МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.І. ВЕРНАДСЬКОГО
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

На правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА НА ЗДОБУТТЯ СТУПЕНЯ ВИЩОЇ ОСВІТИ «МАГІСТР»

ЕЛЕКТРОННЕ АРХІВУВАННЯ ДІЛОВОЇ ДОКУМЕНТАЦІЇ В УСТАНОВАХ ТА ОРГАНІЗАЦІЯХ

Здобувача вищої освіти
Щуки Євгенія Вікторовича
спеціальності «Інформаційна, бібліотечна та архівна справа»
Навчально-наукового інституту муніципального управління та міського господарства

_____
(підпис)

Науковий керівник:
к.держ.упр., професор Гуйда
Олександр Григорович

_____
(підпис)

Національна шкала добре
Кількість балів 80
Оцінка: ECTS B

Київ – 2025

АНОТАЦІЯ

Щука Євгеній Вікторович. Електронне архівування ділової документації в установах та організаціях.

У роботі розглядається електронне архівування ділової документації в установах та організаціях. Під час написання роботи було розглянуто нормативно-правове забезпечення функціонування електронної ділової документації; проаналізовано особливості електронного архівування ділової документації на прикладі приватного підприємства «ВК НАФТОГАЗПРОМБУД»; виявлено шляхи оптимізації процесу електронного архівування ділової документації на прикладі приватного підприємства «ВК НАФТОГАЗПРОМБУД».

Ключові слова: електронне архівування, ділова документація, документообіг, критична інфраструктура, персональні дані, інформаційна безпека.

SUMMARY

Shchuka Yevhenii. Electronic archiving of business documentation in institutions and organizations.

The paper considers electronic archiving of business documentation in institutions and organizations. During the writing of the paper, the regulatory and legal support for the functioning of electronic business documentation was considered; the features of electronic archiving of business documentation were analyzed using the example of the private enterprise "VK NAFTOGAZPROMBUD"; ways to optimize the process of electronic archiving of business documentation were identified using the example of the private enterprise "VK NAFTOGAZPROMBUD".

Key words: electronic archiving, business documentation, document flow, critical infrastructure, personal data, information security.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку інформаційного суспільства характеризується тотальною цифровізацією управлінських процесів, що зумовлює необхідність переходу від традиційного паперового діловодства до електронного. Саме тому питання електронного архівування ділової документації набуває особливої актуальності. Проблема збереження, захисту й забезпечення автентичності цифрових документів стоїть сьогодні перед усіма державними та приватними установами. У світі, де інформація стає ключовим ресурсом, ефективне управління нею неможливе без надійних систем архівування. В умовах війни та нестабільності інформаційного простору України питання електронного архівування набуває ще більшої значущості, адже від належної організації збереження даних залежить безперервність управлінських процесів і безпека державних інформаційних ресурсів [5].

Проблематика електронного архівування активно розробляється у працях таких вітчизняних дослідників, а саме: В. Акуленко [2], О. Кукаріна [36], І. Кучеренко [37], О. Орлова [43], Ю. Палехи [44], О. Смірнова [58] та багатьох інших. Науковці та вчені досліджують питання правового регулювання електронного документообігу, використання штучного інтелекту у модулі е-програм документообігу на підприємствах, стандартизації процесів зберігання цифрових даних, проблеми автентичності та довготривалого доступу до електронних документів. Однак у науковій літературі ще недостатньо розкрито практичні аспекти впровадження систем електронного архівування у вітчизняних організаціях, особливо в умовах воєнного стану та загроз кібербезпеці [60]. Недостатньо вивчено питання інтеграції національних архівних систем з європейськими стандартами, а також проблеми взаємодії між нормативно-правовим і технічним забезпеченням електронного архівування.

Теоретична значущість теми полягає у розкритті закономірностей формування електронного архіву як соціально-правового феномена, що поєднує правові, організаційні та інформаційно-технологічні аспекти. Практична значущість визначається можливістю застосування результатів дослідження для удосконалення архівної політики установ, створення ефективних систем збереження цифрових документів, підвищення рівня їх захисту та оптимізації діловодних процесів.

Стан вивченості проблеми в Україні свідчить про наявність законодавчої бази (Закони України «Про електронні документи та електронний документообіг» [17], «Про електронну ідентифікацію та електронні довірчі послуги» [18], «Про захист інформації в інформаційно-телекомунікаційних системах», [22] накази Державної архівної служби, ДСТУ 4163:2020 [9] тощо), проте реальні механізми електронного архівування ще потребують вдосконалення. На відміну від країн ЄС, де діє єдиний регламент eIDAS, в Україні спостерігається фрагментарність нормативної бази й нерівномірність упровадження сучасних архівних технологій [53]. Саме тому дослідження організації електронного архівування на конкретному підприємстві є важливим кроком до практичної реалізації державної політики цифровізації.

Міжнародний досвід (ISO 14721 OAIS, ISO 15489, MoReq, ISO 30301 [67-69]) засвідчує високий рівень стандартизації процесів збереження електронних документів і підтверджує, що довготривале архівування є складовою інформаційної безпеки держави. У цьому контексті вивчення та адаптація таких стандартів до українських реалій має стратегічне значення для формування надійної архівної інфраструктури. Перспективи розвитку теми полягають у створенні інтегрованих систем електронного архівування, здатних забезпечити взаємодію між державними реєстрами, приватними підприємствами та архівними установами; у розробленні механізмів резервного копіювання й захисту даних від кібератак; у формуванні єдиних стандартів метаданих та форматів збереження. Вивчення питання сприятиме підвищенню рівня інформаційної культури працівників, оптимізації

управлінських процесів і підвищенню ефективності діяльності установ у цифровому середовищі.

Отже, актуальність теми «Електронне архівування ділової документації в установах та організаціях» зумовлюється зростаючими вимогами до інформаційної безпеки, потребою у стандартизації процесів збереження цифрових даних, інтеграцією України у європейський інформаційний простір і необхідністю забезпечення безперервності управління в умовах кризових викликів. Дослідження цієї проблематики має як науково-теоретичну, так і практичну цінність, оскільки дозволяє сформувати цілісну систему знань про сучасні тенденції розвитку архівної справи в епоху цифровізації та визначити шляхи її подальшого вдосконалення.

Мета роботи — дослідити та подати шляхи удосконалення електронного архівування ділової документації в установах та організаціях на прикладі ПП «Нафтогазпромбуд».

Завдання роботи відповідають меті і полягають у вирішення таких задач:

- проаналізувати правові засади ведення електронного документообігу в Україні та міжнародний досвід нормативно-правового регулювання електронного архівування;

- охарактеризувати систему діловодства та документообігу ПП «ВК Нафтогазпромбуд»;

- охарактеризувати організацію процесу електронного архівування документів на Підприємстві;

- з'ясувати можливості удосконалення системи забезпечення захисту персональних даних та інформаційної безпеки електронного архіву підприємства;

- подати перспективи розвитку електронного архівування в Україні: сучасні технологічні рішення та рекомендації для підприємства.

Об'єкт дослідження — нормативно-правова база та система електронного архівуван*ня* ділової документації в установах та організаціях.

Предмет дослідження — електронне архівування ділової документації на прикладі ПП «Нафтогазпромбуд».

Наукова новизна отриманих результатів полягає у комплексному підході до аналізу процесів електронного архівування ділової документації, що поєднує правовий, організаційний і технологічний аспекти з урахуванням сучасних вимог кібербезпеки. Вперше на основі порівняльно-правового, системного та аналітичного методів узагальнено український і міжнародний досвід правового регулювання електронного архівування та визначено напрями його адаптації до національної практики. Крім того, шляхом використання методів моделювання та експертного аналізу розроблено рекомендації щодо удосконалення системи електронного архівування на прикладі конкретного підприємства, що має практичне значення для підвищення ефективності управлінських процесів.

Практичне значення отриманих результатів – результати магістерської роботи можуть бути використані при укладанні теоретичних та практичних курсів для спеціальності 029 «Інформаційна, бібліотечна та архівна справа», а також безпосередньо запропоновані у роботі ПП «Нафтогазпромбуд».

Структура роботи: робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ І. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОЇ ДІЛОВОЇ ДОКУМЕНТАЦІЇ

1.1. Правові засади ведення електронного документообігу в Україні

Електронний документообіг є невід'ємною складовою сучасного управління, що забезпечує оперативність, прозорість і збереження інформаційних ресурсів установи. Його правові засади визначають порядок створення, оброблення, передавання, зберігання та використання електронних документів у різних сферах діяльності. Формування законодавчого підґрунтя для електронного документообігу в Україні є результатом тривалого процесу розвитку інформаційного суспільства, який розпочався ще наприкінці 1990-х років. Поступова цифровізація управлінських процесів зумовила потребу у впровадженні нових правових норм, що забезпечували б легітимність електронних документів та їхню юридичну силу [5].

Першим кроком у цьому напрямі стало ухвалення у 2003 році Закону України «Про електронні документи та електронний документообіг», який заклав основи правового регулювання у сфері цифрових комунікацій [17]. Саме цей закон визначив поняття електронного документа як інформації, зафіксованої у формі електронних даних, що має обов'язкові реквізити та може бути використана як доказ у правовідносинах. Наявність електронного підпису, який прирівнюється до власноручного, забезпечила можливість офіційного обігу документів у цифровому форматі між юридичними та фізичними особами [17].

Паралельно з цим було прийнято Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (2017 р.), який гармонізував українське законодавство із нормами Європейського Союзу [18]. Маємо доповнити, що 1 січня 2025 року було оприлюднено Постанову Верховної Ради України «Про прийняття за основу проєкту Закону України про внесення змін до Закону України "Про електронну ідентифікацію та електронні довірчі

послуги" щодо удосконалення окремих положень та забезпечення безперебійності надання електронних довірчих послуг» [46]. У цілому, цей документ закріпив поняття кваліфікованого електронного підпису, печатки, а також створив правові механізми захисту електронних даних. Його поява ознаменувала новий етап розвитку цифрової держави та створення передумов для повноцінного функціонування електронного документообігу в публічному і приватному секторах.

Із розвитком інформаційно-комунікаційних технологій українська держава послідовно розширювала правову базу електронного врядування. Зокрема, стратегічні документи — такі як Концепція розвитку цифрової економіки та суспільства України (2018–2020 рр.), Державна стратегія цифрової трансформації та Програма розвитку електронного урядування — визначили необхідність переведення більшості адміністративних процесів у цифровий формат [56]. У цьому контексті електронний документообіг розглядається не лише як технічне рішення, а й як правовий інструмент забезпечення прозорості управління, зменшення бюрократичних бар'єрів та підвищення ефективності діловодства. Важливо, що правові засади електронного документообігу охоплюють не лише питання технічної реалізації, а й регламентують інформаційну безпеку, автентичність, цілісність та збереження документів [56].

Нормативно-правові акти встановлюють вимоги до формату, структури, реквізитів і метаданих електронних документів, що забезпечує їхню юридичну значимість. Особливу увагу приділено процедурі архівування електронних документів, оскільки збереження цифрових даних вимагає спеціальних технічних і правових гарантій. Становлення електронного документообігу в Україні супроводжувалося активним упровадженням електронного урядування. З 2019 року завдяки створенню платформи «Дія» було започатковано перехід до цифрової держави, де взаємодія між громадянами, бізнесом і владою грунтується на електронних сервісах [5]. У цьому процесі питання правового регулювання набуло особливої ваги, адже кожен

електронний документ має відповідати принципам достовірності, конфіденційності та збереженості.

Окреме місце у правовому забезпеченні займають підзаконні акти, зокрема постанови Кабінету Міністрів України, накази Міністерства юстиції та Державної архівної служби, що деталізують порядок створення, обліку та зберігання електронних документів в органах державної влади [48]. Вони визначають вимоги до систем електронного документообігу, правила ідентифікації користувачів, стандарти метаданих і формати обміну. Саме узгодженість нормативних положень на різних рівнях забезпечує функціональну стабільність усієї системи електронного діловодства. Сучасна практика доводить, що правові засади електронного документообігу тісно пов'язані із питаннями цифрової безпеки та кіберзахисту. Українське законодавство передбачає створення державних систем захисту інформації, сертифікацію засобів криптографічного захисту, а також контроль за обігом персональних даних. Усі ці елементи утворюють комплексну правову рамку, в межах якої здійснюється обмін електронними документами [55].

Розвиток правових засад у цій сфері відбувається динамічно. Постійне вдосконалення нормативної бази відповідає як внутрішнім потребам суспільства, так і вимогам міжнародної інтеграції України. Впровадження європейських стандартів, зокрема Регламенту eIDAS, сприяє зміцненню довіри до електронних документів, а також розширює можливості для участі українських установ у міжнародних інформаційних обмінах [51].

Таким чином, правові засади ведення електронного документообігу в Україні сформувалися як результат взаємодії державної політики, технологічного прогресу та потреб управлінської практики. Їхня еволюція демонструє прагнення держави до створення цілісного правового поля, у якому електронний документ має повну юридичну силу, а система його обігу — надійну організаційну та технічну основу. Це закладає підґрунтя для подальшого розвитку електронного архівування, що забезпечує довготривале

збереження цифрових даних і безперервність управлінських процесів у сучасних умовах.

Побудова правових засад електронного документообігу в Україні відбувалася у кілька етапів, кожен з яких супроводжувався прийняттям ключових нормативно-правових актів, що визначили напрями розвитку державної інформаційної політики. Основним документом, як ми наголошували вище, що став відправною точкою у цій сфері, є Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV. Саме він заклав фундаментальні положення щодо створення, обігу, зберігання та юридичної сили електронних документів [17]. Закон визначив, що «електронний документ є документом, інформація в якому зафіксована у формі електронних даних, включаючи обов'язкові реквізити, та може бути використаний у правовідносинах нарівні з паперовими аналогами» [17].

У цьому Законі вперше було законодавчо закріплено поняття електронного підпису, який надає електронному документу юридичної сили, еквівалентної власноручному підпису. Він визначає порядок використання електронного підпису, умови його перевірки та юридичну відповідальність за недотримання правил автентифікації. Особливо важливим є те, що закон встановив принцип рівності електронних і паперових документів, що дало змогу започаткувати реальний обіг цифрових документів у правовій та управлінській практиці [17].

Паралельно з основним законом був прийнятий Закон України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV, який деталізував технічні та правові аспекти створення і застосування електронного підпису [47]. Він визначив статус центрів сертифікації ключів, встановив вимоги до формування особистих та відкритих ключів користувачів, а також порядок перевірки достовірності підписів. Цей закон функціонував до листопада 2018 року (документ 852-IV, втратив чинність), коли його норми

були замінені положеннями сучаснішого Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [18].

Саме оновлений Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII гармонізував українське законодавство із європейським регламентом eIDAS (EU Regulation No 910/2014). Закон ввів нові поняття — кваліфікований електронний підпис, електронна печатка, електронна позначка часу, визначив правовий статус довірчих послуг, таких як зберігання ключів та автентифікація електронних документів. У межах цього закону створено Центральний засвідчувальний орган, який здійснює контроль за діяльністю постачальників довірчих послуг і гарантує надійність електронного підпису [18].

У розвиток положень зазначених законів Кабінетом Міністрів України ухвалено Постанову № 55 від 17 січня 2018 року «Про реалізацію експериментального проєкту щодо забезпечення можливості використання електронних документів» (зараз: «Деякі питання документування управлінської діяльності»), яка започаткувала практичне використання електронних сервісів у діяльності органів державної влади. Цей документ фактично започаткував процес цифровізації державного діловодства, що пізніше отримав масштабну підтримку в межах ініціативи «Держава у смартфоні» [45].

Подальшим кроком у вдосконаленні правової бази стало прийняття Постанови Кабінету Міністрів України № 1453 від 28 жовтня 2004 року «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади» (втрата чинності від 07.03.2018 і заміна на Постанову №55). Ця постанова врегулювала процедуру використання електронного підпису у внутрішньому та міжвідомчому документообігу. Зокрема, вона встановила вимоги до сертифікації ключів, порядок створення та перевірки підписів, а також визначила перелік обов'язкових заходів для захисту інформації в державних інформаційних системах [45].

Не менш вагомим документом є Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII, який заклав загальні принципи інформаційних відносин у суспільстві. Він визначив, що інформація є об'єктом правового захисту, а держава гарантує вільний доступ до неї за умови дотримання вимог конфіденційності [23]. Закон забезпечив основоположну базу для подальшого формування спеціального законодавства у сфері електронного документообігу. У системі правового регулювання електронного документообігу важливу роль відіграє Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР [22]. Він визначає основні принципи та вимоги до забезпечення безпеки інформації, встановлює порядок сертифікації засобів захисту, а також відповідальність за порушення вимог кібербезпеки. Цей закон тісно пов'язаний із практикою архівування електронних документів, адже гарантує їхню цілісність та автентичність.

