребує аналізу можливих загроз безпеці інформаційних ресурсів в СЕД. Основною функцією сучасних систем захищеного документообігу (СЗДО) є забезпечення захищеного обміну юридично значимими електронними документами. Даний процес забезпечується сукупністю програмних і технічних засобів захисту інформації і процесів її обробки від доступу нелегітимних користувачів чи процесів.

Сучасні методи обробки, передачі і збереження інформації спричинили виникненню загроз, пов'язаних з можливістю втрати, спотворення та несанкціонованого отримання даних.

Загроза безпеці інформації – сукупність умов і факторів (явищ, дій, процесів), що спричинюють потенційну небезпеку, що призводить до непередбачуваних фактів таких, як витік інформації, модифікація та знищення інформації. Всі можливі дії, які можуть завдати шкоди системі є загрозами безпеки СЕД.

В наш час відомий великий перелік загроз інформаційній безпеці (ІБ), який налічує сотні позицій. Розгляд можливих загроз ІБ проводиться з метою визначення повного набору вимог до системи захисту.

Перелік загроз, оцінки ймовірності їх реалізації, а також модель порушника служать основою для аналізу ризиків здійснення загроз і формулювання вимог до системи захисту СЕД.

Крім виявлення множини можливих загроз доречно проводити аналіз, на основі їх класифікації у відповідності з ознаками. Кожна ознака класифікації відповідає одній узагальненій вимозі до системи захисту і дозволяє деталізувати вимоги щодо захисту.

Необхідність класифікації загроз безпеки ЕД обумовлена тим, що на інформацію чинить негативний вплив велика кількість факторів, тому стає неможливим формалізувати завдання опису повної множини загроз. Класифікація потенційних загроз ЕД (рис. 1).

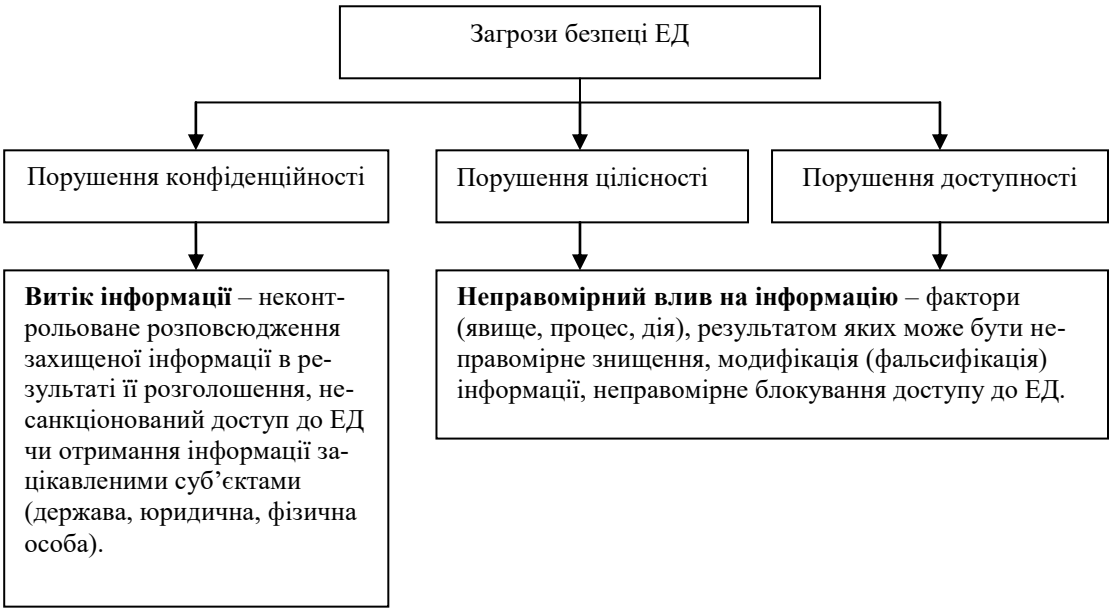

Рисунок 1– Класифікація загроз ЕД

Загроза конфіденційності може виникнути, як наслідок крадіжки, перехоплення інформації, зміни маршрутів руху ЕД. 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. Порушення конфіденційності є причиною отримання суб'єктами несанкціонованого доступу (НСД) до ЕД [3].

