

СЕКЦІЯ 1

ДОКУМЕНТ В ІНФОРМАЦІЙНОМУ ПРОСТОРИ ХХІ СТ.

УДК: 004.056.5:004.91:005.92](043.2)

Буга Анастасія Анатоліївна
(*наук. керівник – канд. наук з соц. ком., доцент Василенко В. Ю.*)
Донецький національний університет імені Василя Стуса, м. Вінниця

КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЇ В СЕРЕДОВИЩІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Анотація. У роботі розглянуто поняття доступності інформації в різних сферах, її основні компоненти, технічні, організаційні та правові аспекти забезпечення доступу до електронних документів. Наведено низку методів визначення рівня публічності інформації та розглянуто алгоритм розподілу прав доступу за допомогою класифікації документів. Результати дослідження можуть бути використані під час розробки систем електронного документообігу.

Ключові слова: доступ до інформації, розподіл прав доступу, електронний документ, класифікація.

В епоху цифровізації документування, від особистих файлів до документних баз даних підприємств, одним з найбільш нагальних та менш очевидних аспектів зберігання електронних документів є доступність до них. Неправильно наданий доступ може як завадити цільовій аудиторії, так і допустити зловмисників до чутливої інформації [1].

Термін «доступність інформації» має декілька визначень, залежно від контексту, в якому він використовується.

У контексті інформаційної безпеки доступність тісно пов'язана з конфіденційністю та цілісністю [2]. Разом ці три показники описують властивості отримання користувачем інформації (рис. 1).

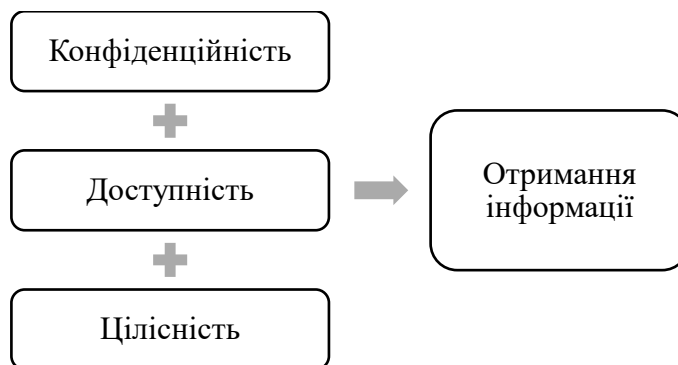


Рисунок 1 – Зв'язок властивостей отримання інформації

Доступність – властивість інформації, що визначається її досяжністю та можливістю використання на вимогу уповноваженою особою. Доступність можна вважати ідеальною, коли після авторизації користувач може безперешкодно знайти потрібну інформацію.

Конфіденційність – властивість інформації, що визначається її недоступністю для неавторизованих осіб, організацій або процесів.

Цілісність – властивість інформації, що визначається неможливістю змінити, знищити або втратити її в несанкціонований спосіб [3].

На відміну від технічної термінології, законодавчі акти не мають єдиного визначення доступу до інформації. В законах, що регламентують права громадян та державних установ, це поняття використане без роз'яснення значення або замінене на синонімічну конструкцію, наприклад: «отримання можливості обробляти інформацію», «порядок одержання, використання, поширення і зберігання інформації», «надання дозволу на ознайомлення з інформацією». Тому із законодавчого погляду, «доступ до інформації» можна ототожнити з терміном «отримання інформації» і вважати правом, яке може мати конкретна людина, група людей чи організація [4].

Отже, якщо виділити загальне визначення, то доступність – це ступінь досяжності інформації для користувача залежно від його прав та повноважень.

Для присвоєння рівня доступу до документа можна визначати конфіденційність інформації в ньому вручну або ж присвоїти рівень доступу групі, де документи об'єднані за спільними ознаками – класифіковані. Під час створення єдиної закономірної системи збереження документів наступним кроком після класифікації документів за категоріями є присвоєння цим категоріям шаблону назви і, в підсумку, визначення рівня конфіденційності (рис. 2) [5].



Рисунок 2 – Етапи організації документів

1 етап. Головні вимоги під час розробки категорій – узгодженість, відмінність та вичерпність. Їх можна виділяти за темами документів, кольорами зображень або будь-яким іншим набором перелічених значень, що описують зміст, проте класичними підходами до класифікації є поділ за змістом, характеристиками чи призначенням.

Класифікація за змістом передбачає визначення категорій документів на основі вмісту документів або файлів. За цієї класифікації досліджується видимий текст, зокрема на наявність ключових слів, щоб визначити тему чи предмет документа.

Коли документи класифікують за характеристиками, враховують зовнішні фактори: формат, метадані або інші атрибути, що оточують створення документа, але безпосередньо не відображаються в ньому.

Визначення призначення допоможе, коли в одній системі працюють користувачі з різними інформаційними потребами [6].

2 етап. У системі, що обслуговує велику кількість документів, випадкові назви можуть перешкоджати ефективній роботі, для чого варто визначити шаб-

лон побудови імен файлів. Головною метою визначення такого шаблону є спрощення орієнтації в файлах та їх пошуку як для досвідченого так і для нового користувача. Найбільш популярними та інформативними елементами назви можна назвати тему (опис вмісту), джерело (проект чи підрозділ, з яким пов'язаний документ), дату (дата створення чи період, який описується в документі) та стан (статус розробки).