Особливої уваги заслуговує Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, який визначає порядок обробки, зберігання та передачі персональної інформації в електронному форматі [20]. Він встановлює обов'язки розпорядників баз даних, права суб'єктів персональних даних, а також відповідальність за порушення правил конфіденційності. Для систем електронного документообігу цей закон має фундаментальне значення, оскільки документи часто містять персональну інформацію співробітників, клієнтів чи контрагентів.

Суттєвий внесок у нормативну розробку цієї сфери зробила Державна архівна служба України, яка ухвалила Наказ № 188 від 11 листопада 2014 року «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» [39]. У цьому документі вперше системно описано порядок роботи з електронними документами, зокрема правила їх реєстрації, обліку, передавання до архіву та зберігання. Особливий

акцент зроблено на необхідності забезпечення збереженості електронних носіїв та створення резервних копій.

Також важливим є Наказ Міністерства юстиції України № 1000/5 від 18 червня 2015 року «Про затвердження Типової інструкції з діловодства в міністерствах, інших центральних органах виконавчої влади, місцевих державних адміністраціях», який деталізує порядок організації електронного документообігу у державних структурах [41]. Цей акт регулює процеси створення електронних документів, їх візування, затвердження, реєстрації та зберігання. Типова інструкція передбачає, що всі документи, створені в електронній формі, повинні зберігатися у форматах, які гарантують їхнє довгострокове відтворення. На рівні державної стратегії важливе значення має вже згадувана нами Концепція розвитку електронного урядування в Україні, схвалена розпорядженням Кабінету Міністрів України № 649-р від 20 вересня 2017 року. Вона визначає електронний документообіг як основний механізм цифрової взаємодії органів влади, бізнесу і громадян. Концепція передбачає створення єдиних стандартів електронного документообігу, інтеграцію державних інформаційних систем та впровадження принципу «єдиного вікна» [41].

Не менш важливим кроком стало ухвалення Стратегії розвитку інформаційного суспільства в Україні, затвердженої розпорядженням Кабінету Міністрів України № 386-р від 15 травня 2013 року [57]. Цей документ визначає електронне урядування як ключовий напрям модернізації публічного управління та встановлює завдання щодо переходу до безпаперового обігу документів у державних установах.

Серед нормативних актів технічного характеру особливе значення має ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів», який визначає структуру реквізитів документів, правила їх оформлення та збереження [9]. Хоча цей стандарт стосується як паперових, так і електронних документів, його дотримання є обов'язковим для забезпечення уніфікації ділової документації.

Окремо варто відзначити роль, що до березня 2021 року відігравав Державний класифікатор управлінської документації (ДК 010-98), який встановлював види документів, що можуть створюватися в електронній формі [6]. Це сприяло впорядкуванню документопотоків і створенню чіткої системи обліку. У березні документ було замінено на НК 010:2021 [52].

Розвиток правових засад електронного документообігу також пов'язаний із діяльністю Міністерства цифрової трансформації України, яке координує реалізацію політики цифровізації. На нормативному рівні міністерство запроваджує підзаконні акти, що регламентують використання електронних сервісів, електронної ідентифікації, а також ведення реєстрів у цифровій формі. Особливу увагу в сучасних умовах приділено нормативному забезпеченню електронної взаємодії між державними реєстрами, що регулюється Постановою Кабінету Міністрів України № 606 від 8 серпня 2016 року «Про затвердження Порядку електронної взаємодії державних електронних інформаційних ресурсів». Цей документ забезпечує можливість автоматизованого обміну даними між державними установами, що значно підвищує ефективність документообігу [48].

У межах судової системи електронний документообіг регулюється Наказом Державної судової адміністрації України № 120 від 14 червня 2018 року «Про впровадження Єдиної судової інформаційно-телекомунікаційної системи», який визначає порядок подання процесуальних документів в електронному форматі. Це стало важливим етапом переходу судової влади до цифрових процесів і підвищення прозорості судочинства. Важливою ланкою є також Постанова Кабінету Міністрів України «Деякі питання електронної ідентифікації та електронних довірчих послуг», яка регламентує порядок обміну офіційними документами в електронній формі. Вона визначає вимоги до технічних протоколів обміну, рівнів доступу, а також обов'язковість застосування електронних підписів [42].

Окремий пласт правового регулювання стосується зберігання електронних документів в архівах. Це питання врегульовано Наказом

Міністерства юстиції України № 1000/5 від 18 червня 2015 року, де зазначено, що електронні документи підлягають обов'язковому резервному копіюванню, а носії інформації повинні відповідати стандартам довгострокового зберігання. Питання стандартизації електронного документообігу активно розвивається завдяки ухваленню Наказу Державної архівної служби України № 202 від 5 грудня 2018 року «Про затвердження методичних рекомендацій щодо впровадження електронного документообігу», який спрямований на практичну реалізацію єдиних вимог у діяльності органів влади та підприємств [38].

Отже, усі перелічені нормативні акти утворюють цілісну систему, у якій чітко окреслено правила створення, обробки, підписання, зберігання та передавання електронних документів. Правове регулювання електронного документообігу в Україні є комплексним і постійно вдосконалюється, адаптуючись до вимог часу та потреб цифрового суспільства. На сьогодні українська правова база забезпечує достатньо високий рівень правової визначеності у сфері електронного документообігу, однак продовжує розвиватися у напрямі гармонізації з європейським законодавством, посилення кіберзахисту та захисту персональних даних. У результаті електронний документообіг став невід'ємним елементом сучасного управління, що має чітку правову основу, технічне забезпечення та організаційні механізми, регламентовані на рівні держави.

1.2. Міжнародний досвід нормативно-правового регулювання електронного архівування

Питання нормативно-правового регулювання електронного архівування в міжнародній практиці набуло особливого значення у другій половині XX століття, коли цифрові технології почали активно впроваджуватися у сферу діловодства та управління. Розвиток інформаційного суспільства спричинив потребу у створенні міжнародних стандартів, що гарантували б юридичну

силу електронних документів, їхню автентичність і довготривале збереження. В умовах глобальної цифровізації архівна справа перестала бути лише національною компетенцією — вона стала предметом міжнародного правового співробітництва та уніфікації підходів [2, с.32].

Перші спроби систематизації вимог до електронних архівів з'явилися у межах діяльності міжнародних організацій, таких як ЮНЕСКО, Міжнародна рада архівів (ICA) та Організація Об'єднаних Націй. Вони ініціювали створення загальних рекомендацій щодо електронного зберігання інформації, а також принципів доступу до неї. Основна увага приділялася питанню автентичності електронного документа, адже саме ця характеристика є ключовою для його архівної цінності та доказового значення [71].

Поступово архівні установи багатьох держав почали розробляти національні політики цифрового архівування, які базувалися на міжнародних стандартах і рекомендаціях. У 1990-х роках у Європі та Північній Америці почали діяти перші нормативні акти, що встановлювали правила електронного зберігання управлінської документації. У цей період з'явилися перші технічні стандарти, спрямовані на забезпечення довготривалого збереження цифрових ресурсів і визначення форматів, придатних для архівування [71].

Міжнародна практика електронного архівування базується на поєднанні правових, організаційних і технологічних підходів. Правова складова визначає вимоги до легітимності документів, порядок їх передачі до архівів, а також критерії відбору документів тривалого зберігання. Організаційний аспект стосується розроблення процедур управління життєвим циклом електронних документів — від моменту створення до архівного зберігання або знищення. Технологічний аспект охоплює стандарти метаданих, форматів файлів, системи контролю доступу та кібербезпеки [71].

У світовій практиці значну роль у формуванні нормативного підґрунтя відіграють міждержавні організації, зокрема Європейський Союз, Організація економічного співробітництва та розвитку, а також Рада Європи. Саме вони виступили ініціаторами розроблення нормативів, що регулюють порядок

зберігання електронних документів та їхню взаємодію в межах транскордонних інформаційних систем. Метою таких документів є забезпечення сумісності архівних рішень, уніфікація стандартів електронних форматів і створення правових гарантій доступу до цифрової спадщини [71].

Питання електронного архівування тісно пов'язане з концепцією електронного урядування, яка набула поширення наприкінці 1990-х років. У межах цієї концепції виникла потреба у правовому врегулюванні збереження офіційних електронних документів, створених у процесі діяльності державних органів. У більшості країн було розроблено спеціальні законодавчі механізми, що регулюють порядок електронного діловодства, автентифікації документів та їх передачі на архівне зберігання. Важливо зазначити, що міжнародне регулювання архівування базується на принципах достовірності, цілісності, доступності та довготривалості. Ці принципи лягли в основу міжнародних стандартів, які визначають вимоги до створення і функціонування електронних архівних систем. Зокрема, на глобальному рівні утвердилися підходи, згідно з якими електронний архів має забезпечувати не лише технічне зберігання файлів, а й відтворення контексту документа, метаданих і доказової бази його походження [72].

Паралельно з архівними нормами розвивалося міжнародне законодавство у сфері електронного підпису та електронної ідентифікації, що безпосередньо вплинуло на легітимність електронних документів. Без правового визнання електронного підпису неможливо гарантувати автентичність документів, які передаються до архівів. Тому більшість міжнародних актів у сфері архівування тісно пов'язані з правовими інструментами, що регулюють електронний документообіг загалом. Сучасний міжнародний досвід демонструє, що ефективне електронне архівування потребує не лише технічних стандартів, а й міждержавної координації. Саме тому створюються спільні програми обміну досвідом, розробляються рекомендації щодо збереження цифрової інформації, а також формуються спільні політики у сфері доступу до електронних архівів. Особливої ваги

набувають питання захисту персональних даних, кібербезпеки та інтелектуальної власності в умовах глобальних інформаційних обмінів [72].

Розвиток міжнародних правових норм у сфері електронного архівування відбувається у динамічному руслі, з урахуванням технологічних інновацій і нових викликів цифрової епохи. У сучасних підходах акцент робиться на забезпеченні довготривалого збереження цифрової інформації незалежно від змін у програмному забезпеченні чи форматах файлів. Це визначає необхідність постійного оновлення нормативно-правових актів і адаптації правових систем до нових реалій інформаційного середовища [72].

Отже, міжнародний досвід нормативно-правового регулювання електронного архівування є результатом тривалої еволюції правових інститутів, міжнародних угод і технічних стандартів. Він демонструє перехід від локального врегулювання до глобальної координації зусиль у сфері збереження цифрової інформації. На сучасному етапі цей досвід є основою для формування національних підходів до архівування електронних документів, зокрема й в Україні, яка активно адаптує свої правові норми до міжнародних вимог.

Формування міжнародної нормативно-правової бази електронного архівування стало результатом взаємодії різних інституцій — міжурядових організацій, професійних об'єднань архівістів, технічних комітетів зі стандартизації та урядів держав, які прагнули забезпечити узгодженість підходів до збереження цифрової інформації. Перші офіційні ініціативи у цьому напрямі з'явилися у 1980–1990-х роках, коли в міжнародній практиці почали розроблятися стандарти для електронних документів та засобів їх тривалого зберігання [71].

Одним із ключових документів, що визначив підходи до управління цифровими об'єктами, є Модель відкритої архівної інформаційної системи (OAIS), затверджена як міжнародний стандарт ISO 14721:2025 [67]. Цей стандарт встановлює концептуальну структуру для побудови систем довготривалого зберігання цифрових об'єктів. У ньому визначено основні

функції архіву — приймання, збереження, управління, доступ і контроль автентичності інформації. OAIS стала базовою моделлю, на яку орієнтуються архіви багатьох країн світу, а її концепція забезпечує уніфікацію вимог до збереження цифрових ресурсів [67].

У 2002 році Міжнародна організація зі стандартизації ухвалила стандарт ISO 15489-1:2001 «Інформація та документація. Управління документами», який став глобальним орієнтиром для побудови систем електронного діловодства. У ньому визначено принципи створення, зберігання, класифікації, автентифікації та знищення документів. Цей стандарт вважається основою міжнародної концепції управління записами (records management) і передбачає використання електронних систем для забезпечення доказової цінності документів. У 2016 році було ухвалено оновлену редакцію ISO 15489-1:2016, що врахувала розвиток цифрових технологій і поширення електронного урядування [68].

Важливим доповненням до цього стандарту став документ ISO/TR 15801:2017 «Електронні зображення. Законодавчі та процедурні вимоги до зберігання документів», який визначає умови, за яких електронні копії документів можуть мати юридичну силу, еквівалентну паперовим оригіналам. Він регламентує вимоги до процедур сканування, форматів файлів і захисту метаданих. Цей стандарт набув поширення в установах, які переводять архівні фонди у цифрову форму, забезпечуючи відповідність процесу міжнародним правовим нормам [66].

Значний вплив на розвиток архівної справи здійснила діяльність Міжнародної ради архівів (ICA), яка з 1990-х років видає рекомендації та керівництва щодо електронного архівування. Серед ключових документів варто відзначити ICA Principles of Access to Archives (2012), що закріплює принципи прозорості, відкритості та збереження автентичності електронних матеріалів. Крім того, ICA спільно з ЮНЕСКО реалізувала програму «Memory of the World», спрямовану на захист документальної спадщини людства, у тому числі цифрової [66].

Паралельно в межах Організації Об'єднаних Націй було розроблено Керівні принципи для електронного урядування (UN E-Government Survey), які містять положення щодо впровадження електронного діловодства, документообігу та архівування у системах державного управління. Ці принципи сприяють підвищенню прозорості та підзвітності державних інституцій, а також визначають електронний архів як невід'ємну складову сучасного врядування [66].

У контексті європейського права важливе значення має Регламент Європейського Союзу № 910/2014 (eIDAS), який регулює електронну ідентифікацію та довірчі послуги. Хоча цей документ безпосередньо не присвячений архівуванню, він створює правові передумови для легітимності електронних документів, які передаються на архівне зберігання. eIDAS визнає юридичну силу електронного підпису, печатки та позначки часу в усіх державах-членах ЄС, що є фундаментом для довготривалого зберігання документів. Європейська комісія також ініціювала створення специфікації MoReq (Model Requirements for the Management of Electronic Records), перше видання якої було оприлюднено у 2001 році, а оновлене — MoReq2010. Цей документ визначає функціональні вимоги до систем електронного управління документами (ERMS). MoReq встановлює стандартизовані вимоги до створення, оброблення, класифікації, зберігання та архівування електронних документів у державних і приватних структурах. Його положення активно впроваджуються у європейських країнах для забезпечення сумісності систем електронного документообігу [53].

На міжнародному рівні значну роль відіграють стандарти серії ISO 30300–30301, присвячені системам управління документами. Зокрема, ISO 30301:2019 «Management systems for records — Requirements» визначає вимоги до впровадження політики управління документами у межах організацій, включаючи аспекти електронного архівування. Він орієнтований на стратегічне управління інформаційними ресурсами і вимагає, щоб організації

створювали систему контролю за життєвим циклом документів, зокрема електронних [73].

Для збереження метаданих електронних архівів застосовується стандарт ISO 23081-1:2017, який регламентує структуру метаданих, необхідних для управління записами. Цей документ визначає, як інформація про походження, контекст, автентичність і цілісність документа має зберігатися разом із його цифровим вмістом. Застосування цього стандарту забезпечує можливість перевірки достовірності електронних документів навіть через десятки років після їх створення. Важливим аспектом міжнародного регулювання є питання довготривалого збереження цифрових об'єктів. У цьому контексті розроблено ISO 19005 (серія PDF/A), який визначає формат архівного зберігання електронних документів на основі PDF. Цей стандарт гарантує, що документ залишиться читабельним незалежно від змін програмного забезпечення у майбутньому. Він широко застосовується у державних і корпоративних архівах для зберігання офіційних документів [68].

Серед інших важливих документів варто згадати ISO 16175:2020 «Information and documentation — Principles and functional requirements for records in electronic office environments», який встановлює загальні принципи управління записами в електронних системах. Цей стандарт розроблено спільно з Міжнародною радою архівів і він забезпечує взаємозв'язок між створенням, веденням і архівуванням електронних документів. Велике значення для архівної практики має і ISO 16363:2012 «Audit and certification of trustworthy digital repositories», який визначає критерії надійності електронних архівів. Згідно з ним, архіви мають дотримуватися вимог щодо організаційної стабільності, безпеки, автентичності та доступу до збережених матеріалів. Виконання цього стандарту підтверджується сертифікацією архівної установи як «надійного цифрового сховища» [69].

Питання автентичності та збереження електронних документів також відображено у документах ЮНЕСКО, зокрема у Хартії про збереження цифрової спадщини (2003). Цей документ наголошує, що цифрова інформація

є частиною культурної спадщини людства і потребує правового та технічного захисту. Хартія рекомендує державам розробляти національні програми цифрового архівування, створювати інституційні системи захисту та забезпечувати міжнародну співпрацю у сфері збереження цифрових ресурсів. На рівні Ради Європи питання збереження електронної інформації відображене у Рекомендації Rec (2003)15 «Щодо архівного управління в інформаційному суспільстві», яка визначає, що електронні документи мають зберігатися відповідно до принципів автентичності, доступності та цілісності. Рекомендація закликає держави-члени розробляти законодавчі механізми для довготривалого збереження цифрових записів і створювати національні стратегії електронного архівування [72].

