УДК 004.056.5:002

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Санжарова А. К.
Науковий керівник – ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: alina.sanzharova@nure.ua .

The work examines potential threats and the most common ways of information leakage from electronic document management systems, analyzes the main measures aimed at increasing data security, protecting confidential information and minimizing cyber threats.

Для швидкого та якісного управління в установах різного рівня все більш широко використовуються системи електронного документообігу (ЕД). Однією з найважливіших вимог до будь-якої системи електронного документообігу (СЕД) є забезпечення безпеки електронного обміну документами. Це пов'язано із збільшенням кількості конфіденційних документів в органах державної влади і організаціях різної форми власності і активним переходом систем документообігу до електронного вигляду.

Найпоширенішими шляхами витоку інформації із системи електронного документообігу є: викрадення носіїв інформації та документів, які є результатом роботи системи; копіювання інформації на персональному комп'ютері; несанкціоноване підключення до апаратури та ліній зв'язку; перехоплення електромагнітного випромінювання в процесі обробки інформації. Основними загрозами для систем електронного документообігу є: загроза конфіденційності, цілісності, доступності інформації. Захист від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. Захист ЕД повинен бути комплексним, включаючи технічні, криптографічні та організаційні методи захисту інформації. В комплекс заходів захисту електронної документації повинні входити: обмеження прав фізичного доступу до об’єктів системи документообігу, розмежування прав доступу до файлів і папок, підтвердження авторства електронного документу, контроль цілісності і конфіденційності ЕД, забезпечення юридичної сили ЕД, забезпечення надійності функціонування технічних засобів, забезпечення резервування каналів зв’язку, резервне дублювання інформації, захист від вірусів [1].

Для забезпечення збереження ЕД застосовується резервне копіювання документів, зберігання їх в архіві, який знаходиться в захищеному хмарному середовищі на декількох дата-центрах.

Для обмеження доступу до ЕД користувач, який бажає увійти в свій акаунт, повинен пройти процедуру аутентифікації. Це може бути здійснено

різними способами, такими як введення пароля, використання USB-ключа або сканування відбитку пальця. Процедура аутентифікації може бути багатоетапною, що містить кілька кроків: пароль і ключ або пароль і біометрична фіксація. Біометричний спосіб проведення ідентифікації й подальшої аутентифікації користувачів є максимально надійним.

Розмежування прав доступу дає змогу мати доступ до окремих документів лише певному колу користувачів. Також воно може передбачати не лише можливість доступу до документів, а й дозвіл на їх підписання за допомогою електронного цифрового підпису (ЕЦП).

Відповідно до статті 6 Закону України «Про електронні документи та електронний документообіг» [2] електронний підпис є обов'язковим реквізитом електронного документу, який використовується для ідентифікації автора та/або підписувача ЕД іншими суб'єктами електронного документообігу. Захищеність ЕЦП від відтворення чи підробки базується на застосуванні у відповідних технологіях методів криптографії.

Для дотримання конфіденційності в СЕД можуть застосовуватися криптографічні методи шифрування даних. Застосування криптографії не дадуть шансу порушити конфіденційність ЕД навіть у разі його потрапляння до сторонніх осіб.

Одним із важливих елементів захисту електронного документообігу є протоколювання дій користувачів СЕД, яке дає можливість відстежувати всі неправомірні дії користувачів та знаходити «винуватця», а в разі оперативного втручання – навіть зупинити спробу неправомірних або шкідливих дій.

Захист СЕД не зводиться лише до захисту документів і розмежування доступу до них. Важливими є питання захисту апаратних засобів системи, персональних комп'ютерів, принтерів та інших пристроїв; захисту мережевого середовища, в якому функціонує система, захист каналів передачі даних і мережевого устаткування, можливе виділення СЕД в особливий сегмент мережі [3].

Список використаних джерел:

1. Безпека електронного документообігу: особливості захисту СЕД. URL:https://edin.ua/bezpeka-elektronnogo-dokumentoobigu-osoblivosti-zaxistu-sed/ (дата звернення: 12.02.2024).

2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР : станом на 01.01.2020 / Верховна Рада України // ЛІГА: ЗАКОН. URL: https://ips.ligazakon.net/document/t030851 (дата звернення: вказати дату).

3. Електронний документообіг та захист інформації: вебсайт. URL: https://e-pidruchniki.com/content/2157_164_Elektronnii_dokymentoobig_ta_zahist_informacii.html (дата звернення: 11.02.2024).