Список використаних джерел:

1. Безпека життєдіяльності: Навчальний посібник / Юрій Скобло, Валентин Цапко, Дмитро Мазоренко, Леонід Тіщенко; Ред. В.Г. Цапко. – 4-те вид., перероб. і доп. – К.: Знання, 2006. – 397 с.
2. Лапін В.М., Навч. посібник. – Львів: Львівський банківський коледж, 1998. – 192 с.
3. Мягченко О.П. Безпека життєдіяльності людини та суспільства. – Навч. пос. – К.: Центр учбової літератури, 2010. – 384 с.

Розломій І.О.

аспірант,

Черкаський національний університет імені Богдана Хмельницького

АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Створення і функціонування системи електронного документообігу (СЕД) сприяє ефективній організації процесу обміну інформацією. Проте впровадження СЕД має специфічні проблеми, головною з яких є необхідність управління інформаційною безпекою (ІБ) і забезпечення захисту електронних документів.

В електронному середовищі процес обробки документованої інформації представляє собою складний організаційно-технічний процес, що супроводжується загрозами ІБ. Реалізація загроз ІБ може призвести до втрати ЕД правового статусу і, як результат нанесенню збитку [1, с. 1]. В роботі розглянуто основні види загроз ІБ, можливі збитки від їх реалізації та способи розрахунку ризиків.

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

Безпечний обмін та збереження електронних документів є основною функцією сучасних систем захищеного документообігу. Захищеність СЕД забезпечується сукупністю програмно-технічних засобів захисту інформації і процесів її обробки від доступу нелегітимних користувачів чи процесів [2, с. 8]. Надання правого статусу ЕД має відповідати таким вимогам:

1) конфіденційність – право доступу лише для тих користувачів (процесів), що володіють визначеними правами доступу;
2) цілісність – незмінність компонентів ЕД;
3) доступність – можливість доступу до ЕД;
4) легітимність – правомірне використання ЕД і технологій їх обробки;
5) достовірність – повне і точне відображення ЕД;
6) автентичність – ідентичність ЕД на протязі всього життєвого циклу.

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 випадкові чи навмисні 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.

При розгляді проблеми захисту СЕД використовується така її властивість, як вразливість. Вразливість СЕД – характеристика системи, що сприяє виникненню загрози. Вразливість може проявлятися в недостатній захищеності та помилках системи. Моделювання процесів порушення інформаційної безпеки доцільно здійснювати на основі розгляду взаємозв'язку загроз, їх джерел та способів реалізації, вразливості, методів захисту та наслідків рис. 1.