Особливе місце займає діяльність Міжнародної організації зі стандартизації (ISO) у розробленні технічних норм з архівування електронних даних у сфері державного управління, фінансів, освіти, охорони здоров'я та науки. Стандарти ISO мають універсальний характер і використовуються як основа для розробки національних нормативних актів у більшості країн світу. Важливу роль у забезпеченні сумісності систем електронного архівування відіграє ініціатива INTERPARES (International Research on Permanent Authentic Records in Electronic Systems), започаткована у 1999 році. У межах цього міжнародного дослідницького проєкту були розроблені принципи збереження автентичності електронних документів, методи перевірки цілісності даних та концепції довгострокового зберігання цифрових записів. Результати дослідження INTERPARES активно застосовуються в архівній практиці Канади, США, Австралії, Італії та інших країн [72].

Окремим напрямом розвитку міжнародних норм є регулювання електронного урядування та відкритих даних, що безпосередньо впливає на архівну діяльність. У цьому контексті варто відзначити Конвенцію Ради Європи про доступ до офіційних документів (Тромсе, 2009), яка встановлює правові гарантії відкритості державних архівів, у тому числі електронних. Значний вплив на правове регулювання архівування здійснили документи

Європейського архівного порталу (European Archives Portal), який координує спільну політику архівних служб держав-членів ЄС. Його діяльність спрямована на створення єдиної системи доступу до архівних матеріалів, у тому числі цифрових, і уніфікацію стандартів опису документів [72].

Сучасна практика також спирається на рекомендації Міжнародної електротехнічної комісії (IEC), які розробляють технічні стандарти з кіберзахисту архівних систем. Зокрема, документи серії ISO/IEC 27001 встановлюють вимоги до систем управління інформаційною безпекою, що є невід'ємною частиною електронного архівування. Останніми роками міжнародні організації акцентують увагу на питаннях стійкості електронних архівів до надзвичайних ситуацій. Так, Програма ЮНЕСКО «PERSIST» (2015) спрямована на розробку глобальної політики збереження цифрової спадщини у контексті ризиків, пов'язаних із війнами, катастрофами та технологічними змінами [72].

Підсумовуючи, можна зазначити, що міжнародне нормативно-правове регулювання електронного архівування формується як багаторівнева система, де поєднуються правові, організаційні та технічні стандарти. Ключовими її характеристиками є універсальність, орієнтація на автентичність, довготривалість і доступність інформації. Ця система постійно вдосконалюється, відображаючи глобальні тенденції розвитку цифрових технологій та інформаційного суспільства. Використання міжнародних стандартів дозволяє державам гармонізувати національне законодавство, підвищувати надійність електронних архівів і забезпечувати сумісність між різними інформаційними системами. Саме на основі цих підходів формується сучасна модель електронного архівування, яка інтегрує правові норми, технічні вимоги й організаційні рішення, забезпечуючи збереження цифрової пам'яті людства на майбутнє.

1.3. Порівняльний аналіз українського та зарубіжного законодавства у сфері електронної ділової документації

У сучасних умовах цифрової трансформації суспільства питання нормативно-правового забезпечення електронної ділової документації набуває особливого значення, оскільки саме від нього залежить ефективність функціонування як державних, так і приватних структур. Ділова документація, у найширшому розумінні цього терміна, охоплює сукупність офіційних документів, що створюються у процесі управлінської, виробничої, наукової, освітньої та іншої діяльності організацій і мають юридичну силу. Вона є матеріальним відображенням ділових процесів, інструментом управління, доказом здійснення певних дій та засобом комунікації між суб'єктами правових відносин. У класичному розумінні ділова документація базується на письмовій формі та відповідних стандартах діловодства, однак поступовий розвиток інформаційних технологій зумовив перехід значної частини документообігу в електронну форму [44, с.67].

Поняття електронної ділової документації поєднує у собі традиційні принципи організації ділового листування, документування управлінських рішень і фіксації юридично значущих фактів із сучасними технологічними можливостями створення, передавання, зберігання та захисту інформації. Електронна ділова документація, за своєю суттю, є продовженням і розвитком паперової системи документообігу, але з урахуванням цифрової форми подання даних, електронного підпису та засобів криптографічного захисту. Вона забезпечує швидкість обміну інформацією, спрощує процеси погодження документів, підвищує прозорість діяльності установ та зменшує витрати на матеріальні ресурси [59]. У той же час її функціонування потребує чіткого правового регулювання, яке б гарантувало автентичність, цілісність і юридичну силу електронних документів.

У контексті порівняльного аналізу варто зазначити, що українське законодавство у сфері електронного документообігу формується відповідно до

європейських стандартів, але має власну специфіку. Закон України «Про електронні документи та електронний документообіг» визначає основні принципи створення, обігу і зберігання електронних документів, встановлює поняття електронного підпису, електронної печатки та електронної ідентифікації [17]. Аналогічні норми містяться і в законодавстві Європейського Союзу, зокрема в Регламенті eIDAS, який закріплює уніфіковані правила для всіх країн-членів ЄС щодо використання електронної ідентифікації та довірчих послуг [53]. Проте, якщо в Європі електронна комунікація між органами влади та громадянами давно стала звичною практикою, то в Україні цей процес іще перебуває на етапі становлення.

Ділова документація, як складова ділової комунікації, виконує не лише інформаційну, але й правову функцію, адже документ є свідченням прийняття рішень, засобом їх фіксації та підтвердженням виконання зобов'язань. Саме тому перехід цієї сфери в електронний формат потребує особливої уваги до питань достовірності, захисту персональних даних та архівного зберігання. Визначення поняття «електронна ділова комунікація» можна розглядати як комплексну категорію, що охоплює процеси обміну діловими повідомленнями, документами, звітами, договорами та іншими управлінськими актами за допомогою цифрових каналів зв'язку. Вона передбачає використання електронної пошти, корпоративних платформ документообігу, систем електронного підпису та засобів ідентифікації користувачів [37, с.25].

Тобто, електронна ділова комунікація виступає не лише технічним, а й правовим феноменом, оскільки її ефективність залежить від наявності нормативної бази, що регулює статус електронних документів та порядок їх обігу. Українська практика у цьому питанні все більше наближається до міжнародних стандартів, однак залишається ряд проблем, пов'язаних із недостатнім рівнем гармонізації національних актів із європейськими вимогами. Зокрема, у деяких випадках ще не повністю врегульовано питання довготривалого зберігання електронних документів, їх передачі до архівів, а

також забезпечення сумісності національних систем електронного підпису з європейськими.

У законодавствах зарубіжних країн можна спостерігати більш системний підхід до цього питання. Наприклад, у Німеччині правове регулювання електронного документообігу здійснюється через комплекс норм, що охоплюють не лише адміністративні процеси, а й приватно-правові відносини, включаючи сферу електронної комерції. У США діє Закон про електронні підписи у глобальній та національній торгівлі (E-SIGN Act), який визнає юридичну силу електронних документів нарівні з паперовими та встановлює чіткі вимоги до процедури автентифікації. У Великій Британії та Франції правове регулювання акцентується на захисті інформації та довірчих сервісах, що забезпечують безпечність обігу даних [76].

Усі ці приклади свідчать про тенденцію до уніфікації підходів у сфері електронного документообігу, коли головними принципами залишаються достовірність, захист, стабільність та доступність інформації. Україна, орієнтуючись на досвід ЄС, адаптує власну нормативну базу, інтегруючи положення європейських актів у національне законодавство. Такий підхід дозволяє не лише підвищити ефективність внутрішнього документообігу, а й забезпечити міжнародну сумісність українських систем електронного документообігу з європейськими. Отже, формування правових засад електронної ділової документації є ключовим чинником побудови сучасного цифрового суспільства, де документ виступає не лише засобом фіксації інформації, а й гарантією її правової значущості.

На нашу думку, розвиток електронного документообігу — це не просто технічна модернізація традиційних процесів, а глибока трансформація управлінської культури, яка потребує узгодженості норм права, технологічних стандартів та організаційних механізмів. У нормативно-правовому полі України одним із ключових актів є вже згадуваний нами у попередніх підрозділах Закон України «Про електронні документи та електронний документообіг» (№ 851-IV), що встановлює принцип: «електронний документ

не може бути відмовлений у юридичній силі тільки тому, що він має електронну форму» . Додатково слід згадати Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (№ 2155-VIII), який набрав чинності 7 листопада 2018 р. і регулює питання електронної ідентифікації, електронного підпису, електронної печатки, електронного маркування часу (таймстамп), електронного зареєстрованого відправлення [18].

У березні 2024 р. Мінфін України наказом № 133 від 18.03.2024 вніс зміни до «Порядку обміну електронними документами із контролюючими органами», узгодивши положення з Законом України «Про внесення змін до окремих законодавчих актів щодо укладення Угоди між Україною та ЄС про взаємовизнання кваліфікованих електронних довірчих послуг» (№ 2801-IX) від 1 грудня 2022 р. Також законодавство про судочинство, зокрема Закон України «Про внесення змін до окремих законодавчих актів щодо обов'язкової реєстрації та використання електронних кабінетів у Єдиній судовій інформаційно-телекомунікаційній системі» (№ 3200-IX від 29 червня 2023 р.), передбачає обов'язковість створення електронного «кабінету» в системі UJITS для певних учасників судового процесу. Українське законодавство охоплює такі напрями: легалізація електронних документів як рівноцінних паперовим, регулювання електронних підписів та довірчих послуг, обмін електронними документами із державними/контролюючими органами, електронізація процесів судової комунікації [50].

З боку Європейського Союзу одним із фундаментальних актів є Регламент (ЄС) № 910/2014 (eIDAS) про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку, який набрав чинності 1 липня 2016 р. у державах-членах ЄС. Цей регламент прямо застосовується в усіх країнах-членах і встановлює, що довірчі послуги (електронний підпис, печатка, відмітка часу, електронне зареєстроване відправлення) мають юридичну силу, як і традиційні паперові процедури, а документи в електронній формі не можуть бути відкинуті тільки тому, що вони електронні. В eIDAS також закладено принцип взаємного визнання

кваліфікованих довірчих послуг між державами-членами. Крім того, 11 квітня 2024 р. ухвалено Регламент (ЄС) 2024/1183, який доповнює eIDAS і стосується створення Європейської цифрової ідентичності (European Digital Identity Wallet) як наступного кроку гармонізації. Отже, зарубіжне законодавство забезпечує універсальний рамковий підхід, взаємне визнання на європейському просторі та пряму дистрибуцію регламенту без потреби транспозиції у національне законодавство [53].

Аналізуючи, можна виокремити кілька спільних тенденцій (Додаток А). По-перше, як українське, так і європейське правове регулювання відходить від того, що електронна форма документації вважалася менш правоздатною або навіть недійсною: встановлюється рівність паперової і електронної форм документа. Наприклад, українське положення, що «електронний документ не може бути відмовлений у юридичній силі тільки тому, що він має електронну форму». По-друге, обидві системи приділяють значну увагу належності ідентифікації сторін, застосуванню електронних підписів чи аналогів, а також довірчих сервісів, що забезпечують автентичність, цілісність і невідмовність електронного документа.

По-третє, існує тенденція до гармонізації і взаємного визнання — наприклад, Україна через закон № 2801-IX адаптує норму взаємовизнання кваліфікованих довірчих послуг відповідно до вимог ЄС. Четверта тенденція — електронізація процесів обміну документами та комунікаційних процедур, зокрема між суб'єктами державно-управлінської діяльності, контролюючими органами, судами. Наприклад, в Україні запроваджується обов'язкова реєстрація електронного кабінету для судового документообігу [50].

Разом із тим між українською та зарубіжною (європейською) системами існують й відмінності, які заслуговують уваги. Кількість та ступінь розвитку законодавчої деталізації: регламент eIDAS є юридичною нормою напряму застосування в державах-членах ЄС, що створює більш однорідне правове поле. В Україні ж законодавство переважно передбачає транспозицію європейських норм, і хоча зроблені значні кроки, все ще є певний

«перехідний» характер регулювання: наприклад, зауважено, що українські служби нотаріату технічно не реалізували повноцінно всі можливості електронного посвідчення, хоча закон дозволяє використання кваліфікованого електронного підпису. В ЄС більш чітко та відразу забезпечено механізми взаємного визнання довірчих послуг між державами-членами, тоді як Україна лише починає упровадження взаємовизнання із третьою країною (з ЄС) [53].

На практичному рівні в ЄС вже налагоджено досить поширене використання електронних документів у державному та приватному секторі на міждержавному рівні, в той час як в Україні ще існують бар'єри щодо сумісності, архівного зберігання електронних документів, стандартизації систем та їх інтеграції між державними органами. У матеріалах зазначено, що в Україні ще не повністю врегульовано питання довготривалого зберігання електронних документів та їх передачі до архівів [46]. В окремих випадках українське законодавство ще встановлює виключення до загального правила рівності електронного та паперового документа — наприклад, зазначено, що деякі документи (паспорт, свідоцтво про народження тощо) можуть залишатись тільки в паперовій формі.

Коли розглядати системну структуру регулювання, можна виокремити такі блоки: створення та визначення електронного документа, встановлення деталей (реквізитів) такого документа, визначення моменту створення і юридичної дії, ідентифікації та аутентифікації сторін, довірчих послуг (електронний підпис, печатка, таймстамп, зареєстроване електронне відправлення), правила обміну та зберігання, архівування та взаємодія між інформаційними системами, а також питання міжнародного/міждержавного визнання. Українське законодавство охоплює більшість з цих блоків, але здійснює поступовий перехід до повної імплементації. Наприклад, законодавство України зобов'язує, що електронний документ, створений із використанням електронного підпису або печатки, має прирівнюватись до оригіналу [46].

У ЄС же підходи більш уніфіковані: регламент напряму встановлює, що юридична сила електронного документа і довірчих послуг визнається скрізь в рамках ЄС. Особливо варто звернути увагу на питання обміну та зберігання електронних документів. В українській практиці — зміни до Порядку обміну електронними документами з контролюючими органами (наказ № 133/2024) чітко регламентують, що створення документа з кількома електронними підписами чи печатками завершується накладанням останнього із зазначенням технології створення такого документа. Водночас, у ЄС довірчі послуги охоплюють також електронні печатки, таймстампи, зареєстроване відправлення, що сприяє більш широкому охопленню електронного документообігу у бізнесі та державному секторі [66].

Отже, у цьому напрямі видно, що законодавства ЄС мають більшу глибину та широту охоплення, тоді як українське законодавство працює за принципом наближення до європейських стандартів з урахуванням національних особливостей. Крім того, значущим є аспект інформаційної інфраструктури та стандартизації: у ЄС питання стандартизації, інтероперабельності та міждержавної сумісності довірчих сервісів вже розроблені (наприклад, через eIDAS і супутні акти). В Україні така інфраструктура, на нашу думку, що потребує додаткових зусиль щодо уніфікації систем і процесів між державними органами та приватним сектором, а також щодо архівного зберігання електронних документів, їх цілості та доступності з часом. Аналіз практики вказує, що суди в Україні визнають електронний документ як доказ і визначають, що його носій або електронна копія можуть бути «оригіналом» за змістом, якщо містять ті самі дані. Це свідчить про зближення з європейськими стандартами, але потребує подальшої імплементації.

Особливо цікавим є питання міжнародного/міждержавного визнання: у ЄС це забезпечується через регламент, який прямо діє у всіх державах-членах, і довірчі послуги кваліфікованого рівня мають бути визнані у всіх країнах-членах. В Україні ж через закон № 2801-IX та відповідні зміни лише почато

процес взаємовизнання українських кваліфікованих довірчих послуг із ЄС [58, с.123]. Хоча механізм національного регулювання в Україні визначено, процес його міжнародної інтеграції ще перебуває в стадії активного розвитку. Що стосується архівування та зберігання електронної документації, то в Україні ще відзначаються прогалини: законодавчо не в повній мірі врегульовано питання тривалого зберігання, передачі електронних документів до архівів, сумісності електронних систем з майбутніми технологіями та забезпечення безпеки протягом усього терміну зберігання. У ЄС стандарти та вимоги до таких питань розвиваються більш системно, з урахуванням міждержавної сумісності та довготривалого зберігання, хоча й там це є складним викликом [1].

Отже, українське законодавство у сфері електронної ділової документації демонструє чітку динаміку розвитку та наближення до європейських норм — забезпечено правовий статус електронних документів, застосування електронних підписів/печать, обмін із державними органами, розвиток електронних процесів судочинства. Зарубіжне (європейське) законодавство має більш системний, уніфікований і інтегрований підхід: є пряме застосування регламентів, взаємне визнання між державами-членами, ширше охоплення довірчих послуг, стандартизація та міждержавна сумісність. Серед ключових відмінностей — ступінь деталізації й масштаб інтеграції, рівень використання електронних документів на практиці, готовність інфраструктури та механізми міждержавного визнання. За подальшої динаміки, можна очікувати, що Україна продовжить імплементацію положень ЄС, удосконалюватиме стандартизовані механізми зберігання і обміну, а також розвиватиме інфраструктуру електронного документообігу.

