3. IT Guild. Сучасна система документообігу. Можливості, інструменти, потік вартості. URL: https://it-guild.com/info/blog/sovremennaya-workflow-sistema-vozmozhnosti-instrumenty-value-stream/

4. Наконечна О. А. Петрук С. В. Модулювання ефективного документообігу для управління діяльністю органів державної влади. *Вісник Східноєвропейського університету економіки і менеджменту.* 2015. Вип. 2(19). С. 169–181. URL: https://eprints.zu.edu.ua/34053/1/Vsuem_2015_2_20.pdf

5. Social and communication challenges and practical cases of implementation of management information systems in higher education / O. Anisimova, O. Prihunov, H. Lukash, T. Yavorska. *Бібліотекознавство. Документознавство. Інформологія.* 2024. Т. 20. № 3. С. 41–54. DOI: 10.63009/lsrsi/3.2024.41.

6. Золотарьова І. О., Бутова Р. К. Автоматизація документообігу: навч. посіб. Харків: ХНЕУ, 2008. 169 с. URL: https://nemk.com.ua/wp-content/uploads/2024/04/.pdf

7. Дебелий А. В. Інноваційні підходи до вдосконалення системи управління документообігом в органах державного управління. Полтава, 2025. 62 с. URL: https://reposit.nupp.edu.ua/files/original/107/16886/a1d07322987babbdc44296e76f860f2ee78ff797.pdf



УДК 005.92:004.056

Оксана Федотова, д-р іст. наук, ст. наук. співробітник, професор,
Гусейн Турсунов, здобувач вищої освіти
Маріупольський державний університет, м. Київ

СПЕЦИФІКА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЯК ОБ'ЄКТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У дослідженні висвітлено специфіку електронного документообігу (ЕДО) як об'єкта захисту. Наголошено на фізичній нематеріальності цифрових даних. Авторами проаналізовано види існуючих загроз, зокрема несанкціонований доступ (НСД), та визначено необхідність використання криптографічних методів для забезпечення цілісності, конфіденційності та автентичність інформації.

Ключові слова: електронний документообіг, об'єкт захисту, інформаційна безпека, несанкціонований доступ, тріада безпеки, документована інформація.

Цифровий перехід сучасних підприємств до автоматизації діловодства потребує аналізу властивостей цифрового документа та конкретизації інструментів, що можуть засвідчувати його автентичність. Організація ефективно захищеної інформаційної діяльності установи базується на усвідомленні особливостей обігу електронних даних та застосуванні надійних засобів для їх збереженості. Зважаючи на те, що електронний документ напряму зазнає впливу технологічних факторів у процесі передачі відкритими мережами, сутнісний аспект операцій документообігу на сучасному етапі розглядається паралельно з технологічною специфікою

криптографічних перетворень та урахуванням наявної інфраструктури довірчих послуг.

Варто уточнити дефініцію «електронний документообіг». Зазвичай мається на увазі комплекс операцій зі створення, обробки, надсилання, отримання, зберігання, застосування та кінцевого знищення електронних документів, що виконуються із паралельним провадженням перевірки їх цілісності та підтвердження факту надходження й одержання таких документів [1]. Для фахівців галузі документознавства та архівної справи впровадження ЕДО означає концептуальну зміну підходів до збереження інформації, організації інформаційної діяльності та корпоративного управління [2].

Специфіка електронного документообігу як об’єкта інформаційної безпеки полягає у фізичній нематеріальності цифрового документа. На відміну від паперового носія, де інформація жорстко прив’язана до матеріалу (паперу, чорнила), електронний документ – структурований набір двійкових даних. Це породжує низку унікальних загроз, які вимагають специфічних методів захисту. Найбільш критичною з таких загроз є несанкціонований доступ (НСД) – одержання доступу до актуальних інформаційних ресурсів певними користувачами чи процесами без відповідних офіційних повноважень [3]. Захист електронного документообігу традиційно розглядається через забезпечення класичної тріади інформаційної безпеки, яка безпосередньо адаптується під потреби сучасного діловодства:

1. Конфіденційність – гарантія того, що зміст електронного документа (особливо з грифом «Комерційна таємниця» або «Для службового користування») буде доступний лише авторизованим користувачам.

2. Цілісність – забезпечення того, що електронний документ не був випадково або навмисно змінений, доповнений чи частково знищений у процесі його передачі корпоративною мережею або під час зберігання на сервері архіву.

3. Доступність – гарантія того, що легітимний користувач (наприклад, діловод або керівник установи) зможе отримати своєчасний і безперешкодний доступ до необхідного документа в базі даних [4].

Окремим, вкрай важливим атрибутом для систем ЕДО, є автентичність – здатність довести, що автором документа є саме та особа, яка під ним підписалася, і що документ дійсно був створений у зазначений час. Без гарантування цих властивостей електронний документообіг втрачає будь-яку юридичну силу та перетворюється на вразливу мішень для зловмисників [5].

