професора О. В.Марцеляка, доктора юридичних наук, професора А. Берлінгуера. Київ: Вид-во «ОСНОВА», 2020. — 672 с.

6. Лобунець В. І. Зарубіжний досвід формування моделей місцевого самоврядування. Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб´єктів господарювання в умовах трансформації публічного управління: Матеріали Міжнародної науково-практичної конференції. — Одеса: Одеський національний політехнічний університет, 2018. — с. 94-95.

7. Сучасні управлінські та соціально-економічні аспекти розвитку держави, регіонів та суб´єктів господарювання в умовах трансформації публічного управління: Матеріали Міжнародної науково-практичної конференції. — Одеса: Національний університет «Одеська політехніка», 2023. — 227 с.

8. Жовнірчик Я. Ф., Мельник В. М. Зарубіжний досвід і вітчизняні традиції здійснення інноваційного розвитку територіальних громад органами місцевого самоврядування. Інвестиції: практика та досвід, № 9, 2015. — с. 92-97.

Антоція: *This research explores the global experience of organizing and functioning of local self-government. Specifically, it examines various models of local self-government, such as continental, Anglo-Saxon, and Iberian, analyzing their characteristics and their impact on the effectiveness of governance at the local level. The study highlights the challenges and prospects of developing this sphere within the context of contemporary global trends.*

Ключові слова: *local self-government, models of local self-government, continental model, Anglo-Saxon model, Iberian model, governance effectiveness, global trends.*

Науковий керівник:
Галунець Н. І.,
старший викладач,
Миколаївський національний аграрний університет

УДК 004.91:651.012:352/354(045)

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ТЕРИТОРІАЛЬНИХ ГРОМАД

Нехайчик Єлизавета Євгенівна,
здобувач вищої освіти спеціальності 281 «Публічне управління та адміністрування»
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація: *роботу присвячено аналізу проблеми забезпечення інформаційної безпеки в контексті електронного документообігу*

територіальних громад. Розглядаються ключові аспекти захисту конфіденційної інформації, зокрема використання криптографічних методів для шифрування даних та застосування кваліфікованого електронного підпису для забезпечення їхньої достовірності.

Ключові слова: *документообіг, інформаційна безпека, територіальна громада, електронний підпис, кіберзагроза.*

Забезпечення інформаційної безпеки електронного документообігу в сучасному світі стає не лише важливою складовою, але й ключовим завданням для успішної діяльності будь-якої територіальної громади. У епоху, коли кіберзагрози стають все більш небезпечними, ефективна система захисту даних та документів стає фундаментальною для збереження довіри та надійності всього бізнесу.

Одним із стратегічних заходів, спрямованих на забезпечення захисту документів, є проведення систематичного резервного копіювання. Правильно налагоджена процедура створення резервних копій і їх зберігання на надійних носіях або у захищених хмарних сервісах може запобігти серйозним наслідкам від катастрофічних ситуацій, таких як кібератаки, стихійні лиха чи технічні аварії.

Сховище в захищеному хмарному середовищі на різних дата-центрах є ще одним важливим елементом у забезпеченні безпеки електронного документообігу. Такі рішення не лише гарантують високу доступність даних, але й забезпечують додатковий рівень захисту через шифрування та мережеві протоколи, що ускладнюють несанкціонований доступ до цінної інформації.

Закритий доступ до системи електронного документообігу відіграє критичну роль у забезпеченні безпеки. Аутентифікація користувачів через багатофакторні методи стає все більш ефективним заходом, оскільки вона забезпечує надійність навіть у випадку компрометації одного з факторів ідентифікації [1].

Одним із важливих аспектів забезпечення інформаційної безпеки є розмежування прав доступу. Цей механізм дозволяє адміністраторам системи електронного документообігу надавати індивідуальні права доступу для кожного користувача або групи користувачів. Такий підхід допомагає забезпечити, що лише авторизовані особи мають доступ до певних документів, тим самим уникнути несанкціонованого доступу та запобігти можливим витокам конфіденційної інформації.

Крім того, важливим елементом є наявність інтегрованих механізмів виявлення інцидентів та моніторингу безпеки. Автоматизоване виявлення підозрілих активностей дозволяє оперативно реагувати на можливі загрози та запобігти їхнім наслідкам, забезпечуючи неперервну роботу системи [2].

До інших технічних заходів забезпечення інформаційної безпеки належить надійне шифрування даних під час їх трансферу та зберігання, а також регулярне оновлення програмного забезпечення та застосунків, використовуваних для електронного документообігу. Ці заходи сприяють

підвищенню рівня захисту та зменшенню ризиків вразливості перед кіберзагрозами.

