УДК 37.091.9;004.056:004.738.5 https://doi.org/10.31713/ve120259
JEL: M10

Маланчук Л. О. [1; ORCID ID: 0000-0002-6341-5639],
к.е.н., доцент,
Мордас О. М. [1; ORCID ID: 0009-0005-1597-3520],
здобувач вищої освіти першого (бакалаврського) рівня

[1]*Національний університет водного господарства та природокористування, м. Рівне*

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Статтю написано з метою дослідження способів та засобів захисту конфіденційної інформації в системі електронного документообігу. Проаналізовано основні способи та методи захисту конфіденційної інформації в ЕД, порівняння та дослідження систем захисту інформації, кібербезпека, робота із конфіденційною інформацією та системами захисту. Виокремлено найкращі із способів, методів та систем захисту для КІ в електронному документообігу.

Ключові слова: конфіденційна інформація; інформація; електронний документообіг; кібербезпека; система захисту; захист; програмне забезпечення.

Постановка проблеми. В нинішніх умовах життя, у світі електроніки, електронних ресурсів, електронному середовищі та цифровізації надважливим є питання захисту, будь-якої, інформації незалежно від структури, установи тощо. Електронний документообіг відіграє важливу роль у роботі та функціонуванні певних організацій. Така система дозволяє заощадити витрати та набагато швидше та ефективніше працювати й виконувати дії та завдання, однак із розвитком цифрових технологій ця система потребує захисту. Важливим є питання кібербезпеки для забезпечення захисту конфіденційної інформації документів в електронному документообігу. На жаль, система електронного документообігу, як і будь-яка інша, є вразливою до хакерських атак, зломів, шкідливого програмного забезпечення.

Мета статті. Метою статті є дослідження захисту конфіденційної інформації в системах електронного документообігу.

Виклад основного матеріалу. З початком розвитку цифрових технологій почала масово застосовуватися в різних підрозділах

система електронного документообігу. Це допомагає значно підвищити рівень ефективності процесів, які раніше виконувалися за довший період часу. Але серед багатьох переваг цієї системи, існує ризик доступу до інформації стороннім особам, кіберзагрози, фішинги, виток даних із бази, що робить питання захисту конфіденційної інформації одним із найважливіших. В табл. 1 наведено основні загрози для системи електронного документообігу.

Таблиця 1

Основні загрози для системи електронного документообігу

№	Загроза	Опис
1.	Загроза цілісності	Знищення, пошкодження або часткове спотворення матеріалів та інформації. Може здійснюватися у випадку збоїв системи та через атаки зловмисниками
2.	Загроза працездатності системи	Загроза, яка провокує порушення чи припинення роботи СЕД, як через навмисні хакерські атаки, так збої в обладнанні та помилки користувачів
3.	Неможливість доказу авторства	Якщо в СЕД не використовується електронний підпис, то неможливо довести, що тим чи іншим користувачем було створено документ. Документообіг – не юридично значущий
4.	Загроза доступності	Порушення можливості отримати потрібну інформацію користувачам, які мають доступ до неї за доступний проміжок часу
5.	Загроза конфіденційності	Порушення конфіденційності (перехоплення інформації, крадіжка тощо)

Джерело: складено автором на основі [1].

Серед загроз конфіденційності інформації в СЕД виділяють зовнішні та внутрішні загрози. Кожна з них несе пряму загрозу для системи електронного документообігу.

До зовнішніх загроз належать:

– кіберзлочинність;
– фішингові атаки;

– використання шкідливого програмного забезпечення (віруси, шпигунське ПЗ тощо);

– перехоплення даних під час передавання через незахищені канали зв'язку.

Внутрішні загрози зазвичай спричинені через самих працівників структур. До таких загроз відносять:

– людський фактор;

– зловмисні дії працівників;

– неналежна політика доступу [2].

Аби зменшити ризики потрібно впроваджувати певні заходи захисту інформації. Це не простий та складний процес. Щоб уникнути великої кількості кібератак, потрібно використовувати потужні методи кібербезпеки. Кожна з організацій має знати основні методи захисту конфіденційних даних. Необізнаність та втрата даних може завдати шкоди руйнівного характеру. Конфіденційна інформація є особливо важливою інформацією, яка потребує належного захисту.

Існує чимало методів захисту конфіденційної інформації, які наведено в табл. 2.

Таблиця 2

Методи захисту КІ

№	Метод	Опис
1.	Класифікація та організація даних	Процес упорядкування даних за критеріями, які спрощують доступ, знижує витрати на зберігання, а також підвищує безпеку. Допомагає визначити рівень ризику, розмежувати загальнодоступну та приватну інформацію та застосувати потрібні заходи захисту. Політика класифікації сприяє оцінці використання конфіденційних даних та забезпечення безпеки
2.	Шифрування даних	Метод шифрування передбачає кодування даних складним алгоритмом, який надає захист від крадіжки чи розкриття інформації. Без ключа дешифрування дані практично неможливо зламати. Шифрування забезпечує конфіденційність передачі інформації підтримує аутентифікацію. Його варто застосовувати для захисту надчутливої інформації