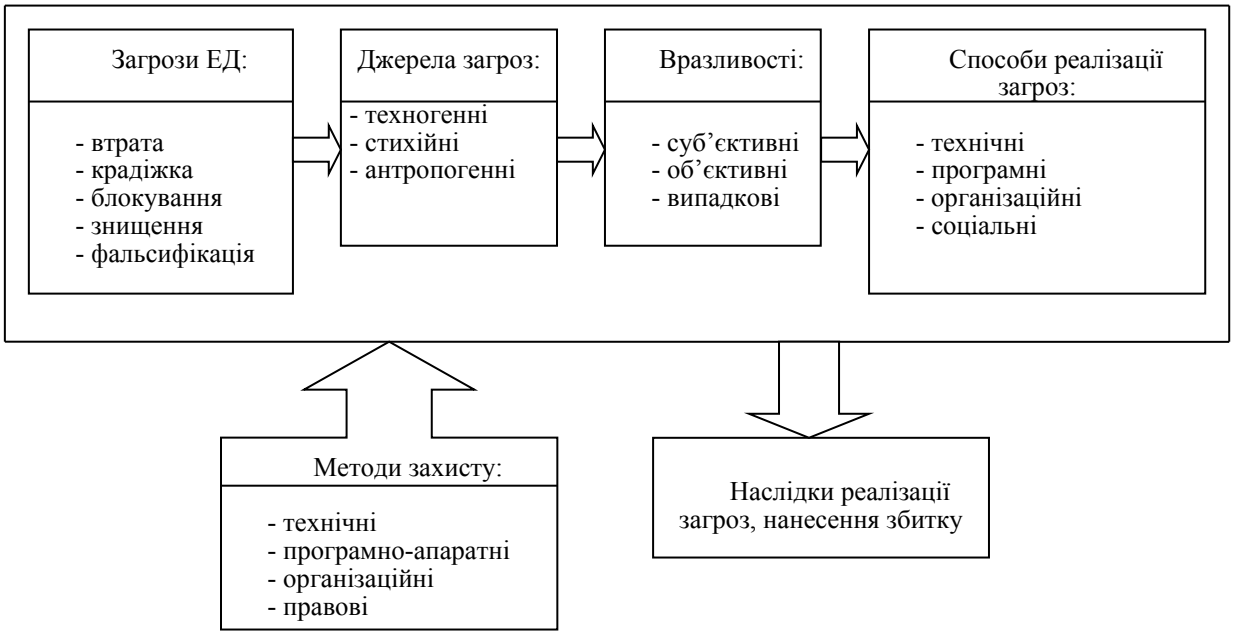

Рис. 1. Модель реалізації загроз безпеці ЕД

Виконання вимог, щодо захисту ЕД характеризується критерієм досягнення мети в сфері безпеки. Критерій ефективності – мінімальні витрати на виконання поставлених функціональних вимог захисту ЕД, який можна показати в вигляді задачі (1).

$$\sum c_i \rightarrow min, \qquad (1)$$

де c_i – витрати на *i*-й засіб захисту. Головним недоліком даного підходу є те, що досить складно визначити найефективніший рівень захисту ЕД, за умови чітко визначених вимог захисту.

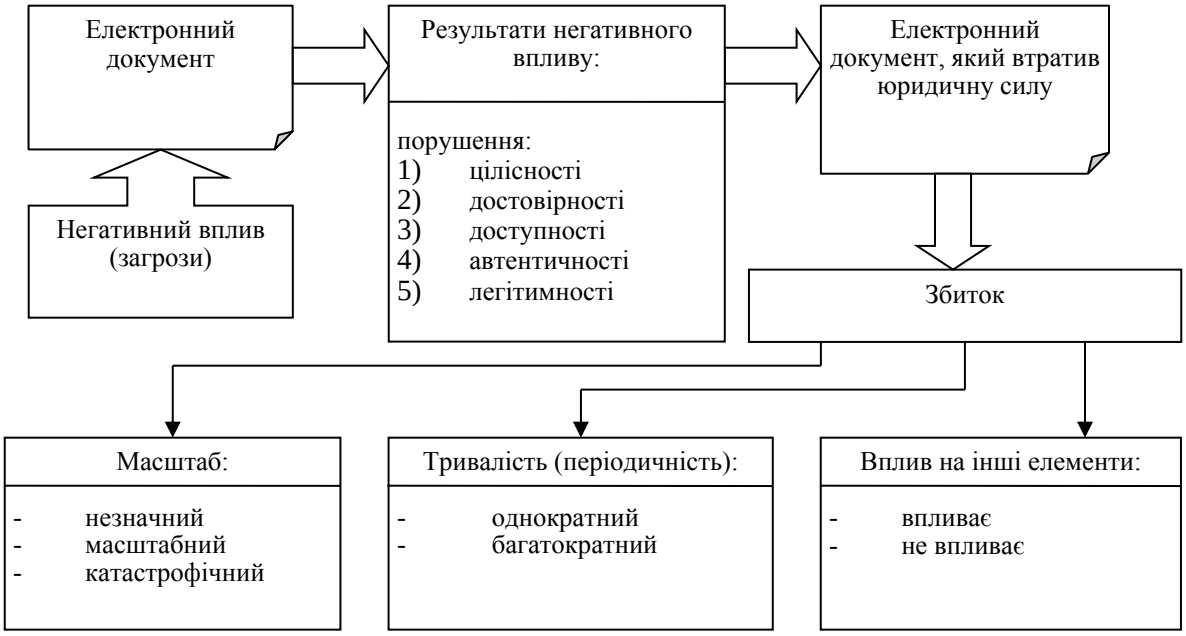

Рис. 2. Схема нанесення збитку від впливу загроз на ЕД

Як показує схема моделі реалізації загроз безпеці ЕД, в процесі обробки на ЕД можуть впливати різні негативні чинники, що призводять до втрати документом юридичної сили. В загальному вигляді схема зв'язку причин і наслідків впливу загроз на ЕД показана на рис. 2.