Загроза 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 [4].

Доступність характеризує можливість несанкціонованого доступу до документів, що зберігаються в СЕД в будь-який момент часу.

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

Захист інформації від НСД – заходи, що запобігають отримання інформації зацікавленими суб'єктами з порушенням встановлених правових норм [5].

Захист інформації від витоку – діяльність спрямована запобігання на неконтрольованого розповсюдження інформації від її розголошення, НСД до інформації і отримання її зловмисниками. Форми витоку інформації (рис. 2).

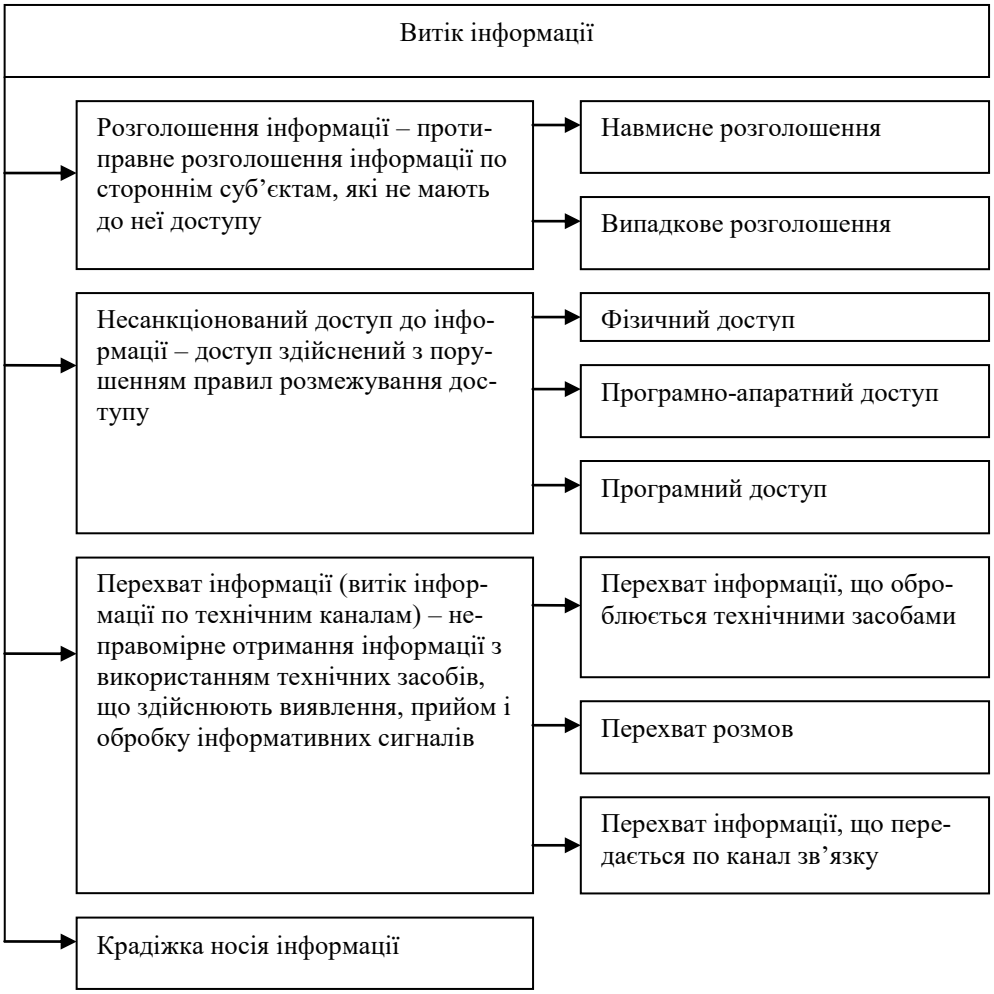

Рисунок 2 – Форми витоку інформації

Для протидії загрозам безпеки СЕД використовують спеціальні механізми захисту. Захист ЕД – сукупність засобів, які дозволяють запобігти витоку інформації, несанкціонованих і неправомірних дій. Об'єктом захисту є інформація, яку містять електронні документи, по відношенню до якої необхідно здійснювати захист від різного роду загроз і порушень.