РОЗДІЛ ІІ. ОСОБЛИВОСТІ ЕЛЕКТРОННОГО АРХІВУВАННЯ ДІЛОВОЇ ДОКУМЕНТАЦІЇ НА ПРИКЛАДІ ПП «ВК НАФТОГАЗПРОМБУД»

2.1. Характеристика системи діловодства та документообігу підприємства

У Розділі ІІ нашої магістерської роботи будуть розглядатися практичні аспекти впровадження та функціонування системи електронного архівування ділової документації на прикладі приватного підприємства «ВК Нафтогазпромбуд» (далі — Підприємство) [3]. Метою цього розділу є аналіз організаційних, технологічних і правових особливостей діловодства підприємства, визначення рівня цифровізації документообігу та оцінка ефективності застосування сучасних інформаційних рішень у сфері архівної справи. У підрозділі 2.1 буде охарактеризовано чинну систему діловодства й документообігу підприємства, визначено її структуру, принципи роботи та основні документообігні процеси.

У підрозділі 2.2 буде досліджено організацію процесу електронного архівування документів, способи їх зберігання, доступу та захисту інформації. У підрозділі 2.3 увага зосереджується на специфіці електронного архівування в умовах воєнного стану, ризиках для об'єктів критичної інфраструктури та практичних шляхах мінімізації загроз для збереження електронних архівів. ПП «ВК Нафтогазпромбуд» (код ЄДРПОУ 33661328) зареєстроване 06 липня 2005 року. Основним видом діяльності є будівництво житлових і нежитлових будівель — код КВЕД 41.20. Також Підприємство здійснює електромонтажні роботи, інші будівельно-монтажні роботи, ремонт електроустаткування, монтаж водопровідних мереж і систем кондиціонування [3].

Сфера діяльності передбачає значний документообіг: контракти з замовниками, технічні завдання, проєктна документація, акти виконаних робіт, бухгалтерські документи, внутрішні накази, протоколи, звіти тощо. У

зв'язку з цим система діловодства і документообігу на Підприємстві організована так, щоб забезпечувати своєчасну, належну і законодавчо-обгрунтовану роботу з документами. Підприємство як юридична особа є платником ПДВ (станом на 23.06.2025) — підлягає чинним вимогам з обліку, звітності та архівування. На рівні організації керівник — директор Прокопенко Микола Васильович, який одноосібно є засновником Підприємства, що характеризує компактну структуру управління і, як наслідок, спрощує прийняття рішень з діловодства [3].

Основні структурні підрозділи, включають відділ бухгалтерії, відділ кадрів, технічний відділ, відділ контролю якості, відділ закупівель та документаційний сектор. Відділ бухгалтерії відповідає за фінансово-економічні документи: рахунки, акти, податкові звіти. Відділ кадрів веде документацію з персоналом: накази про прийом/звільнення, табелі, листки непрацездатності, особові справи. Технічний відділ працює з проєктною документацією, технічними завданнями, актами виконаних монтажних чи електромонтажних робіт. Відділ закупівель формує документи, пов'язані з тендерами, договорами, закупівлями устаткування чи матеріалів – що підтверджується участю підприємства у 98 тендерах.

У документообігу підприємства певна частина документів надходить в електронному вигляді (заявки, тендерна документація, електронна пошта), інша — у паперовій формі (договірні копії, акти підписані сторонами, первинні бухгалтерські документи). Документи входять до системи діловодства через прийом і реєстрацію: кожен вхідний документ отримує реєстраційний номер, дату, підрозділ-одержувач. Вихідні документи оформлюються через відповідний шаблон, погоджуються керівником чи відповідальною особою, реєструються. Внутрішні документи — накази, розпорядження, протоколи — формуються відповідними підрозділами, узгоджуються та передаються до архіву [51].

Строки зберігання документів відповідають чинному законодавству України – бухгалтерські документи зберігаються не менше 5 років, кадрів – 75

років (залежно від категорії), технічна документація – за типовими галузевими переліками. У межах Підприємства застосована наскрізна класифікація за темами:

- договори – закупівлі, будівництво, електромонтаж;
- акти – виконані роботи, приймання;
- бухгалтерські документи – первинні, податкові;
- кадрові – прийом/звільнення, особові справи [51].

Система документообігу передбачає рух документів між підрозділами: наприклад, відділ закупівель → технічний відділ → бухгалтерія → архів. При надходженні договору підрядчиком чи замовником, він реєструється, сканується, передається на погодження, після підписання реалізація робіт супроводжується акторами виконаних робіт, відображеними у системі. Після завершення етапу проєкту документація передається до архіву з електронною копією, паперовий оригінал зберігається або передається до фізичного архівного сховища. Внутрішній контроль забезпечує відповідальну особу за документообіг, яка слідкує за правильністю реєстрації, підписання, передачі на зберігання. Використання електронної пошти, сканування та зберігання документів у файлах формату PDF чи ін. дозволяє прискорити передачу та погодження, але водночас потребує чіткої політики доступу та резервного копіювання [51].

Архів Підприємства, зважаючи на численні об'єкти та роботи, має ділянку паперового сховища та цифровий архів: електронні копії зберігаються на сервері чи у хмарному сховищі, мають індексацію, метадані (дата створення, автор, підрозділ, тема). У частині паперової документації зберігаються оригінали договорів, актів і приймально-передавальних протоколів, що вимагає окремого приміщення з контролем клімату, вогнетривким сховищем. Персонал має доступ до електронного архіву згідно до посадових обов'язків (керівник, технічний фахівець, бухгалтерія). При цьому система доступу може бути багаторівнева — лише керівник має право архівного видалення чи переведення до постійного зберігання. [51]

Поточний стан документообігу характеризується певною частковою цифровізацією, але також високою часткою паперової роботи через специфіку будівельно-монтажної діяльності. На нашу думку, відсутність спеціалізованої системи електронного документообігу (СЕД) може створювати ризики: дублювання документів, затрати часу на ручну реєстрацію, небезпека втрати паперових носіїв. Для подальшої нормалізації ситуації Підприємству доцільно впровадити комплексний модуль СЕД-архіву, який дозволить автоматичну реєстрацію, маршрутизацію документів, контроль термінів зберігання, цифрове підписання. У такій моделі документи створюються у форматі цифрових файлів, з подальшою верифікацією керівництвом, зберігаються у централізованому електронному архіві з версіями, атрибутами та історією змін.

Паперові оригінали після сканування підлягають індексації, і їх фізичне зберігання документується протоколами видачі/повернення. Електронний архів має резервне копіювання, шифрування, аудит доступу. Таким чином, система діловодства і документообігу на підприємстві може бути чітко структурованою, враховувати секторний характер діяльності, масштаб проектної роботи, численні замовлення через тендери, і відповідати класичній моделі, адаптованій до цифрового середовища. Тобто, система діловодства ПП «ВК Нафтогазпромбуд» побудована відповідно до загальноприйнятих принципів організації роботи з документами в будівельно-монтажних підприємствах [51].

Основна мета системи — забезпечення повного циклу обробки документів від моменту їх створення або отримання до передачі на зберігання чи знищення. Діловодство організовується централізовано, через документаційний сектор, який підпорядковується безпосередньо директору Підприємства. На Підприємстві встановлюються єдині правила оформлення, реєстрації, узгодження, виконання, відправлення та зберігання документів. В основі системи лежить принцип уніфікації — усі документи створюються за типовими формами, узгодженими шаблонами або затвердженими бланками

[51]. Документи розподіляються за функціональними видами: організаційно-розпорядчі (накази, розпорядження, протоколи), кадрові (особові справи, трудові контракти, відпустки), фінансові (рахунки, накладні, акти, звіти), технічні (проєкти, креслення, технічні умови, акти випробувань) та договірні (угоди з підрядниками, постачальниками, замовниками).

Усі процеси документування здійснюються із застосуванням комп'ютерних технологій. Для текстових документів використовуються стандартизовані формати (DOCX, PDF), для технічних креслень — DWG або DXF, для бухгалтерських — XLSX чи формати системи M.E.Doc 5. Первинне створення документів здійснюється у відповідних підрозділах. Наприклад, фінансові документи формуються у бухгалтерії, кадрові — у відділі кадрів, технічні — у технічному відділі. Після створення кожен документ підлягає обов'язковій реєстрації у Системі електронного документообігу (СЕД). Для цього призначається відповідальний працівник — секретар, який присвоює документу унікальний реєстраційний індекс, дату та визначає категорію. Реєстрація здійснюється автоматично в електронному журналі, що дозволяє контролювати обіг документів у реальному часі [51].

Усі документи супроводжуються метаданими: найменування, автор, дата створення, короткий зміст, підрозділ-виконавець, рівень доступу, термін зберігання. Для кожного документа формується електронна картка з реквізитами. Якщо документ надходить у паперовому вигляді, він сканується та додається до електронної картки. Таким чином забезпечується паралельне існування електронної та паперової версії. У системі діє класифікація документів за ознаками: вхідні, вихідні та внутрішні. Вхідні документи надходять від зовнішніх контрагентів — замовників, постачальників, державних органів. Їх приймає документаційний сектор, реєструє, визначає виконавця та передає на опрацювання. Вихідні документи готуються підрозділами підприємства, підписуються керівництвом і реєструються перед відправленням адресату. Внутрішні документи створюються для внутрішнього управління: накази, розпорядження, службові записки [51].

Організаційно-розпорядча документація формується у керівництва Підприємства. Накази та розпорядження готуються у цифровому вигляді, підписуються кваліфікованим електронним підписом директора і розсилаються через СЕД працівникам. Кожен співробітник отримує повідомлення про новий документ, підтверджує ознайомлення. Кадрова документація ведеться відповідно до законодавства про працю. Особові справи зберігаються у паперовому вигляді, проте мають електронні дублікати — відскановані документи з обмеженим доступом. Дані про трудові договори, відпустки, табелі обліку часу вносяться до внутрішньої бази даних. Для електронного архівування кадрових документів використовується окрема захищена папка з доступом лише відділу кадрів і директору [51].

Бухгалтерські документи формуються в системі бухгалтерського обліку — первинні накладні, акти, рахунки, звіти автоматично зберігаються на сервері з резервним копіюванням. Для забезпечення відповідності податковим вимогам використовується цифровий підпис бухгалтера. Технічна документація має особливий режим зберігання. Проєктні матеріали, креслення та схеми створюються у спеціалізованих програмах і архівуються в окремому сховищі. Для кожного об'єкта будівництва створюється електронна папка, яка містить: технічне завдання, проєктну документацію, сертифікати, акти виконаних робіт.

Система документообігу забезпечує маршрут руху документів. Після створення документ передається на погодження керівнику підрозділу, потім — директору. Погодження здійснюється електронним шляхом із фіксацією дати й часу. Після затвердження документ або виконується (для наказів, розпоряджень), або надсилається зовнішньому контрагенту (для вихідних листів, актів). У системі діє електронний журнал контролю виконання. Він дозволяє керівництву відстежувати виконання доручень, строки відповідей, статус кожного документа (на погодженні, на виконанні, виконано, в архіві). Це створює прозорість процесів та виключає втрату документів. [51]

Після завершення життєвого циклу документ передається на зберігання до електронного архіву. Для цього визначається термін зберігання згідно з номенклатурою справ. Документи, термін зберігання яких минув, підлягають експертизі цінності — створюється електронний акт на знищення. Електронні копії постійного зберігання дублюються на резервному сервері. Для кожної справи формується електронна обкладинка: індекс, назва, дати початку й завершення, кількість документів, відомості про відповідального виконавця. У паперовому архіві зберігаються лише оригінали особливо важливих документів — договори, акти приймання-передачі, правовстановлюючі документи [51].

Доступ до системи діловодства реалізується за ролями: керівник, начальник відділу, виконавець, секретар, бухгалтер, архіваріус. Кожен співробітник має свій рівень прав: перегляд, редагування, погодження, архівування. Система веде журнал аудиту — хто, коли і який документ переглядав або змінював. Усі дії в СЕД супроводжуються автоматичним резервним копіюванням на хмарне сховище. Раз на добу виконується архівація даних з можливістю відновлення. Для безпеки використовується шифрування, а доступ здійснюється лише через корпоративну мережу з двофакторною автентифікацією [51].

Система документообігу Підприємства працює у тісній взаємодії між підрозділами. Документи можуть передаватися між користувачами без створення паперових копій — усі погодження виконуються електронно. У разі необхідності друку формується офіційний паперовий примірник з QR-кодом, що посилається на електронний оригінал. Для організації документообігу застосовується схема маршрутизації: Ініціатор → Керівник підрозділу → Бухгалтерія/Юридичний відділ → Директор → Канцелярія/Архів. Ця схема забезпечує послідовність узгодження, контроль якості документів і відповідність нормативам. Особливістю системи є використання електронного підпису (КЕП), що прирівнюється до власноручного. Завдяки цьому юридична сила електронних документів відповідає паперовим оригіналам [51].

Для оптимізації документообігу передбачено інтеграцію з бухгалтерськими програмами та електронною поштою. Вхідні документи, що надходять електронною поштою, автоматично реєструються у СЕД. Сканування паперових документів здійснюється на високошвидкісних сканерах із розпізнаванням тексту (OCR). Електронний архів Підприємства має ієрархічну структуру: рік → підрозділ → справа → документ. Це дозволяє швидко знаходити необхідну інформацію за реквізитами чи ключовими словами. Кожен документ має свій статус: «в роботі», «погоджено», «архівований», «знищений» [51].

Керівництво Підприємства отримує аналітичні звіти про обсяги документообігу, середній час погодження, кількість прострочених документів. Це дозволяє оптимізувати управлінські процеси. Отже, така система діловодства забезпечує: оперативність документообігу, прозорість дій, збереження інформації, юридичну значущість документів, а також скорочення витрат часу й ресурсів. Вона відповідає сучасним вимогам до цифровізації управлінських процесів і створює основу для сталого розвитку Підприємства навіть в умовах воєнного стану.

2.2. Організація процесу електронного архівування документів на підприємстві

Електронне архівування на приватному підприємстві «ВК Нафтогазпромбуд» організовано через структурований процес зберігання, систематизації та захисту електронних документів, що забезпечує безперервність управлінських і виробничих процесів [3]. На відміну від державних установ, Підприємство має більшу гнучкість у виборі технологічних рішень, програмного забезпечення та внутрішніх регламентів. Водночас, воно зобов'язане дотримуватись загальнодержавних нормативів діловодства та архівної справи, зокрема вимог Закону України «Про електронні документи та електронний документообіг» [17].

Основною метою електронного архівування є забезпечення надійного зберігання документів у цифровій формі протягом усього терміну їх юридичної значущості. Для цього Підприємство формує власну політику електронного архівування, яка визначає принципи зберігання, доступу, резервного копіювання та захисту інформації. Система побудована на корпоративному сервері з дублюванням у хмарному середовищі. Це дозволяє поєднувати централізоване керування архівом і гнучкий доступ користувачів до документів [51].

Як ми зазначали вище, електронний архів Підприємства структурований за ієрархічним принципом: рік → підрозділ → категорія → справа → документ. Така схема дозволяє зберігати логічні зв'язки між документами, контролювати терміни їх зберігання та спрощує пошук за ключовими параметрами. Кожна справа має електронну обкладинку з реквізитами — індексом, назвою, датами початку і завершення, кількістю документів, відомостями про відповідального виконавця. На першому етапі архівування здійснюється ідентифікація документів, що підлягають зберіганню. Відповідальний працівник (секретар) аналізує завершені документи у Системі електронного документообігу, перевіряє їх статус і готує перелік для передавання до архіву. На цьому етапі проводиться експертиза цінності документів — визначається, які підлягають постійному зберіганню, а які – тимчасовому або знищенню після закінчення строку дії [51].

Другий етап передбачає формування електронних справ. Документи групуються за тематичним принципом: договори, акти виконаних робіт, бухгалтерські звіти, технічні матеріали, кадрові справи. Для кожної справи створюється окрема папка з відповідним індексом і метаданими. До архіву потрапляють лише документи з усіма необхідними реквізитами, підписами (у т. ч. електронними) та затвердженнями. Третій етап — цифрування та форматування. Паперові документи скануються у форматі PDF/A, що відповідає міжнародним стандартам довготривалого зберігання. Електронні файли перетворюються у стандартизовані формати, аби уникнути проблем

сумісності у майбутньому. На кожен файл накладається цифровий штамп (електронна печатка) підприємства [51].

Четвертий етап — індексація документів. У СЕД створюється запис із ключовими параметрами: назва, автор, дата створення, короткий зміст, категорія, рівень доступу, термін зберігання. Для пошуку використовується система метаданих і внутрішній каталог. Індексація є критично важливою для швидкого доступу до потрібної інформації без порушення логіки архівного зберігання. П'ятий етап — перевірка цілісності архіву. Відповідальна особа проводить контроль якості: перевіряє правильність назв файлів, наявність усіх обов'язкових реквізитів, відповідність структури номенклатурі справ. Лише після цього архівна справа набуває статусу «затверджена» й переходить до режиму зберігання. Шостий етап — збереження та резервне копіювання. Архів розміщується на корпоративному сервері, який має дві копії — робочу та резервну. Раз на добу система автоматично створює бекап на окремий носій або у хмару. Задля безпеки використовується шифрування даних та обмеження доступу до конфіденційних категорій документів [51].