Окрім технічних аспектів, важливо звертати увагу на навчання персоналу щодо правил безпеки та впізнавання кіберзагроз. Підвищення культури безпеки серед співробітників сприяє зменшенню ризиків, пов'язаних з людським фактором, та робить електронний документообіг більш стійким до потенційних загроз.

Для ефективного захисту конфіденційних даних та забезпечення недоступності їх стороннім особам застосовуються криптографічні методи, зокрема шифрування даних [3].

Шифрування є надійним методом захисту інформації, оскільки воно перетворює дані у незрозумілий для сторонніх вигляд, який може бути розкритий лише за допомогою відповідного ключа. Такий підхід не лише запобігає несанкціонованому доступу до даних, але й забезпечує їх конфіденційність під час транспортування та зберігання.

Для забезпечення достовірності документів у електронному документообігу широко використовується кваліфікований електронний підпис (ЕЦП/КЕП) [4]. Кваліфікований електронний підпис є електронним еквівалентом звичайного підпису, але забезпечує вищу правову силу та автентичність. Він гарантує, що документ не був змінений після підписання та належить конкретному автору. Для створення кваліфікованого електронного підпису використовуються апаратні або програмні засоби, які реалізують криптографічні алгоритми.

Загалом, застосування криптографічних методів шифрування та кваліфікованого електронного підпису є невід'ємною складовою для забезпечення інформаційної безпеки електронного документообігу територіальних громад. Ці методи дозволяють зберігати конфіденційність та достовірність даних, забезпечуючи надійний обмін інформацією та дотримання вимог законодавства.

Аутентифікація, як процес визначення особи користувача та підтвердження її легітимності, вимагає вдосконалення та застосування надійних методів для забезпечення безпеки та захисту конфіденційної інформації [5].

Хоча парольна аутентифікація є найпоширенішим методом, вона має свої обмеження і ризики, зокрема пов'язані з можливістю вгадування або зламу простих паролів, а також людським фактором у зберіганні паролів. Майнові методи, які використовують спеціальні носії інформації, такі як USB-ключі чи смарт-карти, надають певний рівень безпеки, але можуть вимагати додаткових витрат на інфраструктуру.

Отже, комплексний підхід до забезпечення інформаційної безпеки електронного документообігу, який включає регулярне резервне копіювання, використання захищених хмарних сервісів та ретельну аутентифікацію користувачів, є критичним для успішної та безпечної діяльності будь-якої сучасної організації.

Список використаних джерел:

1. Леоненко Н. А., Поступна О. В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration*. 2022. Issue 2(17)2022. URL: https://doi.org/10.52363/2414-5866-2022-2-14 (дата звернення: 20.02.2024).
2. Новікова О., Азьмук Н. Інформаційна безпека в соціально-трудовій сфері: виклики цифровізації економіки. *Економіка та суспільство*. 2021. № 30. URL: https://doi.org/10.32782/2524-0072/2021-30-30 (дата звернення: 20.02.2024).
3. Субіна Т. В. Інформаційна безпека як один з видів національної безпеки України. Ірпінський юридичний часопис. 2021. № 3. С. 103–113. URL: https://doi.org/10.33244/2617-4154.3.2020.103-113 (дата звернення: 20.02.2024).
4. Шопіна І. М. Інформаційна безпека цифрової трансформації. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2023. № 1. С. 28–35. URL: https://doi.org/10.32782/2311-8040/2023-1-4 (дата звернення: 20.02.2024).
5. Шульженко Н. Інформаційна безпека суспільства від загроз організованої злочинності. Наукові перспективи (Naukovì perspektivi). 2023. № 12(30). URL: https://doi.org/10.52058/2708-7530-2022-12(30)-367-373 (дата звернення: 20.02.2024).

Анотація: *the paper analyses the problem of information security in the context of electronic document management of territorial communities. The key aspects of confidential information protection are considered, in particular, the use of cryptographic methods for data encryption and the use of a qualified electronic signature to ensure their authenticity.*

Ключові слова: *document flow, information security, territorial community, electronic signature, cyber threat.*

Науковий керівник:
Галунець Н. І.
старший викладач
кафедри публічного управління та адміністрування
і міжнародної економіки,
Миколаївський національний аграрний університет

УДК 352.07

ЗАРУБІЖНИЙ ДОСВІД УПРАВЛІННЯ КАДРОВИМ ПОТЕНЦІАЛОМ В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ

Макадзьоба Валерія Євгеніївна
здобувач вищої освіти спеціальності 281 Публічне управління та адміністрування
Миколаївський національний аграрний університет
м. Миколаїв, Україна

Анотація : *Досліджено особливості управління кадрового потенціалу у таких країнах, як: США, Франція та Німеччина. Визначено, що кожна країна має свої*