Система захисту інформації – сукупність програмних, технічних та організаційних засобів захисту, які організовані і функціонують згідно правил нормативно-правових документів [6].

Основним для електронного документообігу є забезпечення гарантії авторства документа і цілісності при передачі, а також виключення несанкціонованого доступу. Перше завдання вирішується шляхом використання цифрового підпису, друге – шляхом застосування криптографічних методів захисту [7]. Розв'язати задачу несанкціонованого доступу покликані такі механізми захисту, як ідентифікація та аутентифікація користувачів.

Електронний цифровий підпис (ЕЦП) – засіб, що дозволяє на основі криптографічних методів встановити авторство і цілісність ЕД [8]. Цифровий підпис забезпечує такі процеси:

1) контроль цілісності ЕД за будь-якому випадковому чи навмисному спотворенню документа, оскільки підпис стане не дійсним, тому що він ство-

рений 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 можливо лише володіючи закритим ключем, який відомий тільки власникові.

Найнадійнішим засобом забезпечення конфіденційності інформації є шифрування. Під шифруванням розуміють процес перетворення відкритих даних в закриті, за визначеним криптографічним алгоритмом з використанням секретного ключового елементу – ключа шифрування.

Шифрування інформації вважається надійним засобом захисту від несанкціонованого перегляду, читання [9]. Вихідний текст ЕД – зашифрований, тобто недоступний для читання і його неможливо або дуже важко розшифрувати. Системно-парольні методи захисту від несанкціонованого доступу вразливіші до нейтралізації. Досвідчений зловмисник за короткий термін здатний нейтралізувати захист від несанкціонованого доступу, а розсекретити алгоритм і ключ шифрування під силу тільки технічно-оснащеному крипто аналітику з великими часовими затратами.

Робота користувача з ЕД можлива лише в тому випадку, якщо він має до них доступ. Доступ до ЕД – отримання суб'єктом можливості ознайомлення з інформацією. Розрізняють санкціонований і несанкціонований доступ (НСД) до інформації. Санкціонований доступ не порушує встановлені правила розмежування доступу. НСД до ЕД – порушення встановлених правил розмежування доступу. НСД є найбільш розповсюдженим видом порушень безпеки в СЕД. Несанкціонований доступ до СЕД характеризується порушенням правил розмежування доступу. Суб'єкт (процес, фізична особа), котрий здійснює несанкціонований доступ вважається порушником безпеки системи [10].

Доступ до ЕД пов'язаний з поняттями аутентифікація, ідентифікація та авторизація.

Ідентифікація суб'єкта – це процес розпізнавання його при спробі входу в систему.

Аутентифікація – перевірка достовірності ідентифікатора суб'єкта. Після ідентифікації і аутентифікації відбувається процедура авторизації, тобто суб'єкт, який успішно пройшов попередні етапи отримує певні повноваження і доступ до ресурсів СЕД. Захищеність СЕД характеризується рівнем безпеки. Модель захищеної СЕД (рис. 3).

