насамперед, створення і зберігання різних неструктурованих документів, підтримка версій документів і ЕЦП; структурування документів по папках; призначення прав доступу на документи; історія роботи з документами; повнотекстовий і атрибутивний пошук документів; підтримка процесів узгодження і обробки документів на всіх стадіях їх життєвого циклу; видача електронних завдань і контроль їх виконання; взаємодія між співробітниками в ході бізнес-процесів; підтримка вільних і жорстких маршрутів.[3]

Підхід до захисту електронного документообігу повинен бути комплексним. Треба тверезо оцінити потенційні загрози і ризики системи електронного документообігу та ступінь потенційних втрат від загроз. Захист системи електронного документообігу не зводиться до захисту документів і обмеження доступу до них. Захист системного обладнання, комп'ютерів, принтерів та інших пристроїв є важливим завданням, захист мережного середовища, в якій працює система, захист каналів передачі даних і мережевих пристроїв.

Комплекс організаційних заходів відіграє важливу роль на кожному рівні захисту. Погана організація може звести нанівець всі технічні дії, незалежно від того, наскільки вони досконалі. При виборі засобів захисту слід оцінити реальні втрати від розкриття або спотворення інформації і порівняти з вартістю засобів захисту [4]. Але будь-якому випадку слід вводити елементарні, найдешевші і не менш ефективні засоби - вхід в систему управління документами повинен здійснюватися через систему паролів з розмежованими рівнями доступу. Фізичний доступ в приміщення, де встановлена система управління електронним документообігом, повинен здійснюватися відповідно до внутрішніх правил та бути обмежений стороннім особам.

Список використаних джерел

1. Про електронні документи та електронний документообіг [Електронний ресурс] – Режим доступу: URL: http://zakon1.rada.gov.ua/laws/show/851-15
2. Про електронний цифровий підпис [Електронний ресурс] – Режим доступу: URL: http://zakon2.rada.gov.ua/laws/show/852-15/
3. DIRECTUM - [Електронний ресурс]: – Режим доступу: URL: https://ru.wikipedia.org/wiki/Directum
4. ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ [Електронний ресурс] – Режим доступу: URL: http://elartu.tntu.edu.ua/bitstream/lib/23058/2/CAZST_2017v2_Zavodyanskiy_V_O-Protection_of_information_65-66.pdf

---

УДК 004.056.55

АНАЛІЗ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Коротка Г. М., студ. гр. КБ-161,
Петренко Т. А., доцент кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка»

Всі підприємства, незалежно від форми власності, масштабів та сфери діяльності, створюють, опрацьовують та зберігають документи. Організація системи електронного документообігу (СЕД) – дієвий сучасний процес документообігу, що дозволяє оптимізувати роботу компанії. Електронні документи можуть одночасно використовуватися співробітниками в рамках однієї робочої групи, відділу або всього підприємства. На відміну від паперового документообігу, де процес одержання доступу до документів може тривати декілька хвилин, годин, днів, а іноді і тижнів, доступ до електронних документів здійснюється за декілька секунд. Використовуючи СЕД, будь-яка організація зможе заощаджувати свій робочий час та приймати оперативні рі

шення в декілька разів швидше.

Широке використання СЕД робить актуальною проблему захисту інформації, адже у міру розвитку технологій електронних платежів та документообігу є велика небезпека втручання сторонніх осіб, з метою завдання шкоди підприємству, що призведе до значних збитків. У захищеній СЕД інформація у процесі обміну буде доступною конкретному колу користувачів без можливості її фальсифікації або модифікації у процесі передачі [1].Традиційний підхід до захисту інформації заснований на попередньому аналізі загроз і зіставленні їм сукупності механізмів захисту. Основні загрози для систем електронного документообігу представлені на рисунку 1.