Важливим етапом розробки системи захищеного документообігу є оцінка ризиків ІБ системи. Перелік загроз, оцінки ймовірності їх реалізації, а також модель порушника служать основою для аналізу ризиків здійснення загроз і формулювання вимог до системи захисту СЕД. Ризик – потенційна можливість понести збитки через порушення безпеки СЕД. Ризик, на відміну від загрози, визначається кількісною оцінкою можливих втрат і ймовірності реалізації загроз [3, с. 2]. Для оцінки ризиків інформаційних загроз безпеці ЕД існує ряд методів та підходів, які можна розділити на:

1) методи, які використовують оцінку ризику на якісному рівні, наприклад, за шкалою – низький, середній, високий ризик;

2) кількісні методики, тобто ризик оцінюється числовим значенням, наприклад, розмір очікуваних втрат за певний проміжок часу;

3) методи, що використовують комбіновані оцінки [4, с. 5].

Найпростіший спосіб оцінки ризиків за двома факторами: ймовірність здійснення загрози (негативного впливу) та вартість можливих наслідків, його можна виразити формулою (2).

$$R = P_i \times C, \tag{2}$$

де, P – ризик ІБ, P_i – ймовірність здійснення i-ї загрози, C – вартість можливих наслідків.

Деякі методи для оцінки ризиків використовують три параметри: ймовірність здійснення загрози, вразливість та вартість можливих наслідків. В такому разі ризик охарактеризувати такими факторами:

1) загроза, реалізацією якої може бути викликаний даний ризик;

2) ЕД, по відношенню до якого може бути реалізована загроза;

3) вразливість, через яку може бути реалізована загроза по відношенню до ЕД [5, с. 11].

Відповідно, ризик обчислюється за формулою (3).

$$R = P_i \times V \times C, \quad (3)$$

де, P – ризик ІБ, P_i – ймовірність здійснення i-ї загрози, V – вразливість СЕД, C– вартість можливих наслідків.

Таким чином, ключовими вимогами до сучасної захищеної СЕД є надання легітимним користувачам доступу до ЕД і засобам їх обробки. Порушення функціонування СЕД може призвести до втрати юридичної сили ЕД і, як наслідок, збитку. Модель загроз та схема нанесення збитку дозволяє визначити необхідні заходи забезпечення ІБ. Показані способи оцінки ризиків, які необхідно здійснювати з метою розробки рекомендацій щодо зниження рівня ризиків, а також прийняття ефективних рішень забезпечення інформаційної безпеки ЕД.

Список використаних джерел:

1. Елисеев Н.И. Модель угроз безопасности информации при ее обработке в системе защищенного документооборота // Известия ЮФУ. Технические науки Тематический выпуск. – 2013. – 7 с.

2. Ярочкин В.И. Информационная безопасность // В.И. Ярочкин. – М.: Фонд «Мир»: Акад. Проект. – 2003. – 640 с.

3. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности // Доклады ТУСУРа. – 2012. – № 1(25). – 7 с.

4. 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. – 2014. – № 1(2). – 10 с.

5. Симонов С.П. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2 (117). – 32 с.

Сорокін В.А, Дзьон В.М.

студенти,

Науковий керівник: **Вовк Р.Б.**

кандидат технічних наук, доцент,

Івано-Франківський національний технічний університет нафти і газу

ПРОЕКТУВАННЯ ЕЛЕКТРОННОЇ СИСТЕМИ АВТОМАТИЗОВАНОГО ОБЛІКУ ПАЦІЄНТІВ У МЕДИЧНИХ ЗАКЛАДАХ

На даний час системи обліку пацієнтів в медичних закладах України знаходяться на досить низькому рівні. Протягом останніх 24 років, з моменту розпаду СРСР, використовуються застарілі і примітивні методи ведення медичної статистики для пацієнтів. Щодня громадяни стикаються з реальними