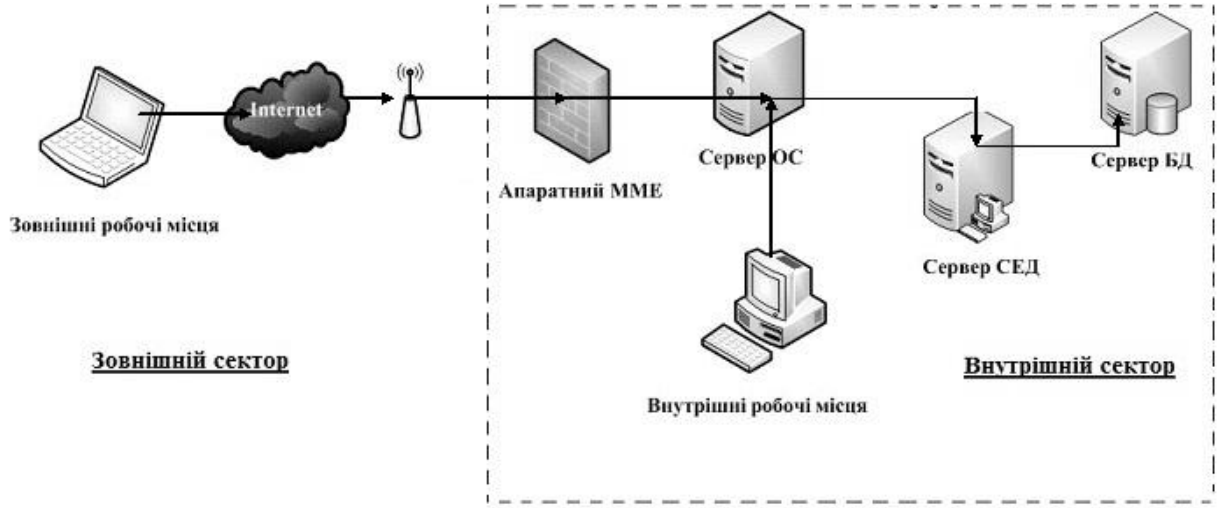

Рисунок 3 – Модель захищеної СЕД

В зовнішній сектор входять віддалені робочі місця, об'єднані в локально-обчислювальну мережу. В внутрішній сектор входить апаратний між мережевий екран (ММЕ), робочі місця, сервер бази даних (БД), сервер операційної системи (ОС) та сервер СЕД. Всі ці компоненти утворюють єдиний механізм доступу до електронних документів.

Інформаційна безпека СЕД досягається забезпеченням конфіденційності, цілісності і доступності ЕД. Безумовно, на сьогоднішній день, ринок засобів захисту інформації колосальний і зростає швидкими темпами. Тому виникає проблема вибору ефективних засобів захисту, які б задовольняли більшій кількості вимог і потреб.

Під ефективністю розуміється ступінь відповідності результатів захисту ЕД щодо поставленої мети. Завдання вибору засобів захисту, які б забезпечували надійну безпеку від множини загроз і мали б мінімальну собівартість є складною проблемо.

Перелік загроз постійно змінюється, тому оцінка ефективності системи захисту є необхідним і актуальним завданням. Існують кількісні і якісні критерії аналізу ефективності системи захисту ЕД. Переважно використовуються кількісні показники, оскільки вони є точнішими. Чисельні дослідження в своїй практиці показують такі типи критеріїв:

1) економічний показник, оцінює досягнення мети захисту при визначеній собівартості засобів захисту;

2) критерії оцінки якості СЗЕД, що визначені методами дискретного програмування;

3) імітаційні, штучні критерії на основі методів теорії нечітких множин.

Для вибору засобів забезпечення безпеки електронного документообігу можна використати показник ефективності, який базується на мінімізації затрат на засоби захисту, іншими словами – економічно ефективний показник. Даний критерій передбачає мінімальну вартість системи захисту і максимальні вимоги щодо забезпечення безпеки СЕД.

Варто враховувати, що СЕД в цілому э складним об'єктом, який виконує багато функцій. Захист структурних компонентів системи має виконуватися належним чином. Щодо побудови системи захисту електронних документів (СЗЕД) існує ряд варіантів та підходів, що відрізняються структурою, складом, принципом дії, техніко-економічними показниками, такими, як вартість, швидкодія та надійність. У зв'язку з несумісністю показників СЗЕД з певними засобами захисту, вибір конкретних методів захисту призводить до необхідності вирішення задачі оптимізації.