Сьомий етап — контроль доступу та аудит дій. Кожен користувач отримує персональний логін і пароль, а всі дії з архівом фіксуються у журналі аудиту. Це дозволяє відслідковувати, хто і коли переглядав чи редагував документ. Такий контроль особливо важливий для приватного підприємства, де значна частина інформації має комерційну таємницю. Електронний архів підтримує багаторівневу систему доступу:

1. загальнодоступні документи (інструкції, накази з питань безпеки);
2. обмежені — лише для керівників підрозділів;
3. конфіденційні — лише для директора, бухгалтера і кадровика.

Ця система дозволяє запобігати несанкціонованому доступу й витоку інформації. Для зручності користування передбачено пошук за реквізитами та повнотекстовий пошук. Система здатна знаходити документи за фразами, датами чи авторами [51]. Пошукові фільтри скорочують час роботи з архівом і зменшують ризик дублювання файлів. Особливістю архівування на ПП «ВК

Нафтогазпромбуд» є поєднання електронного архіву з фізичним сховищем. Усі паперові оригінали документів, що мають юридичну силу (договори, акти, накази), зберігаються в окремій архівній кімнаті. Їх цифрові копії — в електронній системі, із зазначенням місця розташування оригіналу. Це забезпечує повну відповідність між двома носіями.

Для підтримання актуальності архіву Підприємство запроваджує щорічну перевірку електронного фонду. У процесі ревізії визначаються документи, термін зберігання яких сплив, формуються акти на вилучення та знищення. Знищення відбувається шляхом повного видалення файлів із серверів із створенням електронного протоколу, підписаного керівником [51]. Електронний архів також передбачає механізм передавання документів до державного архіву, якщо цього вимагає законодавство. Такі документи експортуються у форматах, затверджених державними стандартами, і супроводжуються електронними описами. Важливою рисою архівування приватних підприємств є оперативність оновлення політик зберігання. Підприємство може адаптувати тривалість зберігання або змінювати структуру архіву відповідно до змін у законодавстві чи бізнес-процесах. Це забезпечує динамічність та ефективність управління інформаційними ресурсами.

Електронне архівування сприяє також оптимізації простору, оскільки більшість документів зберігається у цифровій формі, що дозволяє скоротити витрати на оренду приміщень для паперових архівів. Водночас, це підвищує швидкість доступу до інформації і полегшує віддалену роботу співробітників. Особливу увагу приділено захисту від кібератак і втрат даних. Підприємство впроваджує антивірусний захист, моніторинг підозрілих дій у мережі, резервне копіювання на захищених носіях, а також регламент відновлення роботи архіву у випадку надзвичайних ситуацій [51].

Таким чином, система електронного архівування ПП «ВК Нафтогазпромбуд» ґрунтується на принципах централізації, стандартизації, захисту та довготривалого зберігання документів. Її організаційна структура,

технічна підтримка та система контролю доступу забезпечують відповідність сучасним вимогам інформаційної безпеки, стабільність управлінських процесів і збереження корпоративної пам'яті підприємства.

Власне процес електронного архівування на ПП «ВК Нафтогазпромбуд» здійснюється за чітко визначеним алгоритмом дій, у якому кожен працівник виконує свою роль відповідно до посадових обов'язків [3]. Першим етапом виступає ініціювання архівування, коли підрозділ-виконавець повідомляє діловода про завершення роботи над певним проєктом або документом. Відповідальний працівник у СЕД позначає такі документи статусом «готовий до архівування». На другому етапі секретар проводить попередній перегляд документів, перевіряє наявність усіх обов'язкових реквізитів — підписів, печаток, дат, електронних підтверджень. Якщо документ неповний або не затверджений, він повертається виконавцю на доопрацювання. Так здійснюється первинна експертиза цінності та повноти документації [3].

Третій етап передбачає групування документів у справи. Секретар разом із керівником підрозділу визначає тематичну належність документів: договірна, бухгалтерська, кадрова чи технічна. Для кожної справи створюється окрема електронна папка з відповідним індексом, до якої додаються скановані або електронні версії файлів. На четвертому етапі до процесу долучається фахівець із інформаційних технологій (адміністратор СЕД). Він перевіряє відповідність форматів файлів стандартам архівування (PDF/A, TIFF, XML), проводить шифрування метаданих і створює резервну копію справи. Цей крок гарантує технічну цілісність та сумісність даних у довгостроковому зберіганні. П'ятий етап — внесення метаданих. Секретар заповнює картки документів у базі архіву: вказує автора, дату створення, короткий зміст, термін зберігання, відповідального виконавця та рівень доступу. Адміністратор перевіряє правильність індексації й запускає автоматичне резервне копіювання [51].

На шостому етапі керівник структурного підрозділу перевіряє правильність формування справи. Він підтверджує, шо документи належать до

відповідної категорії, погоджує перелік і підписує електронний акт передачі справи до архіву. Після цього справа переходить до компетенції архіваріуса. Сьомий етап — приймання документів архіваріусом. Працівник архіву Підприємства завантажує електронні справи на сервер архіву, перевіряє їхню структуру, наявність супровідних описів і актів. У разі виявлення розбіжностей архіваріус повідомляє діловода для коригування даних. На восьмому етапі архіваріус проводить внутрішню експертизу цінності. Він звіряє терміни зберігання документів із чинними нормативами, визначає, які документи підлягають постійному, тривалому чи тимчасовому зберіганню. Результати фіксуються у звіті про приймання документів [51].

Дев'ятий етап полягає у присвоєнні архівних індексів. Кожна справа отримує унікальний номер, що відповідає номенклатурі архіву. Цей номер вноситься до електронного журналу обліку справ, що дає змогу швидко відстежувати місцезнаходження кожного документа. Десятий етап передбачає забезпечення захисту інформації. Системний адміністратор встановлює права доступу: лише уповноважені користувачі можуть переглядати, редагувати або копіювати документи. Архіваріус створює списки доступу за категоріями співробітників і підтверджує їх із директором. Одинадцятий етап — фізичне архівування оригіналів. Якщо документ існує в паперовій формі, архіваріус отримує його від секретаря, формує справу, нумерує аркуші й розміщує в архівному приміщенні. У СЕД робиться позначка про місце зберігання оригіналу. На дванадцятому етапі керівник підприємства затверджує електронний акт приймання справи до архіву своїм кваліфікованим електронним підписом. З цього моменту документи набувають статусу «архівовані» і переходять у режим обмеженого доступу.

Тринадцятий етап — створення резервних копій архіву. Адміністратор СЕД налаштовує автоматичне дублювання даних на резервному сервері, а також на зовнішньому носії або у хмарному сховищі. Це забезпечує захист архіву від втрати інформації у разі технічних збоїв. Чотирнадцятий етап полягає у регулярному моніторингу стану архіву. Архіваріус здійснює

щомісячну перевірку наявності справ, тестує доступність файлів і коректність пошуку. У випадку пошкодження або зникнення файлу він відновлює його з резервної копії. П'ятнадцятий етап — використання архівних документів. Коли підрозділу необхідно переглянути архівний документ, він подає електронний запит через СЕД. Архіваріус перевіряє повноваження запитувача і надає тимчасовий доступ або копію документа. Усі такі дії фіксуються в журналі запитів [51].

На шістнадцятому етапі працівники, які отримали тимчасовий доступ, зобов'язані повернути документ у систему після завершення роботи. Архіваріус підтверджує факт повернення та знімає тимчасові права доступу. Таким чином зберігається контроль за кожною архівною одиницею. Сімнадцятий етап стосується оновлення термінів зберігання. Раз на рік архіваріус разом із діловодом формують список документів, строк зберігання яких завершується. Після погодження з директором формується електронний акт на знищення таких справ.

Вісімнадцятий етап — знищення електронних документів, термін зберігання яких минув. Адміністратор здійснює повне видалення файлів із серверів із створенням протоколу дій. Протокол підписується керівником і зберігається у системі як доказ виконання вимог законодавства. Дев'ятнадцятий етап передбачає оновлення номенклатури архіву. Після знищення старих справ архіваріус вносить зміни до електронного каталогу, оновлює списки справ і формує звіт про стан архіву за рік. На двадцятому етапі здійснюється аудит архівної діяльності. Директор Підприємства або уповноважена особа перевіряє відповідність процедур архівування внутрішнім регламентам, а також наявність резервних копій. За результатами аудиту складається службова записка з пропозиціями щодо вдосконалення процесу [51].

Такий алгоритм забезпечує безперервність архівного процесу, чіткий розподіл обов'язків, контроль якості та прозорість усіх дій. Він поєднує технологічні рішення з традиційними архівними принципами, створюючи для

приватного підприємства ефективну систему управління документами, що гарантує надійність, доступність і довготривале зберігання інформації.

2.3. Електронне архівування в умовах воєнного стану: ризики для критичної інфраструктури та шляхи їх мінімізації

В умовах повномасштабної військової агресії проти України особливого значення набуває нормативно-правове регулювання функціонування держави та суб'єктів господарювання в режимі воєнного стану. Воєнний стан визначається Законом України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII як особливий правовий режим, що вводиться у разі збройної агресії чи загрози нападу, та передбачає надання органам державної влади, військовому командуванню і органам місцевого самоврядування додаткових повноважень [29]. Його впровадження спрямоване на забезпечення обороноздатності держави, підтримання громадського порядку та захист критичних об'єктів.

Нормативна база воєнного стану також охоплює Закон України «Про оборону України», Укази Президента України про введення та продовження воєнного стану, постанови Кабінету Міністрів України, а також відомчі інструкції, що регламентують діяльність суб'єктів у сфері енергетики, транспорту, зв'язку, інформаційних технологій тощо [26]. У цьому контексті особливої ваги набуває захист критичної інфраструктури, до якої віднесено об'єкти, системи та ресурси, порушення функціонування яких може призвести до загроз національній безпеці, здоров'ю населення, або економічній стабільності.

Відповідно до Закону України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX, критична інфраструктура — це сукупність об'єктів, послуг, систем та ресурсів, які є життєво важливими для суспільства і держави, а також забезпечують належне функціонування державного управління, економіки, охорони здоров'я, енергетики, транспорту, зв'язку, інформаційних

технологій та інших сфер [25]. Ключовим критерієм віднесення підприємства або установи до критичної інфраструктури є ступінь впливу її діяльності на національну безпеку та стабільність функціонування суспільства.

До категорії критичної інфраструктури, зокрема, належать підприємства паливно-енергетичного комплексу, оскільки вони забезпечують безперервність енергопостачання, що є основою для існування інших секторів економіки [25]. Приватне підприємство «Нафтогазпромбуд» можна обґрунтовано віднести до об'єктів критичної інфраструктури з огляду на його виробничо-економічний профіль. Підприємство здійснює діяльність у сфері будівництва, ремонту та технічного обслуговування об'єктів нафтогазової галузі, бере участь у створенні та відновленні інженерних мереж, що забезпечують транспортування енергоресурсів.

Функціонування ПП «Нафтогазпромбуд» безпосередньо пов'язане із підтриманням безперебійної роботи енергетичної системи України, особливо в умовах підвищених загроз об'єктам паливно-енергетичного комплексу під час воєнних дій [3]. Порушення діяльності Підприємства може мати ланцюговий ефект для суміжних галузей — енергетики, промисловості, комунального господарства, транспорту, а також безпосередньо вплинути на обороноздатність держави. Саме тому воно належить до сектору енергетичної критичної інфраструктури згідно з Національним переліком секторів і підсекторів критичної інфраструктури, затвердженим постановою Кабінету Міністрів України № 1109 від 09.10.2020 [25].

Підприємства цього типу мають особливі зобов'язання щодо захисту інформаційних систем, збереження технічної документації та забезпечення безперервності управлінських процесів. У сучасних умовах одним із ключових аспектів їхньої діяльності є електронне архівування, що забезпечує захист і доступність даних незалежно від фізичного стану об'єктів або ризиків знищення матеріальних носіїв. Проте воєнний стан створює низку додаткових викликів для безпеки електронних архівів — від кіберзагроз і втрати енергопостачання до фізичного пошкодження серверів чи порушення

логістики резервного копіювання. Розуміння нормативного контексту та статусу підприємства як об'єкта критичної інфраструктури є передумовою для розроблення ефективних стратегій інформаційного захисту [25].

Для ПП «Нафтогазпромбуд» це означає необхідність упровадження комплексної системи електронного архівування, що відповідає державним стандартам у сфері інформаційної безпеки, зокрема вимогам Закону України «Про основні засади забезпечення кібербезпеки України». Підприємство повинно забезпечити не лише фізичний захист даних, а й стійкість електронних систем до атак, технічних збоїв і зовнішніх загроз. Отже, у воєнний період ефективне електронне архівування стає не лише питанням внутрішньої організації документообігу, а й елементом національної безпеки. Розроблення заходів щодо мінімізації ризиків вимагає інтеграції правових, технічних і організаційних підходів, спрямованих на збереження інформаційних ресурсів критичної інфраструктури, серед яких — ПП «Нафтогазпромбуд» [3].

Загалом, електронне архівування в діяльності підприємств критичної інфраструктури має визначальне значення для збереження інформаційних ресурсів, підтримання безперервності управління та забезпечення правової достовірності документів. У сучасних умовах воєнного стану електронні архіви стають не просто інструментом документообігу, а елементом національної стійкості, оскільки втрата або компрометація даних може мати стратегічні наслідки. Для ПП «Нафтогаз промбуд» як суб'єкта енергетичної інфраструктури питання надійного архівування електронної інформації має особливу вагу через складну логістику будівельно-монтажних процесів і взаємодію з державними замовниками [3].

Основним завданням системи електронного архівування є створення структурованого, безпечного й доступного середовища для довгострокового зберігання електронних документів. Проте у воєнних умовах на перший план виходить фактор ризику. Ризики електронного архівування для критичної інфраструктури можна поділити на три великі групи: технічні, організаційні

та кібернетичні. Кожна з цих груп має свій механізм впливу, свої наслідки і потребує специфічних заходів для мінімізації. До технічних ризиків належать фізичне знищення серверних потужностей, втрата доступу до обладнання через обстріли, відключення електроенергії, пошкодження кабельних ліній, а також вихід з ладу систем резервного копіювання. Для ПП «Нафтогаз промбуд» такі ризики особливо актуальні, оскільки його діяльність зосереджена у промислових регіонах, які можуть бути об'єктами військових дій [3]. Будь-яке пошкодження дата-центрів або локальних серверів може призвести до повної втрати архівної бази проектно-кошторисної документації, контрактів та технічних звітів.

Організаційні ризики включають недосконаліть внутрішніх регламентів, нестачу підготовленого персоналу, відсутність чітких процедур відновлення даних після інцидентів та недостатній контроль за доступом до архівів. У воєнних умовах ці ризики посилюються через мобілізацію кадрів, вимушену евакуацію персоналу, а також скорочення часу на контроль управлінських процесів. Недостатня організаційна дисципліна може стати передумовою для витоку інформації або порушення ланцюга збереження документів. Кібернетичні ризики, у свою чергу, мають найбільш руйнівний потенціал. У період воєнного стану зростає активність ворожих хакерських угруповань, спрямованих на дестабілізацію роботи критичних об'єктів. Кібератаки можуть призвести не лише до крадіжки конфіденційних даних, а й до повного шифрування архівів або їх знищення.

За даними Державної служби спеціального зв'язку та захисту інформації, кількість кібератак на енергетичні підприємства України у 2024-2025 роках зросла на 70% [60]. ПП «Нафтогазпромбуд» як субпідрядник стратегічних енергетичних об'єктів також перебуває у зоні підвищеного ризику, оскільки обробляє технічну та геолокаційну інформацію, яка може становити інтерес для противника. Загальносистемна вразливість полягає в тому, що електронне архівування без належного резервування даних не гарантує їх повного збереження. Тому однією з основних вимог для ПП

«Нафтогазпромбуд» має бути створення багаторівневої системи резервного копіювання. Це передбачає одночасне зберігання архівів у кількох незалежних середовищах — на локальних серверах, у хмарних сховищах і на фізичних носіях, розташованих у безпечних регіонах.

Крім того, важливо забезпечити криптографічний захист архівних файлів. Згідно з вимогами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», підприємства критичної інфраструктури мають впроваджувати сертифіковані засоби захисту, які відповідають державним стандартам ДСТУ ISO/IEC 27001 [22]. Для ПП «Нафтогазпромбуд» це означає необхідність використання систем шифрування, електронного підпису та контрольних журналів для відстеження всіх дій з документами. Додатковим напрямом мінімізації ризиків є формування політики безперервності бізнес-процесів. Така політика повинна містити процедури відновлення електронних архівів у разі втрати доступу, кібератаки або фізичного знищення обладнання. На Підприємстві доцільно розробити «План аварійного реагування на інциденти електронного архівування», який визначатиме порядок дій відповідальних осіб, джерела резервних копій і часові рамки відновлення інформації.