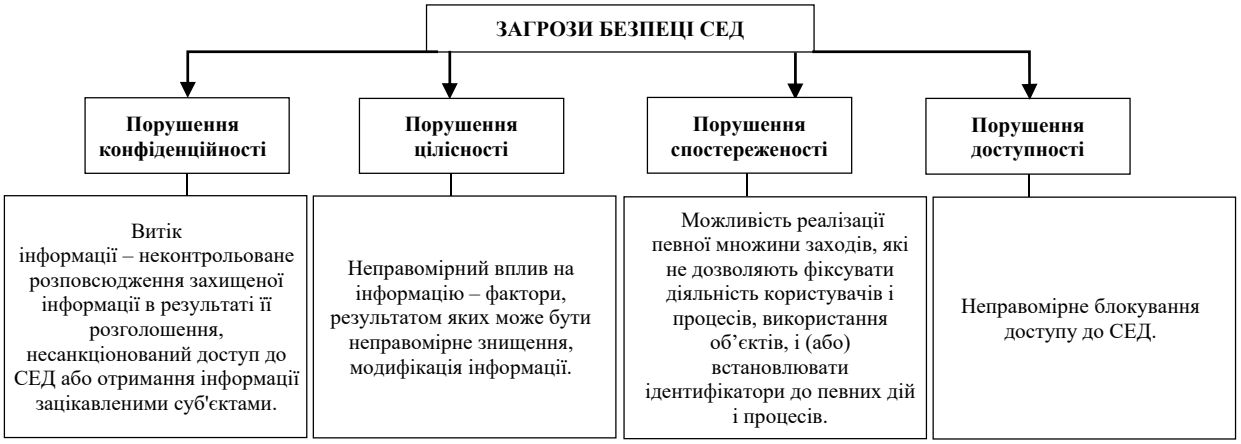

Рисунок 2 – Класифікація загроз для СЕД

Загальні проблеми захисту електронного документообігу розкриті в роботах Г.А. Гришина, Б.В. Глазунова, А.А. Козуба, Р.В. Мещерякова, М.В. Соловйова, Б.Р. Досмухамедова, І.Д. Корольова, С.П. Панасенка та інших науковців. В працях Т.І. Булдакова, Н.І. Єлісєєва, Н.В. Медведєва досліджено моделі загроз безпеки інформації в системах документообігу, методики розробки захищених систем електронного документообігу.

Мета даної статті – обґрунтувати складові та принципи функціонування СЕД, а також охарактеризувати аспекти інформаційної безпеки під час організації СЕД.

Функціональні елементи, пропоновані СЕД своїм користувачам можна розділити на такі категорії:

1. Збереження і централізований пошук документів – найважливіший аргумент використання СЕД. Використовуються системи управління базами даних, наприклад, Microsoft SQL, Oracle та інші.

Серед функцій для пошуку документів розрізняють:

−пошук за вкладеними в документи файлами (повнотекстовий пошук);

−складний пошук (з використанням логічних операцій);

−гнучка система надання прав доступу.

2. Функції підтримки канцелярії та діловодства:

−реєстрація документа у вигляді електронної картки – аналога реєстраційної картки документа;

−повний цикл роботи з вхідними/вихідними документами;

−ведення журналів реєстрації та обліку паперових оригіналів документів.

3. Функції маршрутизації і контролю виконання документів дозволяють керувати та контролювати виконання робіт з документами:

−підтримка різних дій над документами під час маршруту: узгодження, накладення резолюції, підписання тощо;

−повідомлення працівників про надходження до них на виконання нових документів;

−автоматичний контроль термінів виконання документів та звіти про виконання робіт з документами.

4. Функції інформаційної безпеки [2]. На основі загроз інформаційній безпеці СЕД можна виділити наступні елементи захисту, що представлені на рисунку 2.

Рисунок 2 – Складові захисту системи електронного документообігу

Основне проблемне місце при організації захисту СЕД – це забезпечення конфіденційності. Як тільки документ потрапляє до користувача, конфіденційність цього документа по відношенню до користувача вже порушена. Користувач може знайти безліч способів скопіювати інформацію, від збереження його на зовнішній носій до банального фотографування. Тому протоколювання дій користувачів – важливий пункт захисту СЕД. Для запобігання загроз спостереженості необхідна правильна організація ведення історії дій користувачів у системі, що дає смогу слідкувати за діями користувачів і, у випадку виникнення спроб несанкціонованого доступу швидко знаходити зловмисника. Ця складова є невід'ємною частиною захищеної СЕД. За відсутністю її використовують програмне забезпечення для захисту систем керування базами даних та місця зберігання даних (наприклад, категоріювання користувачів, політика безпеки, безпека доступу, безпека даних, авторизація та ін. у БД від компанії Oracle, продуктами якої користуються різні СЕД).

Забезпечення безпечного доступу до даних в середині СЕД реалізується зазвичай автентифікацією та розмежуванням прав користувачів. Найпоширенішим серед всіх способів автентифікації користувача є логін і пароль, другим по надійності є Toch-«ключі» (автентифікація відбувається шляхом вводу певного коду – смарт карти, USB-ключі, CD та інші), і найбезпечнішим є біометричний метод розпізнавання користувача системи (зчитування відбитків пальців, конфігурації сітківки ока та ін.) [3]. У СЕД обов'язково повинно бути передбачено розмежування прав користувачів. Розмежування прав у системі налаштовується по-різному: це може бути підсистема, що створена розробниками СЕД, або підсистема безпеки системи керування базами даних, яку використовує СЕД.