Назва документа повинна бути максимально лаконічною, але водночас відображати достатньо інформації, щоб відрізнити однотипні файли між собою. Тому якщо названі вище елементи не є достатньо вичерпними для унікального імені, також можуть включатись додаткові елементи, як-от номери версій, порядкові номери, імена чи назви фірм, що є авторами чи об'єктами документа тощо [7].

3 етап. Залежно від чутливості інформації та кола користувачів, що мають право на ознайомлення з цією інформацією, рівні доступу поділяють на 4 основні типи: публічні, внутрішні, конфіденційні, закриті (табл. 1).

Таблиця 1 – Основні рівні конфіденційності інформації

Тип доступу	Користувачі	Опис
Публічний	Усі	Розголошення не несе загрози, у деяких випадках оприлюднення вимагається законом
Внутрішній	Члени організації	Переважно доцільна лише в контексті внутрішніх процесів організації, розголошення не є грубим порушенням
Конфіденційний	Окремі відділи	Інформація про клієнтів, співробітників, окремі проекти тощо, обмежено поширюється всередині підприємства
Закритий	Окремі відділи / вповноважені користувачі	Лише для вузького кола осіб, часто стосується безпеки чи фінансів, розголошення заборонене

Джерело: [8]

Ці чотири рівні можуть присвоюватись документам на основі характеристик, як-от контент, контекст та користувач. Визначення на основі контенту передбачає аналіз інформації всередині документа та визначення рівня її конфіденційності, тобто аналізується зміст, як під час визначення класифікації. Під час аналізу контексту доступ призначається за метаданими, отже, за зовнішніми характеристиками документа. Встановлення рівня доступу за користувачем означає визначення повноважень та інформаційних потреб особи, яка переглядатиме документ, яка перекликається з класифікацією за призначенням [6].

Висновки

1. Паралельність критеріїв для створення класифікації та розподілу прав доступу означає, що класифікатор, розроблений для структурного розподілу документів, може використовуватись в обох випадках.

2. Коректно розроблена класифікація документів є багатофункціональною та може стати фундаментом для правильного присвоєння доступу.

Список використаних джерел

1. Анісімова О., Кулибаба Ю. Цифровізація у формуванні корпоративної культури. *Інформація та соціум*. Вінниця: ДонНУ імені Василя Стуса, 2025. С. 108–111.

2. Martin A. P., Khazanchi D. Information Availability and Security Policy. *Proceedings of the Twelfth Americas Conference on Information Systems*, (Acapulco, 4–6 August 2006). 2006. P. 1257–1268.

3. Information Security Glossary of Terms. 3rd ed. Washington: CCSDS Secretariat, 2024. 35 p.

4. Марущак А. Визначення поняття «доступ до інформації». *Правова інформатика*. 2006. № 3(11). С. 69–74.

5. Chakraborty S. Document Classification: Insights from Teams Who've Done It. *Docsumo*. URL: <https://www.docsumo.com/blog/what-is-document-classification> (дата звернення: 01.04.2026).

6. 3 Types of Data Classification: Understanding the Fundamental Categories. *Deasy Labs*. URL: <https://www.deasylabs.com/post/3-types-of-data-classification-understanding-the-fundamental-categories> (дата звернення: 31.03.2026).

7. Creating and Maintaining File Naming Standards. *Queen's University*. URL: <https://www.queensu.ca/accessandprivacy/guidance/file-naming-standards> (дата звернення: 01.04.2026).

8. What are the Four Levels of Data Classification? *Cyera*. URL: <https://www.cyera.com/blog/four-levels-of-data-classification> (дата звернення: 31.03.2026).



УДК 005.92:004.63]:331.108

Гориславець Аліна Дмитрівна
(наук. керівник – канд. філол. наук, доцент Дерев'янюк Л. І.)
Національний університет «Полтавська політехніка
імені Юрія Кондратюка», м. Полтава

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В КАДРОВОМУ ДІЛОВОДСТВІ

Анотація. Розглянуто впровадження систем електронного документообігу в кадровому діловодстві; описано їх основні функції: створення, облік, зберігання, узгодження, підписання, обмін документами й контроль виконання. Обґрунтовано переваги СЕД, зокрема автоматизацію процесів, підвищення ефективності, безпеки та прозорості управління персоналом.

Ключові слова: системи електронного документообігу, кадрове діловодство, автоматизація процесів, електронні документи, інформаційна безпека, цифровізація управління персоналом.

У сучасних умовах цифровізації особливого значення набуває впровадження систем електронного документообігу (СЕД), зокрема у сфері кадрового діловодства. Використання СЕД дає змогу оптимізувати роботу з документами, підвищити швидкість оброблення інформації та забезпечити її надійне зберігання.

Кадрове діловодство охоплює широкий спектр процесів, пов'язаних з оформленням, обліком і зберіганням документів працівників. Тому СЕД мають виконувати низку ключових функцій. Однією з базових функцій є створення, реєстрація та зберігання документів, що має ключове значення для кадрового діловодства. СЕД дають змогу автоматизувати формування кадрових документів, зокрема наказів про прийняття на роботу, звільнення, переведення, заяв працівників, трудових договорів та інших документів, пов'язаних з управлінням персоналом.