Не менш важливим аспектом є людський фактор. Практика свідчить, що понад 70% інцидентів із витоком або втратою даних пов'язані саме з помилками персоналу [3]. Тому система електронного архівування ПП «Нафтогаз промбуд» повинна передбачати багаторівневу систему авторизації користувачів, а також обмеження доступу до архівів за принципом службової необхідності. Працівники, які мають доступ до конфіденційної інформації, мають проходити регулярні тренінги з інформаційної безпеки. У контексті воєнного стану особливу загрозу становить також можливість втручання зсередини — так званий «внутрішній саботаж». Це ситуації, коли співробітники, перебуваючи під психологічним тиском або через зовнішній вплив, навмисно пошкоджують або передають інформацію стороннім особам. Для зниження цього ризику важливо встановити системи аудиту дій

користувачів і автоматичні сповіщення про спроби несанкціонованого доступу [3].

Технологічно ефективне електронне архівування передбачає використання систем управління документами (DMS), що мають модулі архівації, резервного копіювання та контролю версій. Для ПП «Нафтогаз промбуд» доцільним є впровадження програмних рішень, сумісних із державними стандартами електронного документообігу, зокрема платформ, які підтримують протоколи безпечного обміну даними (S/MIME, HTTPS, VPN). Це забезпечить сумісність архівних процесів із державними системами, наприклад, «Єдиним державним вебпорталом електронних послуг» [13]. Окрему увагу слід приділити питанням зберігання технічної та конструкторської документації, яка має великі обсяги графічних і текстових файлів. Електронні архіви таких документів повинні мати оптимізовану систему метаданих, що дозволяє швидко знаходити потрібні файли за параметрами проекту, дати, об'єкта чи замовника. Це сприятиме ефективному управлінню даними в екстремальних умовах, коли доступ до архівів може бути обмеженим у часі.

У сучасній практиці підприємств енергетичного сектору зростає роль хмарних технологій [61]. Вони дозволяють зберігати дані на віддалених серверах за межами зон бойових дій. Для ПП «Нафтогазпромбуд» це означає можливість створення «географічно розподіленого архіву», де основні копії зберігаються в українських центрах обробки даних, а резервні — у закордонних дата-центрах, наприклад, у країнах ЄС. Це мінімізує ризик одночасної втрати всіх архівів у разі катастрофічних подій. Втім, використання хмарних технологій вимагає суворого дотримання вимог до передачі персональних і комерційних даних за кордон, встановлених законодавством України. Тому будь-які контракти на зберігання даних повинні супроводжуватись угодами про конфіденційність і технічними протоколами шифрування [61].

Ще одним аспектом мінімізації ризиків є забезпечення енергетичної незалежності архівних систем. У воєнний час перебої з електропостачанням можуть бути тривалими, тому важливо оснащувати сервери системами безперебійного живлення (UPS) та генераторами. ПП «Нафтогаз промбуд» може застосовувати моделі мобільних серверних модулів, які можна оперативно переміщати в безпечні райони. Інформаційна безпека архівів повинна також враховувати ризик руйнування мережевої інфраструктури. Для цього доцільно застосовувати офлайн-резервування — періодичне копіювання архівів на зовнішні носії, які зберігаються в ізольованих сховищах. Такі копії можуть бути життєво необхідними у разі повного відключення мережевого доступу або втрати зв'язку [61].

У системі ризиків особливе місце посідає питання збереження юридичної сили електронних документів. Під час воєнного стану існує ризик втрати електронних підписів або неможливості перевірити автентичність файлів через відсутність доступу до реєстрів. Тому підприємству слід використовувати технології зберігання електронних підписів у форматі довгострокового зберігання (LTV — Long Term Validation), що дозволяє підтвердити підпис навіть через кілька років. З метою мінімізації ризиків також необхідно впроваджувати моніторинг стану електронного архіву. Це передбачає постійний контроль за цілісністю даних, автоматичну перевірку резервних копій і системне тестування планів відновлення. Для цього ПП «Нафтогазпромбуд» може створити окремий підрозділ інформаційної безпеки або закріпити відповідальних осіб за підтримання архівної інфраструктури [3].

Ефективна система архівування має спиратися на внутрішню політику інформаційного менеджменту. Цей документ повинен регулювати порядок створення, обробки, зберігання, передачі та знищення електронних документів, визначати рівні доступу та правила резервування. У воєнних умовах політика має передбачати також алгоритм дій у разі евакуації або втрати доступу до фізичних приміщень підприємства [3].

Необхідно наголосити, що захист електронних архівів — це не разовий захід, а безперервний процес. З огляду на динамічність воєнної ситуації та розвиток кібертехнологій, підприємство повинно регулярно оновлювати програмне забезпечення, аналізувати нові загрози і адаптувати до них свої політики безпеки. Узагальнюючи, можна зазначити, що система електронного архівування ПП «Нафтогазпромбуд» у воєнний період повинна відповідати принципам стійкості, відмовостійкості та конфіденційності. Її ефективність залежить від гармонійного поєднання технічних, правових і організаційних рішень.

Таким чином, шляхами мінімізації ризиків електронного архівування є:

- впровадження багаторівневої системи резервного копіювання;
- використання сертифікованих засобів криптографічного захисту;
- розроблення політики безперервності бізнес-процесів;
- проведення системного навчання персоналу;
- застосування географічно розподілених сховищ;
- створення автономних джерел живлення;
- впровадження моніторингу цілісності архівів.

Завдяки цим заходам ПП «Нафтогазпромбуд» зможе забезпечити безперервність своєї діяльності навіть у найскладніших умовах воєнного часу, зберігаючи інформаційні ресурси, що мають стратегічне значення для енергетичної безпеки України.

РОЗДІЛ ІІІ. ОПТИМІЗАЦІЯ ПРОЦЕСУ ЕЛЕКТРОННОГО АРХІВУВАННЯ ДІЛОВОЇ ДОКУМЕНТАЦІЇ НА ПРИКЛАДІ ПП «ВК НАФТОГАЗПРОМБУД»

3.1. Удосконалення системи електронного архівування та управління документацією

Як ми неодноразово наголошували у попередніх Розділах І та ІІ, сучасні умови цифровізації бізнес-процесів питання ефективного електронного архівування ділової документації стають ключовим чинником підвищення продуктивності та інформаційної безпеки підприємств. Використання сучасних технологій, автоматизація процесів, інтеграція з іншими системами підприємства та забезпечення нормативної відповідності створюють основу для ефективного управління діловою документацією. Наступні підрозділи Розділу ІІІ магістерської роботи будуть присвячені питанням захисту персональних даних та технологічній оптимізації архівних процесів, що є логічним продовженням представленого напряму удосконалення.

Приватні компанії, зокрема такі як ПП «ВК Нафтогазпромбуд», щодня генерують великі обсяги даних, які потребують системного зберігання, швидкого доступу та захищеності [3]. Оптимізація процесу електронного архівування дозволяє не лише раціоналізувати документообіг, а й мінімізувати витрати часу та ресурсів на оброблення інформації. Одним із напрямів удосконалення є створення уніфікованої системи управління документами, що інтегрується з іншими інформаційними системами підприємства. Така система забезпечує єдиний стандарт обліку, збереження та пошуку файлів, що сприяє прозорості внутрішніх процесів.

Важливим кроком оптимізації є автоматизація процедур реєстрації, класифікації та архівації документів. Завдяки впровадженню спеціалізованих програмних рішень можна суттєво скоротити час на виконання рутинних операцій. Це дозволяє працівникам зосередитись на аналітичних та

управлінських завданнях, підвищуючи загальну ефективність діяльності [1]. Системи електронного архівування нового покоління підтримують інтелектуальний пошук за метаданими, ключовими словами або контентом документів, що значно спрощує процес їхнього опрацювання. Для приватних підприємств важливо також забезпечити сумісність архівних рішень із чинними нормативно-правовими вимогами.

Оптимізація має враховувати стандарти електронного документообігу, терміни зберігання різних категорій документів та вимоги до форматів файлів [1]. Це дозволяє уникнути правових ризиків і забезпечити належний рівень довіри до електронних копій. Одним із ефективних інструментів є впровадження електронних підписів, що гарантують автентичність та цілісність інформації. Удосконалена система архівування повинна підтримувати багаторівневу структуру доступу, що дає змогу гнучко розподіляти права між користувачами. Це особливо актуально для підприємств, де функціонує кілька відділів із різними рівнями відповідальності. Оптимізація у цьому напрямі передбачає застосування систем контролю версій, що дає змогу відстежувати зміни у документах і зберігати історію їх оновлень. Такий підхід не лише підвищує прозорість управління, а й спрощує аудит інформаційних процесів.

Важливим аспектом є централізація архівного простору, коли всі документи зберігаються в єдиному захищеному сховищі [61]. Це унеможливлює дублювання файлів, втрату актуальних версій та сприяє формуванню єдиної бази знань підприємства. Для підвищення зручності користування архівом доцільно запровадити інтуїтивно зрозумілий інтерфейс з можливістю фільтрації, сортування та групування документів. Окрему увагу слід приділити стандартизації назв файлів та внутрішніх індексів, що забезпечує логічну структуру збереження даних [58, с.167]. Такий підхід спрощує навігацію та пошук інформації, особливо при роботі з великими масивами документації. Оптимізація процесу архівування також передбачає створення резервних копій та системи відновлення даних у разі технічних

збоїв. Впровадження хмарних технологій дозволяє підвищити гнучкість та мобільність доступу до архівів, що є перевагою для підприємств із розгалуженою структурою [61].

Важливо, щоб удосконалена система електронного архівування підтримувала інтеграцію з бухгалтерським, кадровим та виробничим програмним забезпеченням. Це забезпечить безперервність інформаційних потоків і зменшить ймовірність помилок під час обміну даними. Застосування аналітичних інструментів на базі архіву дозволяє керівництву отримувати статистичні дані про документообіг, виявляти вузькі місця та прогнозувати навантаження на систему. Ще одним напрямом оптимізації є впровадження політики життєвого циклу документів, що передбачає автоматичне визначення термінів зберігання та архівації. Це зменшує обсяг непотрібних файлів і підтримує актуальність бази даних. Для підвищення рівня контролю доцільно використовувати журналізацію дій користувачів, що фіксує всі операції з документами [61].

Сучасні тенденції демонструють, що цифрове архівування поступово переходить від пасивного зберігання до активного управління інформаційними ресурсами. Це означає, що архів стає не лише сховищем, а й інструментом аналітики, управління знаннями та підтримки прийняття рішень. Оптимізація процесів архівування на ПП «ВК Нафтогазпромбуд» має на меті створити саме таку систему — динамічну, безпечну та орієнтовану на користувача [3]. Загалом, удосконалення системи електронного архівування передбачає комплексний підхід, який поєднує технічні, організаційні та управлінські рішення.

Подальше вдосконалення системи електронного архівування на ПП «ВК Нафтогазпромбуд» потребує переходу від лінійної моделі збереження документів до інтегрованої цифрової екосистеми управління інформацією [3]. Оптимізація процесів, окреслених у підрозділі 2.2, повинна бути спрямована на підвищення швидкодії, автоматизацію, зменшення людського фактору та підвищення надійності даних. Насамперед доцільно модернізувати етапи

ідентифікації та класифікації документів, впровадивши технологію інтелектуального розпізнавання вмісту (OCR). Це дозволить автоматично визначати тип документа, ключові реквізити та метадані ще до втручання працівника.

Також варто автоматизувати процедуру експертизи цінності документів за допомогою алгоритмів машинного навчання, які зможуть класифікувати файли за категоріями зберігання відповідно до затверджених критеріїв. Таке рішення не лише скоротить час архівування, а й зменшить ймовірність помилок при ручному відборі матеріалів. Оптимізація процесу групування документів у справи може бути досягнута шляхом застосування шаблонів діловодства — система автоматично формуватиме справи за попередньо визначеними параметрами (тип документа, рік, підрозділ). Це дозволить уникнути дублювання папок і підвищить структурованість архіву.

Удосконалення етапу форматування передбачає впровадження централізованого конвертера, що автоматично перевіряє відповідність файлів стандарту PDF/A чи XML, накладає електронні печатки й створює резервні копії [61]. Такі механізми значно підвищують надійність і довготривалу збереженість інформації. Для поліпшення точності індексації доцільно інтегрувати функції автозаповнення метаданих на основі інформації із самих документів або попередніх шаблонів. Це спростить процес введення даних, мінімізує помилки й забезпечить одноманітність архівних описів.

Етап контролю цілісності архіву потребує автоматизації через систему регулярної перевірки контрольних сум. Вона здатна фіксувати будь-які зміни в документах, що підвищує рівень безпеки та прозорості. Для збереження резервних копій доцільно застосовувати стратегію «3–2–1»: три копії даних, дві на різних носіях, одна — у хмарному сховищі [61]. Це забезпечить стійкість архіву навіть у разі фізичних пошкоджень серверів або кібератак. Контроль доступу до архіву можна вдосконалити шляхом впровадження системи багатофакторної автентифікації та ролей користувачів. Кожен співробітник матиме не лише логін і пароль, а й тимчасовий одноразовий код доступу. Це

підвищить рівень кіберзахисту без ускладнення роботи персоналу. Для зручності адміністрування прав доступу варто запровадити автоматичне оновлення ролей відповідно до кадрових змін у підприємстві.

Резервом оптимізації є впровадження централізованого порталу архіву з інтерфейсом, який поєднує функції пошуку, перегляду, обміну та аналітики. Такий портал може підтримувати роботу через веббраузер і мобільні пристрої, що забезпечить віддалений доступ працівників. У контексті цифрової трансформації доцільно перейти на модель «архів як сервіс», коли зберігання, індексація, пошук і резервне копіювання здійснюються на єдиній платформі [62]. Особливу увагу слід приділити вдосконаленню процесу запитів до архіву. Автоматизована система запитів дозволить працівникам отримувати доступ до документів через електронну заявку, яка проходить погодження відповідальними особами без втручання архіваріуса. Це зменшить навантаження на персонал і скоротить час очікування користувачів. Усі запити мають автоматично фіксуватися в журналі дій, що забезпечить повну прозорість.

Для оптимізації перевірки наявності архівних одиниць варто запровадити функцію автоматичного звіряння даних. Система періодично перевірятиме відповідність фактичного складу архіву його електронному опису, повідомляючи про можливі розбіжності, що полегшить роботу архіваріуса та забезпечить постійну актуальність бази даних. Ще одним важливим напрямом удосконалення є створення інтегрованого календаря архівних подій. У ньому система автоматично нагадуватиме про закінчення терміну зберігання документів, необхідність ревізії або передачі до державного архіву. Така функція мінімізує ризик порушення регламентів і дозволяє своєчасно планувати роботи [62].

Важливо забезпечити гнучкість архівної системи до змін у законодавстві. Для цього рекомендується впровадити модуль оновлення нормативних параметрів, який автоматично коригуватиме політику зберігання відповідно до нових правил. Це гарантує, що архів Підприємства завжди буде

відповідати вимогам чинних стандартів [51]. Із метою підвищення ефективності оброблення документів варто застосовувати технології штучного інтелекту, здатні розпізнавати закономірності у потоках даних. Наприклад, система може самостійно визначати тип документа (договір, акт, звіт) і присвоювати йому відповідну категорію зберігання. Такі алгоритми підвищують точність архівування та скорочують участь людини.

Для покращення контролю за достовірністю електронних підписів і печаток доцільно впровадити автоматичну перевірку сертифікатів у режимі реального часу. Це дозволить вчасно виявляти документи з простроченими або недійсними електронними ключами. У свою чергу, система має зберігати журнали перевірок, щоб забезпечити юридичну доказовість дій. Підвищити рівень безпеки архіву допоможе впровадження модулів шифрування «на льоту», коли дані шифруються одразу при створенні або редагуванні документа. Також варто використовувати технологію токенізації, що дозволяє замінювати конфіденційні дані у базі спеціальними ідентифікаторами. Це мінімізує ризик витоку персональної чи комерційної інформації [62].

Система резервного копіювання повинна мати можливість віддаленого відновлення архіву. Для цього доцільно створити аварійний план дій, що визначає алгоритм відновлення роботи у разі збоїв. До плану мають входити графіки тестування резервних копій та періодичні тренування працівників. Із метою підвищення ефективності взаємодії між підрозділами підприємства слід забезпечити інтеграцію архівної системи з бухгалтерським, кадровим, технічним і проектним програмним забезпеченням. Це дозволить створити єдине інформаційне середовище, де документи автоматично передаватимуться між системами без повторного введення даних.