продовження табл. 2

3.	Оцінка на захист персональних даних (DPIA)	DPIA – це один з інструментів захисту корпоративної інформації, що допомагає оцінити ризики обробки даних. Також визначити їхній обсяг та мету, запровадити заходи безпеки та забезпечити відповідність вимогам
4.	Маскування (обфускація) даних	Метод захисту, який спрямований на заміну оригінальних даних фіктивними. Таким чином, можна приховати дані від розробників, випробувачів та інших фахівців компанії
5.	Багатофакторна автентифікація	Паролі та аутентифікація – це простий спосіб захисту, але дані корпорацій часто опиняються в DarkNet, тому варто використовувати багатофакторну автентифікацію для підвищення безпеки
6.	Резервні копії	Резервне копіювання – ключовий елемент управління безпекою даних, який слід виконувати не рідше ніж раз на тиждень
7.	Надійна мережна безпека	Надійна мережева безпека включає різні інструменти для захисту конфіденційних даних від крадіжки та несанкціонованого доступу, зокрема антивірусне ПЗ, DLP-системи, IDS/IPS, брандмауери, VPN, сегментацію мережі та засоби видалення даних

Джерело: складено автором на основі [3].

Захист конфіденційної інформації в системі електронного документообігу повинен відповідати чинному законодавству та усім міжнародним стандартам інформаційної безпеки. Це регулюється основним нормативним документом – Законом України «Про захист інформації в інформаційно-комунікаційних системах». Саме цей закон регулює правові та організаційні засади захисту інформації в державних і приватних системах. Він визначає вимоги до обробки, зберігання та передачі даних, встановлює заходи безпеки та відповідальність за їх порушення. Закон спрямований на запобігання несанкціонованому доступу, втраті або викривленню інформації, що є критично важливим для кібербезпеки України [4].

Висновки. Захист конфіденційної інформації в системах електронного документообігу є надважливим завданням для організацій, які працюють з чутливими даними. З розвитком цифрових технологій, цифровізації та зростанням кіберзагроз необхідно впроваджувати комплексні заходи безпеки, що включають колійний захист, багаторівневу автентифікацію, контроль доступу та регулярний моніторинг системи. Ефективне управління інформаційною безпекою передбачає не лише використання сучасних технічних рішень, а й підвищення рівня кіберграмотності співробітників, дотримання нормативних вимог і постійне вдосконалення політики безпеки. Лише комплексний підхід дозволить мінімізувати ризики витоку даних та забезпечити надійний захист інформації в умовах сучасного цифрового середовища.

1. Забезпечення конфіденційності електронних документів. Електронний підпис. URL: https://surl.li/svyqkl (дата звернення: 26.02.2025). **2.** Захист систем електронного документообігу: юридичні й технічні моменти. URL: https://surl.li/pnkmmo (дата звернення: 26.02.2025). **3.** Основні методи захисту конфіденційної інформації. URL: https://surl.li/pqabmn (дата звернення: 26.02.2025). **4.** Про захист інформації в інформаційно-комунікаційних системах : Закон України. URL: https://surl.li/lywjwa (дата звернення: 26.02.2025).

REFERENCES:

1. Zabezpechennia konfidentsiinosti elektronnykh dokumentiv. Elektronnyi pidpys. URL: https://surl.li/svyqkl (data zvernennia: 26.02.2025). **2.** Zakhyst system elektronnoho dokumentoobihu: yurydychni y tekhnichni momenty. URL: https://surl.li/pnkmmo (data zvernennia: 26.02.2025). **3.** Osnovni metody zakhystu konfidentsiinoi informatsii. URL: https://surl.li/pqabmn (data zvernennia: 26.02.2025). **4.** Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh : Zakon Ukrainy. URL: https://surl.li/lywjwa (data zvernennia: 26.02.2025).

Malanchuk L. O. [1; ORCID ID: 0000-0002-6341-5639],
Candidate of Economics (Ph.D.), AssociateProfessor,
Mordas O. M. [1; ORCID ID: 0009-0005-1597-3520],
Senior Student

[1]*National University of Water and Environmental Engineering, Rivne*

PROTECTION OF CONFIDENTIAL INFORMATION IN ELECTRONIC DOCUMENT CIRCULATION SYSTEMS

This article explores the protection of confidential information within electronic document management (EDM) systems. In the modern digital landscape, safeguarding sensitive data is an essential component of organizational cybersecurity. The research examines various approaches to protecting confidential information, including analysis of key methods, tools, and technologies applied in the EDM environment. The study covers modern challenges of information security and evaluates strategies used to ensure data confidentiality, integrity, and accessibility.

Special attention is given to cybersecurity issues, risk mitigation techniques, and mechanisms of secure data exchange. The article compares different security systems, assessing their strengths and weaknesses when applied to electronic document circulation. Encryption, user authentication, access control systems, secure communication protocols, and data masking are considered as part of a comprehensive approach to information protection.

The article also addresses how confidential data should be handled within the framework of digital workflows, ensuring compliance with data protection standards and regulations. Key emphasis is placed on the layered model of security, which combines multiple defense techniques to reduce the risk of data breaches and unauthorized access.

As a result of the conducted analysis, the study identifies the most effective and practical methods and tools for protecting confidential information in EDM systems. The findings can serve as guidance for IT specialists, administrators, and organizations aiming to enhance the security of their document management infrastructure and reduce vulnerability to cyber threats.

Keywords: confidential information; information; electronic document management; cybersecurity; protection system; protection; software.

Отримано: 27 лютого 2025 року
Прорецензовано: 03 березня 2025 року
Прийнято до друку: 28 березня 2025 року