Забезпечення цілісності інформації є однією з складових задач в процесі електронного обміну даних. Одним з ефективних способів забезпечення цілісності електронних документів є засоби криптографії, зокрема використання електронного цифрового підпису. 7 листопада 2018 року набув чинності Закон України «Про електронні довірчі послуги». Одним із важливих нововведень закону про електронні довірчі послуги є те, що він запроваджує поняття «**кваліфікований електронний підпис**», яке замінило поняття «електронного цифрового підпису». Кваліфікований електронний підпис (КЕП) – спосіб криптографічного шифрування тексту електронного документа унікальною послідовністю символів, які знає тільки відправник [4]. КЕП призначений для захисту документа від підробки. Принцип роботи КЕП заснований на технології шифрування з асиметричним ключем, тобто ключі для шифрування та дешифрування даних різні. «Закритим» ключем шифрують, а «відкритим» – розшифровують інформацію. Текст електронного документа разом з КЕП передається отримувачу, який повинен перевірити на цілісність документа наявністю КЕП. Для перевірки КЕП він використовує «відкритий» ключ відправника – таку ж унікальну послідовність символів, але, що знаходиться у відкритому доступі та пов'язана з «закритим» ключем відправника. Перевірка КЕП вважається пройденою, якщо «відкритий» ключ відправника буде

однаковий з «закритим». Якщо до тексту електронного документа були внесені зміни після його підписання КЕП, то система заблокує дану процедуру. Таким чином, підписати електронний документ може тільки власник «закритого» ключа, а перевірити наявність КЕП – будь-хто, у кого є «відкритий» ключ, відповідний «закритому» ключу відправника.

Отже, було систематизовано і виділено принципи функціонування, засоби захисту інформації у ході організації електронного документообігу. Впровадження СЕД забезпечує підприємство усім необхідним для своєчасного прийняття рішень, реагування на ситуації та оптимізація робочого процесу на підприємстві. СЕД можна називати захищеною, якщо в ній присутні такі системи захисту інформації: захист електронних документів, що містять конфіденційну інформацію, шляхом перевірки її КЕП на цілісність даних; керування доступом та автентифікація; контроль та протоколювання роботи співробітників з документами та ін..

Напрямком подальших досліджень є створення моделі всебічно захищеної системи електронного документообігу, що може бути використаною у діяльності реального підприємства для підвищення рівня інформаційної безпеки та ефективності його роботи.

Список використаних джерел

1. Кандзюба С. П. Електронний документообіг. Реінжиніринг адміністративних процесів в органах публічної влади / Кандзюба С. П., Матвійчук Р. М.. – Київ, 2017.
2. Матвієнко О. Основи організації електронного документообігу. Навчальний посібник / Матвієнко О., Цивін М. – Київ: Центр учбової літератури, 2008. – 112 с.
3. Кукарін О. Б. Електронний документообіг та захист інформації. Навчальний посібник / Кукарін О. Б. – Київ: НАДУ, 2015. – 84 с.
4. Закон України «Про електронні довірчі послуги». https://zakon.rada.gov.ua/laws/show/2155-19.

УДК 004.056.53

МЕТОДИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ ВІД КИБЕРАТАК

Вильотніков В. В., студ. гр. КБ-161
Науковий керівник**: Базилевич В. М.,** к.е.н., доцент
Національний університет «Чернігівська політехніка»

На сьогоднішній день, зважаючи на велику інформатизацію суспільства, потребу у мобільності користувачів мережі Internet все більшою і більшою популярністю користуються бездротові мережі. Сучасний розвиток бездротових мереж дозволяє встановлювати з'єднання такої ж якості, як і мережі з використанням фізичного середовища передачі даних, але із значно більшою кількістю користувачів. Але при цьому виникає необхідність захисту переданої інформації в таких типах мереж, тобто використання механізмів захисту і шифрування даних. Так як загрози інформаційним ресурсам, в деяких випадках, можуть бути великими і катастрофічними. Тому актуальним є дослідження методів підвищення ефективності захисту інформації в бездротових комп'ютерних мережах.

Для проведення досліджень необхідно провести аналіз можливих загроз, визначити результати їх впливу та здійснити системний аналіз методів захисту від них.

Базовим стандартом, який визначає набір протоколів для передачі даних в бездротових мережах є IEEE 802.11. Цей стандарт постійно доповнюється та оновлюється, таким чином його нові версії були опубліковані в 1999, 2007, 2012 роках, а також наступна очікується ще в 2016 році.

Існують основні та допоміжні методи захисту бездротових мереж.

Основними протоколами, які використовуються на даний час в бездротових мережах є: WEP Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access II), а