В загальному вигляді задачу оптимізації можна записати в наступному вигляді. Нехає є M = {1,…, m} – множина вимог захисту інформації; N = {1,…, n} – множина засобів захисту інформації, реалізованих різними способами і функціями захисту, що можливі для застосування в конкретному випадку; $p_1,...,\ p_n$ – вартість засобів захисту інформації. Потрібно визначити необхідний набір засобів захисту інформації $x_1,...,\ x_n$, щоб вартість рішення була мінімальною, а вибрані засоби задовольняли вимоги щодо захисту інформації. Таким чином, необхідно розв'язати наступну задачу оптимізації (1):

$$\sum_{j=1}^{n} p_j x_j \to \min \qquad (1)$$

$$\sum_{j=1}^{n} k_{ij} x_j \geq 1, i = 1,..., m, x_j \in \{0,1\}, j = 1,..., n \qquad (2)$$

$k_{ij} =$ 1, якщо j- засіб захисту закриває і- вимогу, 0 – в іншому випадку), де k_{ij} – коефіцієнти нейтралізації негативного впливу загроз. В результаті отримаємо задачу цілочисельного лінійного програмування (2), для розв'язання якої існують спеціальні методи.

Організація захисту ЕД має здійснюватися з урахуванням системного підходу, що забезпечує оптимальне поєднання взаємопов'язаних методологічних, організаційних, програмних та апаратних засобів. Розробка системи захисту СЕД повинна проводитися з урахуванням захисту від виявлених загроз і можливих інформаційних ризиків, для яких визначаються способи захисту, на основі запропонованого показника оцінки її ефективності. При цьому система має задовольняти таким вимогам:

1) система повинна розвиватися безперервно, так як способи реалізації загроз інформації безперервно вдосконалюються; управління інформаційною безпекою (ІБ) – це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення систем ІБ, безперервному контролі, виявлення її слабких місць, потенційних каналів витоку інформації і нових способів несанкціонованого доступу;

2) система повинна передбачати поділ і мінімізацію повноважень з доступу до ЕД і процедур обробки;

3) система повинна забезпечувати контроль і реєстрацію спроб несанкціонованого доступу, містити засоби для точного встановлення ідентичності кожного користувача і протоколювання дій;

4) забезпечувати надійність захисту ЕД та контроль за функціонуванням системи захисту, тобто використовувати методи і засоби контролю працездатності механізмів захисту.

Реалізація перелічених вимог при створенні системи захисту інформації в СЕД сприятиме організації ефективного захищеного документо-обігу [11]. Протидія загрозам безпеки є метою засобів захисту ЕД і системи в цілому. Захищена СЕД – система, засоби захисту якої успішно і ефективно протидіють загрозам безпеки.

ВИСНОВКИ. В статті описано принципи впровадження та функціонування СЕД. Проведено аналіз електронних документів, їх основних властивостей. Запропонована класифікація загроз ЕД за певними ознаками з метою формалізації задачі опису повної множини загроз. Досліджено механізми та засоби забезпечення безпеки СЕД, покзана модель захищеної СЕД. Показано оптимізаційну задачу оцінки ефективності системи захисту СЕД на основі визначення економічного показника ефективності. В результаті проведених досліджень сформульовано вимоги щодо розробки системи захисту СЕД.

ЛІТЕРАТУРА

1. Елисеев Н.И. Модель угроз безопасности информации при ее обработке в системе защищенного документооборота // Известия ЮФУ. Технические науки. Тематический выпуск. – Выпуск № 12 (137), том 137, 2012. – С. 112–118.

2. Математическая модель и методика разработки защищенных систем электронного документооборота на базе технологии IBM LOTUS NOTES/DOMINO / Н.В. Медведев, Г.А. Гришин, Д.П. Кацыв // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение», Москва. – 2007. – № 1(66). – С. 105–114.

3. 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. – 26 с.

4. Астахова Т.С., Чадаева Е.П. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа // Известия Томского политехнического университета, Хабаровск.– 2012. – Т. 320 – № 6. – С. 153–157.

5. Хорев А.А. Угрозы безопасности информации // журнал «Специальная Техника», Москва. – 2010. – № 1. – С. 58–63.

6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: Форум, 2008. – 416 с.

7. 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». – Том 13, № 3(2013). – С. 54–60.

8. Панасенко С.П. Защита электронных документов: целостность и конфиденциальность // Банки и технологии. – 2000. – № 4. – С. 82–87.