Упровадження єдиного довідника реквізитів документів забезпечить уніфікацію назв, індексів і категорій. Це підвищить зручність пошуку, зменшить кількість помилок та сприятиме узгодженості архівних метаданих. Додатково можна реалізувати функцію автоматичного формування звітів про документообіг: кількість справ, обсяг збережених даних, частоту звернень до

архіву. Такі звіти допоможуть керівництву оцінювати ефективність системи. Для підвищення продуктивності працівників архіву доцільно використовувати адаптивне навчання персоналу. Система електронного архівування може містити інтерактивний довідник або навчальний модуль із порадами щодо виконання основних дій. Це скоротить час адаптації нових працівників і підвищить рівень дисципліни у роботі з документами [62].

Важливою складовою оптимізації є моніторинг ефективності архівних процесів. Для цього потрібно розробити показники ефективності: середній час обробки документа, швидкість пошуку, кількість помилок індексації, обсяг архіву, використання ресурсів. Аналіз таких показників дозволить своєчасно виявляти проблеми та коригувати роботу системи. Оптимізація процесів передбачає також раціональне використання технічних ресурсів. Доцільно запровадити автоматичний розподіл навантаження між серверами, що дозволить забезпечити стабільну роботу навіть при пікових зверненнях. Також варто впровадити енергозберігаючі механізми для серверів і систем зберігання даних, що зменшить експлуатаційні витрати підприємства.

Одним із перспективних напрямів є створення цифрових дублікатів архівних процесів. Такий підхід дозволяє моделювати роботу архіву у віртуальному середовищі, прогнозувати наслідки змін і тестувати нові технологічні рішення без ризику для основної системи. Для забезпечення високої якості архівування варто періодично проводити внутрішні аудити, що перевірятимуть відповідність процедур вимогам стандартів ISO 15489 та ДСТУ 4423 [10]. Це дозволить підтримувати високу репутацію підприємства й забезпечити надійність інформаційних процесів.

Особливу увагу слід звернути на зручність користувацького інтерфейсу. Його варто зробити інтуїтивним, із можливістю персоналізації — кожен користувач може налаштовувати робочий простір під свої потреби. Наявність темного режиму, фільтрів і швидких дій підвищить комфорт роботи й зменшить навантаження на працівників. Важливим елементом удосконалення є створення системи оповіщень та звітності. Система повинна надсилати

повідомлення про завершення архівування, появу нових документів, зміни статусів або помилки. Такі повідомлення можуть надходити через електронну пошту або месенджери [64].

Із метою забезпечення стабільності архівного процесу доцільно створити окремий підрозділ або робочу групу, яка відповідатиме за розвиток електронного архіву. Ця група повинна розробляти пропозиції щодо модернізації, тестувати нові функції та проводити навчання персоналу. Загалом, оптимізація процесів архівування має бути спрямована не лише на технічне вдосконалення, а й на формування нової корпоративної культури роботи з інформацією. Працівники повинні усвідомлювати важливість належного збереження документів і дотримання регламентів.

Підприємству варто запровадити політику постійного поліпшення архівної системи (Continuous Improvement Policy) 62. Вона передбачає регулярний аналіз проблем, обговорення нових рішень та поступове впровадження змін. Це забезпечить гнучкість системи й адаптацію до технологічних інновацій. Таким чином, оптимізація процесів електронного архівування на ПП «ВК Нафтогазпромбуд» полягає у комплексному поєднанні автоматизації, інтеграції, безпеки та навчання персоналу. Запропоновані напрями вдосконалення дозволять перетворити архів із пасивного сховища документів на ефективний інструмент управління знаннями, що сприятиме стратегічному розвитку підприємства.

3.2. Удосконалення системи забезпечення захисту персональних даних та інформаційної безпеки електронного архіву підприємства

Коли більшість управлінських, фінансових та кадрових процесів переходять в електронну форму, питання захисту персональних даних і інформаційної безпеки набувають першочергового значення. Для приватних підприємств, які працюють із великими базами даних, це не лише питання технічного захисту, а й елемент корпоративної відповідальності, що впливає

на репутацію, стабільність і довіру клієнтів. Електронний архів є одним із найбільш вразливих сегментів інформаційної інфраструктури, адже він містить не лише комерційно важливі відомості, а й персональні дані співробітників, контрагентів, клієнтів. Будь-яке порушення конфіденційності або цілісності даних може спричинити значні правові та фінансові наслідки для підприємства.

Важливість забезпечення захисту персональних даних в електронному архіві зумовлена тим, що інформація про фізичних осіб — це стратегічний ресурс. У випадку ПП «ВК Нафтогазпромбуд» це — дані про працівників, клієнтів, постачальників, учасників проєктів, які обробляються під час виконання виробничих і адміністративних завдань. Система електронного архівування має гарантувати, що ці дані зберігаються відповідно до вимог Закону України «Про захист персональних даних» і міжнародних стандартів GDPR [20]. Це означає, що доступ до інформації має бути чітко регламентований, а її оброблення — здійснюватися лише з метою, визначеною політикою конфіденційності підприємства [20].

Важливо наголосити, що для приватних компаній із великими обсягами даних ключовою загрозою є несанкціонований доступ до архіву, що може відбуватися як із зовнішніх джерел (кібератаки), так і зсередини (помилки або зловживання співробітників) [51]. Тому забезпечення інформаційної безпеки має базуватися на принципі багаторівневого захисту, який включає технічні, організаційні та правові заходи. До технічних належать шифрування даних, контроль доступу, автентифікація користувачів, моніторинг підозрілих дій. Організаційні заходи передбачають регламентацію процесів доступу до архіву, навчання персоналу та ведення журналів аудиту.

Особливу увагу необхідно приділити питанню контролю за правами доступу. У системі електронного архівування слід чітко визначити ролі користувачів, встановити принцип мінімізації привілеїв, за яким кожен працівник має доступ лише до тієї інформації, що потрібна йому для виконання посадових обов'язків. [1] Це мінімізує ризики несанкціонованого

ознайомлення з конфіденційними файлами. Для додаткового захисту варто впровадити механізми багатофакторної автентифікації та електронних підписів, що унеможливлює доступ сторонніх осіб навіть у разі викрадення пароля. Забезпечення інформаційної безпеки електронного архіву також передбачає створення системи виявлення та реагування на інциденти.

Підприємство має застосовувати засоби моніторингу, які відстежують спроби несанкціонованого доступу або змін у файлах, а також системи сповіщення, що оперативно повідомляють відповідальних осіб про потенційні загрози [1]. Така проактивна позиція дозволяє вчасно реагувати на ризики й запобігати втратам даних. Не менш важливим аспектом є резервне копіювання інформації. Для приватних підприємств, які працюють із великими базами даних, створення багаторівневої системи резервування — критично необхідне. Резервні копії мають зберігатися у різних фізичних і хмарних середовищах із дотриманням принципу географічного розподілу. Це гарантує відновлення архіву у випадку технічних збоїв, стихійних лих чи кібератак [1].

Варто також підкреслити, що ефективний захист даних неможливий без постійного оновлення програмного забезпечення та систем безпеки. Застарілі програми часто містять уразливості, якими користуються зловмисники. Тому ПП «ВК Нафтогазпромбуд» має впровадити регулярне оновлення програмного забезпечення архіву, систем шифрування, антивірусного захисту й серверного обладнання [3]. Це забезпечить актуальність рівня безпеки відповідно до сучасних викликів. Важливою складовою інформаційної безпеки є навчання персоналу. Навіть найкращі технічні рішення можуть бути марними, якщо працівники не дотримуються правил безпечної роботи з даними. Тому на Підприємстві слід систематично проводити інструктажі та тренінги з питань захисту персональних даних, розпізнавання фішингових атак, використання електронних підписів і дотримання внутрішніх політик безпеки [51].

Захист персональних даних має розглядатися як частина корпоративної культури підприємства. Кожен працівник повинен усвідомлювати свою

відповідальність за збереження інформації. Для цього доцільно запровадити систему мотивації за дотримання вимог інформаційної безпеки та персональної відповідальності за їх порушення. Необхідним елементом системи захисту є регулярний аудит безпеки, який дозволяє оцінювати ефективність діючих заходів та виявляти потенційні слабкі місця. Аудит може проводитись як внутрішніми силами, так і зовнішніми експертами. За його результатами формується план усунення виявлених недоліків і модернізації системи [65].

Таким чином, забезпечення захисту персональних даних і інформаційної безпеки електронного архіву є невід'ємною частиною ефективного управління інформаційними ресурсами підприємства. Для ПП «ВК Нафтогазпромбуд» це питання має стратегічне значення, оскільки підприємство працює з великими обсягами чутливої інформації, від якої залежить його ділова репутація, конкурентоспроможність і довіра партнерів. Формування комплексної системи захисту, що поєднує сучасні технології, правові механізми й освічений персонал, є запорукою стабільності та безпеки електронного архіву в умовах зростаючих кіберзагроз [65].

Удосконалення комплексної системи захисту персональних даних та інформаційної безпеки на ПП «ВК Нафтогазпромбуд» має базуватись на поєднанні сучасних технологічних рішень, управлінських підходів і нормативного регулювання. Для приватного підприємства, яке оперує великими масивами інформації, критично важливо сформувати стійку архітектуру безпеки, що гарантує безперервність бізнес-процесів навіть у разі кібератак чи технічних збоїв. Центральним завданням є створення інтегрованої системи кіберзахисту, яка поєднує моніторинг, попередження, реагування та відновлення після інцидентів. Такий підхід дозволяє не лише виявляти загрози, а й запобігати їм на ранніх етапах [65].

Передусім варто модернізувати політику управління доступом до архівних ресурсів. Необхідно впровадити багатофакторну автентифікацію, яка поєднує пароль, токен і біометричну перевірку. Це мінімізує ризик

компрометації облікових записів, особливо у випадках віддаленої роботи. Система має підтримувати принцип «мінімальних прав» — кожен користувач отримує лише ті дозволи, що відповідають його посадовим обов'язкам. Це запобігає внутрішнім витокам і несанкціонованим змінам у даних. Для підвищення прозорості доступу слід запровадити централізований аудит усіх дій користувачів у системі. Усі спроби входу, копіювання чи редагування файлів мають автоматично фіксуватися в журналі подій. Аналітичний модуль дозволятиме виявляти підозрілі дії, наприклад масові спроби доступу або несанкціоноване копіювання великих обсягів даних. Такі механізми створюють цифровий «слід довіри», що забезпечує підзвітність і контроль [65].

Для захисту даних на рівні зберігання необхідно впровадити сучасні методи шифрування. Оптимальним рішенням стане використання симетричного шифрування AES-256 для локального зберігання та асиметричного RSA для передачі інформації [62]. Це гарантує, що навіть у випадку фізичного доступу до носіїв дані залишаться недоступними для сторонніх осіб. Усі резервні копії архіву мають зберігатися в зашифрованому вигляді із застосуванням різних ключів доступу. Особливої уваги потребує захист даних під час їх передавання між внутрішніми підрозділами підприємства. Для цього рекомендується використовувати протоколи захищеного зв'язку SSL/TLS та VPN-тунелі для віддалених підключень. Така система гарантує, що інформація не буде перехоплена або модифікована під час передавання [64].

Сучасна система безпеки має бути побудована за принципом Zero Trust, що означає, що навіть внутрішні користувачі мають проходити автентифікацію при кожному зверненні до ресурсу. Впровадження такого підходу мінімізує наслідки компрометації облікових даних і знижує ризик внутрішніх загроз. Для підвищення стійкості системи варто запровадити багаторівневу архітектуру захисту: мережевий рівень (фаєрволи, IDS/IPS-системи), прикладний (контроль дій користувачів, фільтрація запитів), і рівень

даних (шифрування, токенізація, контроль цілісності). Така модель дозволяє ізолювати загрози й локалізувати інциденти без порушення роботи всієї системи.

Окремим елементом має стати система управління вразливостями, яка регулярно сканує архівну інфраструктуру на наявність потенційних слабких місць. Її поєднання з автоматизованим оновленням програмного забезпечення забезпечить постійний контроль за безпекою серверів і баз даних. Для підприємства, яке працює з великими обсягами персональних даних, надзвичайно важливо впровадити інструменти анонімізації та псевдонімізації даних. Це означає, що особисті відомості можуть бути тимчасово приховані або замінені умовними ідентифікаторами при роботі з аналітичними звітами чи тестуванням систем. Такий підхід дозволяє виконувати внутрішні процеси без порушення конфіденційності [64].

Ключовою умовою ефективного захисту є розроблення внутрішньої політики безпеки, яка визначає порядок зберігання, оброблення, передавання та видалення персональних даних. Ця політика має містити опис відповідальності кожного працівника, алгоритми реагування на інциденти та порядок проведення внутрішніх перевірок. Удосконалення системи безпеки передбачає створення центру моніторингу інформаційних подій (SOC), який у режимі реального часу аналізуватиме журнали активності, стан серверів, мережеві з'єднання та сигнали безпеки. SOC дозволить підприємству не лише фіксувати атаки, а й оперативно реагувати на них, ізолюючи потенційні загрози [62].

Варто також впровадити систему резервного копіювання з функцією версіонування. Це дозволяє зберігати історію змін файлів і відновлювати дані в попередньому стані у випадку втрати або шифрування зловмисниками. Резервні сервери мають бути фізично відокремлені від основної інфраструктури. Особливу роль у забезпеченні кібербезпеки відіграє регулярне тестування на проникнення. Такі перевірки, проведені внутрішніми фахівцями або зовнішніми аудиторами, дозволяють оцінити стійкість архівної

системи до реальних атак і виявити слабкі місця до того, як ними скористаються зловмисники [62].

Не менш важливим напрямом є створення системи безперервного навчання персоналу. На підприємстві слід впровадити програму підвищення цифрової грамотності працівників, що охоплює основи інформаційної безпеки, правила створення складних паролів, методи захисту електронних підписів і розпізнавання фішингових повідомлень. Інформаційна безпека повинна стати частиною корпоративної культури. Для посилення правового захисту варто впровадити практику укладання угод про нерозголошення (NDA) з усіма працівниками, які мають доступ до персональних даних. Такі угоди формують правові межі використання інформації та забезпечують додаткову дисципліну при роботі з архівом [62].

Із метою мінімізації ризиків витоку інформації слід застосовувати технологію DLP (Data Loss Prevention), яка контролює всі канали передачі даних і блокує спроби несанкціонованого копіювання або відправлення конфіденційної інформації. Це особливо важливо для підприємств, де документи можуть містити технічні або комерційні таємниці. Для зміцнення захисту електронного архіву від кібератак доцільно інтегрувати аналітичні системи на базі штучного інтелекту, що аналізують поведінкові патерни користувачів і мережеві аномалії. Така система здатна виявляти відхилення від звичайної активності та автоматично блокувати потенційні загрози [62].

Окремим напрямом удосконалення є створення плану реагування на інциденти безпеки (Incident Response Plan). У ньому повинні бути визначені відповідальні особи, порядок дій у разі атаки, канали комунікації та правила відновлення роботи архіву. Регулярне тестування цього плану дозволить перевірити готовність персоналу до кризових ситуацій. ПП «ВК Нафтогазпромбуд» доцільно впровадити сертифікацію інформаційної системи відповідно до міжнародних стандартів ISO/IEC 27001 [12]. Це забезпечить системний підхід до управління безпекою, підвищить рівень довіри з боку

партнерів і замовників, а також сприятиме участі підприємства в міжнародних тендерах.

Необхідно також розробити процедури знищення персональних даних після закінчення терміну їх зберігання. Така функція може бути реалізована автоматично, із формуванням електронного акта видалення, який підтверджує дотримання законодавчих вимог. Для посилення фізичного захисту архівних серверів слід передбачити контроль доступу до приміщень, відеоспостереження, датчики руху та системи пожежогасіння. Усі серверні кімнати мають бути обладнані резервним живленням і кліматичним контролем для стабільної роботи обладнання. Важливою складовою є аудит постачальників ІТ-послуг, адже у сучасних умовах частина процесів може виконуватись на аутсорсингу. Підприємство повинно укладати контракти лише з тими партнерами, які дотримуються високих стандартів безпеки та мають відповідні сертифікати [12].

Щоб підвищити рівень захисту баз даних, варто застосовувати механізми маскування конфіденційної інформації при тестуванні чи розробці програмних оновлень. Це унеможливить витік реальних даних під час експериментів або технічного обслуговування. Система безпеки повинна мати адаптивний характер — реагувати на зміни загроз у реальному часі. Для цього доцільно впровадити аналітичні панелі (dashboards), які відображають стан архіву, активність користувачів і поточний рівень ризику. Такі інструменти дозволять керівництву оперативно приймати рішення.

Окрім технічних заходів, важливу роль відіграє створення етичної політики поводження з інформацією. Працівники мають усвідомлювати, що персональні дані — це не лише службовий ресурс, а й частина прав людини, яку необхідно захищати. У перспективі ПП «ВК Нафтогазпромбуд» може розглянути можливість використання блокчейн-технологій для забезпечення цілісності архівних даних [3]. Розподілений реєстр дозволить створити незмінний цифровий слід кожної операції з документом, що підвищить рівень довіри до системи.

