Запека М.Ю.
спеціальність «Інформаційні системи та технології»
Науковий керівник - к.т.н., доцент Дегтярьова Лариса

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА ЕЛЕКТРОНИХ СИСТЕМАХ ДОКУМЕНТООБІГУ

Широке використання спеціалізованих і глобальних інформаційних систем (ІС) в органах управління, структурах охорони здоров'я, на транспорті та у сфері державотворення дають можливість накопичувати і передавати величезні обсяги цінної інформації [1].

Системи захисту інформації в інформаційних системах (ІС) та в електронних системах документообігу (ЕСД), що можуть використовуватись в межах «діяльності» певної інформаційної системи, повинні відповідати запитам сьогодення в умовах росту числа потенційних інформаційних загроз, які виникають в процесі функціонування самих корпоративних мереж. Сучасні системи безпеки повинні захищати не окремі елементи мережі, а інформаційні потоки і ресурси незалежно від місця й часу їх створення та використання.

Для коректного функціонування сучасних ІС та ЕСД виникає потреба у комплексному використанні методики виявлення ризиків та підтримки корпоративних систем захисту інформації, залежно від галузі, форми власності, кількості і чисельності підрозділів підприємств в межах єдиної системи. Отже, виникає необхідність вирішення ряду питань, які дозволять:

- оцінити наявний рівень інформаційної безпеки компанії, що потребує виявлення ризиків, які можуть виникнути на всіх рівнях забезпечення захисту інформації: правовому, організаційно-управлінському, технологічному, маркетинговому, фінансовому та технічному;
- розробити і реалізувати план дій та спланувати кількість фінансових вкладень для розробки або/та вдосконалення корпоративної системи захисту інформації для досягнення прийнятного рівня захищеності інформації компанії.

Система обміну даними в межах ІС та ЕСД повинна забезпечити не тільки передачу інформації, але її збереження від викрадення чи модифікації, а також мати можливість її швидкого відновлення. Переважна більшість випадків втрат інформації стаються через причини, обумовлені помилками користувачів. Це досить розповсюджена ситуація в організаціях з необізнаними користувачами, які не дотримуються основних заходів кібернетичної безпеки. Також мають місце проблеми щодо втрати даних через недбале ставлення до технічного стану техніки, задіяної для передачі інформації. Тому проведення періодичного технічного обслуговування апаратного обладнання створить умови для її безперебійного і правильного функціонування [2].

До основних і найбільш дієвих методів, які входять до комплексної системи забезпечення інформаційного захисту входять [3]:

• Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту обчислювальної техніки, які спеціально призначені для створення фізичних перешкод на потенційно можливих шляхах проникнення і несанкціонованого доступу до компонентів ІС, що потребують захисту.

• Апаратні засоби захисту – це різні електронні, електронномеханічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів ОТ: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

• Програмні засоби захисту, які входять до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

• Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.

•Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації.

• Криптографічні методи захисту – це методи, основані на криптографічних перетвореннях даних, тобто на їх шифруванні. Їх застосування забезпечує конфіденційність документа навіть у разі його потрапляння до рук сторонньої особи.

Треба зазначити, що до механізмів забезпечення інформаційної безпеки належать прийоми розподілу рівнів доступу до інформації в залежності від статусу кожного співробітника в межах його функціональних обов'язків. В якості цих засобів захисту виступають паролі, які використовуються для підтвердження особи або її рівня доступу до певної інформації, що циркулює в ІС або ЕСД.

Отже, значного підвищення безпеки будь-якого об'єкта можна досягти шляхом багаторівневої та багатокомпонентної побудови системи захисту, яка забезпечує збереження документів, безпечний доступу до інформації, при цьому зберігаючи достовірності документів та протоколювання дій користувачів.

Список використаних джерел

1. Дегтярьова Л.М., Мірошникова М.В., Волошко С.В. Аналіз структури системи захисту інформації. Полтава, 2019. № 2 (54). С. 78-83.

2. Захист інформації в системах обміну даними : стаття. URL: https://www.mil.gov.ua/ukbs/zahist-informaczii-v-sistemah-obminu-danimi.html

3. Олійник А.В., Шацька В.М. Інформаційні системи і технології у фінансових установах. Львів: Новий Світ-2000, 2006. 436 с.