9. Koblitz N., Algebraic Aspects of Cryptography, Springer-Verlag, Berlin, 1998. – 215 p.

10. Панасенко С.П. Защита документооборота в современных компьютерных системах// Информационные технологии. – 2001. – № 4. – С. 41–45.

11. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота, Математическое обоснование и теоретические аспекты информационной безопасномти*:* Доклады ТУСУРа, Томск. – 2012. – № 1 (25), часть 2. – С. 52–56.

DEPLOYING AND MEASURING THE EFFECTIVNESS OF A SECURE DOCUMENT MANAGEMENT SYSTEM

I. Rozlomii

Cherkassy Bogdan Khmelnytckyi National Unersity

blvd. Shevchenko, 81, Cherkassy, 18031, Ukraine. E-mail: innulichka-best@inbox.ru

Purpose. The purpose of the article is to research different aspects of deployment and functioning of the Secure Document Management System (SDMS). Identifying and describing the set of possible threats to integrity and confidentiality of digital documents. Also, we analyze the effectiveness of methods of ensuring information security for the document management. Ensuring authenticity and integrity of digital documents in transit and preventing unauthorized access are the basis of reliable functioning of DMS. **Originality.** For the first time such a complete set of Security Threats for SDMS has been analyzed and the effectiveness of the information security methods against those threats has been measured. Based on the identified information security threats different ways of data leaking were determined and presented as a diagram. **Methodology.** We use Fuzzy Logic Theory for measuring the effectivness of a SDMS. The task of optimization is based on economical measurement, which shows level of achieving the goal of protecting while the cost of the tools for protecting information is defined. **Findings.** Model of the Secured DMS that has been built demonstrates the way to access digital documents and other information resources of the system. Standard cryptographic protection methods have been researched, among those are: encryption and Digital Signature (DS), principles of authentication and authorization. New criteria of measuring the effectiveness of the information security methods for SDMS have been discovered. **Practical value.** This methodology can be applied to evaluating SDMS using quantified economic criteria, which represent the effectiveness of the security methods of the SDMS. **Conclusions.** According to the achieved results, we have come up with the list of suggestions regarding the development of SDMS. References 12, figures 3.

Key words: confidentiality, integrity, availability, authentication, authorithation.

REFERENCES

1. Eleseev, N.A. (2013), "Threat Model for the Secure Document", *Izvestiya YuFU*, pp. 112–118.

2. Medvedev, N.V., Grishin, G.A. and Katsyv, D.P. (2007), "Mathematical models and Methods for Developing Secure Document Management systems with IBM LOTUS NOTES / DOMINO", *Bulletin of Moscow Bauman State Technological University "Instrument"*, no. 1 (66), pp. 105–114

3. 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, Berlin, Germany.

4. Astakhova, T.S. and Chadaev, E.P. (2012), "Using Digital Signature for Ensuring Integrity and Authenticity of the Document", *Bulletin of the Tomsk Polytechnic University*, no. 6, pp. 153–157.

5. Horev, A.A. (2010), "Information Security Threats", *Special Equipment*, no. 1, pp. 58–63.

6. Shangin, V.F. (2008), *Informatsionnaya bezopasnost kompyuternyih sistem i setey* [Information Security of Computer Systems and Networks], Forum, Moscow, Russia.

7. 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",* vol. 13, no. 3, pp. 54–60.

8. Panasenko, S.P. (2000), "Securing Digital Documents", *Integrity and Confidentiality in Information Technology*, no. 4, pp. 82–87.

9. Koblitz, N., (1998), *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin, Germany.

10. Panasenko, S.P. (2001), "Document Security in Modern Computer Systems", *Information technologies*, no. 4, pp. 41–45.

11. Buldakova, T.I., Glazunov, B.V. and Lyapina, N.S. (2012), "Evaluating the Security of Digital Document Management Systems, Mathematical Reasoning and Theoretical Aspects of Information Security", *Reports TUSUR*, no. 1(25), part 2, pp. 52–56.

Стаття надійшла 26.12.2015.