Головною вимогою щодо захисту інформації відкритого типу є збереження її цілісного стану, що досягається за допомогою організації захисту даних від несанкціонованих дій, які здатні спричинити їх випадкове чи навмисне спотворення, модифікацію або знищення.

Дотримання встановленого режиму доступу до інформації передбачає забезпечення безперешкодного ознайомлення користувачів із відкритими даними та надання права на їх зміну або знищення виключно уповноваженим особам. Водночас доступ до конфіденційної та таємної інформації має надаватися лише користувачам із відповідними повноваженнями, причому обсяг дозволених операцій з такими даними повинен чітко визначатися відповідно до їхніх функціональних обов'язків. Несанкціоновані спроби доступу, модифікації або знищення інформації мають своєчасно виявлятися та блокуватися, а права доступу користувачів – обмежуватися або скасовуватися за необхідності.

Характерними різновидами несанкціонованих дій під час інформаційної роботи на підприємстві є:

1) ознайомлення з конфіденційними даними різноманітними способами, але без порушень їх структури та цілісності;

2) зміна інформації з незаконною метою або як часткова, так і загальна модифікація її складу;

3) цілеспрямоване знищення даних для завдання матеріальних збитків.

Наслідком неправомірних операцій з інформацією стає порушення її конфіденційності, повноти, достовірності та доступності, що спотворює режим управління даними і знижує його якість [6].

Забезпечення ефективного збереження інформації передбачає впровадження комплексу інструментів. Для ефективного захисту документованої інформації необхідно застосовувати комплексний підхід, що об'єднує програмно-апаратні засоби, організаційні заходи та спеціальні математичні методи перетворення даних, які повністю виключають можливість їх прочитання сторонніми користувачами [7]. Зокрема криптографічні методи захисту та загальна технологія шифрування є найбільш надійним способом протидії несанкціонованому доступу та перехопленню даних [6, с. 44]. Криптографічний захист перетворює інформацію електронного документа на незрозумілий шифротекст, роблячи його марним для зловмисника, який не володіє правильним ключем дешифрування.

Отже, специфіка електронного документообігу як об'єкта захисту полягає у фізичній нематеріальності цифрового документа, який становить собою структурований набір двійкових даних. Організація захищеної інформаційної діяльності установ потребує одночасного забезпечення конфіденційності, цілісності та доступності відомостей, а також перевірки їх автентичності за допомогою криптографічних перетворень та інфраструктури довірчих послуг, без чого цифрові масиви втрачають юридичну силу.

Список використаних джерел

1. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. *Рада: офіційний вебпортал парламенту України.* 2003. № 36. Ст. 276. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
2. Бездрабко В. В. Документознавство в Україні: історія, сучасний стан і перспективи розвитку: монографія. Київ: Четверта хвиля, 2020. 284 с.
3. НД ТЗІ 1.1-003-99. Термінологія у сфері технічного захисту інформації. Основні положення / Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. Київ, 1999. 28 с.
4. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посіб. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. 128 с.
5. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посіб. Запоріжжя: НУ «Запорізька політехніка», 2020. 192 с.
6. Методи та засоби захисту інформації / А. Н. Аль-Амморі, М. М. Дехтяр, Р. М. Іщенко, А. Є. Клочан. *Сучасні інформаційні системи.* 2024. Т. 8. № 1. С. 44–48.
7. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

УДК 002.6:659.4(477)

Олена Шевченко, д-р наук із соц. комунікацій, професор
Національний університет «Одеська політехніка», м. Одеса

ІНФОРМАЦІЙНІ УСТАНОВИ УКРАЇНИ ТА ЇХ ПРЕЗЕНТАЦІЙНИЙ СТИЛЬ

Анотація. Досліджено особливості інформаційних установ, їх інформаційно-комунікаційну діяльність, процес формування брендингу, айдентики та документаційного стилю.

Ключові слова: інформаційні установи, брендинг, айдентика, документообіг, брендбук, цифрові платформи.

Актуальність теми дослідження обумовлена тим, що інформація в сучасному суспільстві є ключовим ресурсом, а інформаційні установи забезпечують створення, обробку, зберігання, поширення інформації та взаємодію між інформаційними ресурсами і користувачами. У період цифровізації важливим стає не лише надання інформаційних послуг, а й презентаційний стиль: через вебресурси, соціальні мережі та документообіг формується впізнаваність, довіра й цілісний образ установи. Єдиний візуальний та документаційний стиль підтримує професійну комунікацію з аудиторією та підвищує довіру до інформаційних продуктів і послуг. Брендинг та айдентика сьогодні є важливими не лише для комерційних компаній, а й для бібліотек, архівів, інформаційних центрів, цифрових платформ та інших установ, діяльність яких пов’язана з інформацією.