Загалом комплексна система захисту електронного архіву повинна бути гнучкою, масштабованою і постійно вдосконалюватися. Поєднання сучасних технологій — штучного інтелекту, шифрування, блокчейну, аналітики великих даних — створює основу для стійкої інформаційної екосистеми підприємства. Реалізація зазначених заходів дозволить ПП «ВК Нафтогазпромбуд» не лише зміцнити безпеку персональних даних, а й підвищити загальний рівень корпоративної культури управління інформацією. Комплексна система захисту стане запорукою стабільності бізнесу, довіри партнерів і конкурентної переваги у сучасному цифровому середовищі.

3.3. Перспективи розвитку електронного архівування в Україні: сучасні технологічні рішення та рекомендації для підприємства

У сучасних умовах цифрової трансформації електронне архівування - один із ключових напрямів модернізації системи управління діловою документацією на приватних підприємствах. Зростання обсягів інформації, що створюється у цифровому форматі, зумовлює потребу в розробленні ефективних технологічних рішень для її зберігання, захисту та швидкого доступу. Для приватних підприємств, зокрема таких, як ПП «ВК Нафтогазпромбуд», це відкриває перспективи оптимізації внутрішніх процесів, підвищення інформаційної безпеки та зменшення адміністративних витрат [3].

Перш за все, однією з головних тенденцій розвитку електронного архівування є поступовий перехід до хмарних технологій. Використання хмарних сховищ дозволяє підприємствам забезпечити доступ до архівних документів у режимі реального часу, незалежно від місця перебування працівників. У контексті воєнного стану це має особливе значення, оскільки зменшує ризики втрати критично важливої інформації через фізичне знищення офісів або серверів. Хмарні рішення, що підтримують шифрування даних і багаторівневу автентифікацію, стають запорукою кіберстійкості архівної

системи [61]. Наступним перспективним напрямом є впровадження систем електронного документообігу з функцією автоматизованого архівування.

Такі системи забезпечують автоматичну класифікацію документів, створення метаданих, а також контроль термінів зберігання. Для ПП «ВК Нафтогазпромбуд» це може означати перехід від фрагментарного зберігання документів до цілісної інформаційної екосистеми. Застосування програмного забезпечення на зразок «M.E.Doc», «Вчасно» чи «BAS Документообіг» дає змогу інтегрувати архів із бухгалтерськими та управлінськими системами [64]. Важливою тенденцією є також використання технологій блокчейн для підтвердження автентичності документів. Завдяки децентралізованому зберіганню записів блокчейн може гарантувати незмінність архівних даних і захист від несанкціонованих змін. Для приватного підприємства це створює можливості зменшити ризики внутрішнього шахрайства та втрат доказової сили документів.

У перспективі особливої актуальності набуде впровадження штучного інтелекту в системи електронного архівування. Алгоритми машинного навчання здатні автоматично розпізнавати типи документів, вилучати ключову інформацію та прогнозувати терміни зберігання. Такі функції дозволяють скоротити витрати часу на ручну обробку архівів та підвищити точність пошуку інформації. Серед технологічних трендів майбутнього варто також відзначити використання електронного підпису та цифрової ідентифікації як базових елементів електронного архіву. Вони не лише забезпечують юридичну силу електронних документів, але й спрощують процеси внутрішнього погодження та затвердження. Для ПП «ВК Нафтогазпромбуд» інтеграція системи електронного підпису може стати важливим етапом у підвищенні прозорості бізнес-процесів [3].

У контексті воєнного стану питання надійності архівних рішень набуває стратегічного значення. Часті кібератаки, перебої в електропостачанні та ризики фізичного знищення серверів змушують підприємства шукати стійкі та розподілені системи зберігання даних. Для мінімізації ризиків доцільно

застосовувати гібридні архітектури — поєднання локальних серверів із хмарними сховищами. Це дозволяє зберігати копії найважливіших документів у безпечних дата-центрах поза зоною бойових дій. Важливо також розвивати нормативно-правове забезпечення електронного архівування на рівні приватного сектору [64]. Підприємства мають розробляти внутрішні положення, що регламентують створення, класифікацію, зберігання та знищення електронних документів. Документи повинні узгоджуватися із Законом України «Про електронні документи та електронний документообіг» та іншими актами у сфері захисту інформації [17].

Не менш перспективним напрямом є підвищення рівня цифрової грамотності працівників. Без належної підготовки персоналу навіть найсучасніші технологічні рішення можуть залишатися неефективними. Тому ПП «ВК Нафтогазпромбуд» доцільно впроваджувати регулярне навчання з питань кібергігієни, роботи з електронними архівами та застосування цифрових інструментів управління документацією [3]. У середньостроковій перспективі розвиток електронного архівування сприятиме не лише внутрішній оптимізації підприємства, але й його конкурентоспроможності на ринку. Наявність сучасної архівної системи дозволяє швидко надавати звітність партнерам і контролюючим органам, що підвищує довіру до компанії. Крім того, цифрове архівування дає змогу зберігати історію підприємства як елемент його корпоративної культури та репутаційного капіталу.

Отже, перспективи розвитку електронного архівування в Україні, особливо для приватних підприємств, є багатовимірними й тісно пов'язаними з цифровою трансформацією економіки. Сучасні технології — хмарні рішення, блокчейн, штучний інтелект, електронний підпис — формують основу для створення надійних, безпечних і гнучких архівних систем [43, с.548]. Для ПП «ВК Нафтогазпромбуд» це відкриває шлях до підвищення ефективності управління інформаційними потоками, мінімізації ризиків у воєнний час та забезпечення стабільності ділової діяльності. У довгостроковій

перспективі впровадження таких рішень сприятиме формуванню нової культури документування, де архів стає не просто сховищем, а інтелектуальним ресурсом розвитку підприємства.

Відмовлення від паперових носіїв та перехід до електронних форматів документів на Підприємстві сприяв формуванню нової культури архівування, орієнтованої на ефективність, безпеку й довготривале зберігання даних. Для ПП «ВК Нафтогазпромбуд» це і надалі відкриває можливості удосконалення внутрішніх процесів, підвищення оперативності управлінських рішень і зміцнення інформаційної стійкості підприємства [3]. Насамперед перспективи розвитку електронного архівування пов'язані з використанням хмарних технологій. Хмарні платформи дозволяють Підприємству відмовитися від утримання локальних серверів і забезпечити безперервний доступ до архівів через мережу Інтернет. Такий підхід особливо актуальний у період воєнного стану, коли існують ризики знищення фізичної інфраструктури. Хмарні сервіси, зокрема Google Workspace, Microsoft 365 чи українські рішення на базі «De Novo» та «Трембіта», пропонують надійне шифрування та резервне копіювання даних. Це знижує ризики втрати документів і спрощує процес відновлення інформації у разі аварій або кібератак [13].

На нашу думку, ПП «ВК Нафтогазпромбуд» доцільно впровадити гібридну архітектуру зберігання даних, що поєднує локальні сервери для оперативної роботи та хмарні сховища для архівного збереження. Такий підхід забезпечить баланс між швидкістю доступу, безпекою й контролем над інформацією. Крім того, сучасні хмарні технології дозволяють налаштовувати розмежування прав доступу, що важливо для дотримання конфіденційності службової документації. Подальшим напрямом є впровадження інтелектуальних систем управління документами, що автоматизують архівні процеси. Вони дозволяють здійснювати повнотекстовий пошук документів, автоматично формувати індекси та метадані, контролювати строки зберігання.

Для Підприємства це означає значне зниження трудових витрат на ручну обробку документів. згадувані нами вище у підрозділі програмні рішення на

зразок «BAS Документообіг», «Вчасно», або «DocsVision» можуть бути адаптовані під структуру підприємства, інтегровані з бухгалтерськими програмами та CRM-системами [13]. Важливою технологічною тенденцією є впровадження блокчейн-технологій у систему електронного архівування. Завдяки незмінності записів у блокчейні можна гарантувати автентичність документів та унеможливити їхнє несанкціоноване редагування. Це особливо актуально для договорів, фінансових звітів і технічної документації, що потребують збереження доказової сили. Використання приватного блокчейну дає змогу створювати журнал подій архіву, де фіксуються всі зміни, що відбуваються з документами.

Ще одним перспективним напрямом є інтеграція штучного інтелекту у процес електронного архівування. Алгоритми AI можуть автоматично класифікувати документи за типами, розпізнавати текст за допомогою технології OCR, визначати рівень важливості інформації та пропонувати оптимальні терміни зберігання [43, с.549]. Це дозволяє скоротити людський фактор і мінімізувати ризики помилок під час архівування. Наприклад, система може розпізнати акт виконаних робіт, автоматично внести його до відповідного розділу архіву та пов'язати з договором підряду. Сучасні технології також передбачають застосування електронного підпису та цифрової ідентифікації як невід'ємних елементів електронного архіву. В Україні вже функціонує розвинена інфраструктура кваліфікованих електронних довірчих послуг, що забезпечує юридичну значущість електронних документів. Використання електронного підпису у ПП «ВК Нафтогазпромбуд» дозволить пришвидшити погодження документів і зменшити час між етапами документообігу [3].

Паралельно з цим доцільно впровадити систему мультифакторної автентифікації, щоб запобігти несанкціонованому доступу до архівних даних. У поєднанні з шифруванням це створить високий рівень захисту інформації. Такі заходи відповідають європейським стандартам інформаційної безпеки ISO/IEC 27001 [12]. Важливою складовою розвитку електронного архівування

є створення корпоративного нормативного середовища. Підприємству варто розробити Положення про електронний архів, Інструкцію з діловодства в електронній формі та Регламент з резервного копіювання. Документи повинні регулювати етапи створення, обробки, зберігання, передачі та знищення електронних документів. Наявність чітких внутрішніх правил сприяє підвищенню дисципліни інформаційних процесів і забезпечує юридичну чистоту операцій з документами. У межах організаційного розвитку ПП «ВК Нафтогазпромбуд» варто створити постійну комісію з питань архівування електронних документів [3]. До її складу можуть входити представники IT-відділу, бухгалтерії та адміністрації. Комісія має контролювати стан архівних баз, забезпечувати відповідність нормативним вимогам і впроваджувати нові технологічні рішення.

З метою підвищення ефективності роботи архіву доцільно проводити регулярні аудити інформаційної безпеки. Перевірка стану резервного копіювання, тестування систем доступу та оцінка стійкості до кіберзагроз допоможуть уникнути інцидентів втрати даних. В умовах війни такі заходи мають не лише технічне, а й стратегічне значення, адже інформаційні системи стають об'єктом постійних атак [60]. Окремо слід звернути увагу на навчання персоналу, адже жодна технологія не буде ефективною без кваліфікованих користувачів. Рекомендовано проводити тренінги з цифрової грамотності, основ кібергігієни, правил роботи з електронними архівами. Це дозволить уникнути помилок при завантаженні, класифікації чи передачі документів. У перспективі ПП «ВК Нафтогазпромбуд» може розглянути можливість інтеграції архівної системи з державними електронними реєстрами. Це дасть змогу оперативно отримувати інформацію про контрагентів, дозволи, ліцензії, не виходячи з корпоративного середовища. Така інтеграція відповідає стратегії розвитку цифрової держави «Дія» [7].

Ще одним напрямом розвитку є впровадження аналітичних модулів у систему архівування, які дозволяють аналізувати динаміку документообігу. За допомогою таких інструментів можна відстежувати, які типи документів

створюються найчастіше, які підрозділи генерують найбільші обсяги інформації, де виникають затримки в обробці. Ці дані допомагають керівництву приймати обґрунтовані управлінські рішення. В умовах глобальної цифровізації важливо розвивати систему електронного зберігання технічної документації. Для ПП «ВК Нафтогазпромбуд», яке працює в галузі будівництва та енергетики, актуальним є оцифрування креслень, проєктів, технічних звітів. Використання форматів PDF/A та XML гарантує довготривале зберігання таких документів без втрати якості. Підприємству варто звернути увагу на перспективи використання технологій віртуалізації. Віртуальні сервери дозволяють розгортати архівні середовища у безпечних дата-центрах, що підвищує рівень стійкості до зовнішніх загроз. У поєднанні з системами моніторингу це забезпечує цілодобовий контроль за станом архіву [43, с.566].

Для ефективної взаємодії структурних підрозділів підприємства доцільно створити єдиний інформаційний портал, що поєднує функції архіву, документообігу та комунікації. На цьому порталі працівники зможуть завантажувати, погоджувати й архівувати документи в одному середовищі. Це сприятиме скороченню часу на виконання внутрішніх процедур. Суттєвим чинником подальшого розвитку електронного архівування стане гармонізація національних стандартів з міжнародними нормами, зокрема MoReq2010, ISO 15489 та ISO 16175 [10]. Впровадження цих стандартів забезпечить сумісність українських рішень із глобальними системами електронного архівування. (59)

У довгостроковій перспективі можна очікувати, що електронні архіви перетворяться на інтелектуальні сховища знань, які не лише зберігають документи, а й генерують аналітичні звіти, рекомендації та прогнози. Такі системи сприятимуть формуванню корпоративної пам'яті підприємства. Для реалізації вищезазначених напрямів ПП «ВК Нафтогазпромбуд» доцільно розробити дорожню карту цифрової трансформації архіву [3]. У ній слід визначити етапи модернізації, технічні вимоги, терміни впровадження та відповідальних осіб. Планування має відбуватися з урахуванням фінансових

можливостей підприємства та поступового оновлення інфраструктури. Важливим завданням стане оцінка економічної ефективності впровадження електронного архіву. Необхідно проаналізувати потенційне скорочення витрат на друк, папір, оренду приміщень для архівів та трудові ресурси. (66) Зазвичай ефект від переходу на електронне архівування проявляється вже протягом перших двох років після впровадження.

У перспективі розвитку електронного архівування слід також враховувати психологічний аспект сприйняття цифрових технологій працівниками. Важливо формувати позитивне ставлення до цифрових змін через інформаційні кампанії, внутрішні консультації та підтримку користувачів. Отже, можливості розвитку електронного архівування на приватних підприємствах, зокрема на ПП «ВК Нафтогазпромбуд», є надзвичайно широкими [3]. Використання сучасних технологічних рішень забезпечує стійкість до зовнішніх викликів, гнучкість у роботі та прозорість управлінських процесів.

Ефективне електронне архівування сприяє не лише економії ресурсів, але й зміцненню ділової репутації підприємства, що демонструє високий рівень організації внутрішніх процесів. Подальший розвиток цифрових технологій архівування перетворюватиметься на стратегічний інструмент управління знаннями. Завдяки цьому архів може виконувати роль центру збереження не лише документів, а й досвіду, аналітики та корпоративної історії. Тобто, сучасні технологічні рішення у сфері електронного архівування формують підґрунтя для створення гнучких, безпечних і високоефективних систем управління інформацією. Запровадження таких інновацій дозволить підприємству зберігати дані безпечно, швидко обробляти інформаційні потоки та приймати рішення на основі достовірних даних. У результаті електронне архівування стане невід'ємною частиною системи стратегічного управління підприємством. Його розвиток визначатиме не лише рівень технологічної зрілості компанії, а й її готовність до викликів майбутнього.

ВИСНОВКИ

У результаті проведеного дослідження нами було досягнуто мети магістерської роботи, що полягала у комплексному аналізі процесів електронного архівування ділової документації в установах та організаціях на прикладі ПП «ВК Нафтогазпромбуд» та розробленні практичних рекомендацій щодо їх удосконалення. У роботі послідовно вирішено поставлені завдання, що дозволило сформувати цілісне уявлення про правові, організаційні та технологічні аспекти електронного архівування. Проведений аналіз нормативно-правових засад електронного документообігу в Україні показав, що законодавча база поступово гармонізується з європейськими стандартами, зокрема Регламентом ЄС № 910/2014 (eIDAS), проте залишається потреба у вдосконаленні механізмів практичної реалізації норм. Визначено, що основними проблемами у сфері електронного архівування є недостатня уніфікація технічних стандартів, обмеженість доступу до якісних довірчих послуг, фрагментарність підзаконних актів та слабка інтеграція між державними інформаційними системами.

У процесі здійснення порівняльного аналізу українського та міжнародного законодавства з'ясовано, що провідні країни світу — США, Канада, Велика Британія, Німеччина, Франція — вже мають усталені моделі правового регулювання електронного архівування, побудовані на стандартах ISO 14721 (OAIS), ISO 15489, ISO 30301, MoReq. В Україні ж ці стандарти адаптовані, що створює потребу у розробленні національних методичних рекомендацій, узгоджених із міжнародною практикою. Підтверджено, що запровадження єдиної системи електронного архівування сприятиме забезпеченню автентичності, цілісності та довготривалого збереження документів, а також підвищить ефективність управлінської діяльності вітчизняних підприємств.

Дослідження особливостей електронного архівування ділової документації на прикладі ПП «ВК Нафтогазпромбуд» показало, що

підприємство вже активно впроваджує сучасні системи електронного документообігу, однак процес архівування потребує подальшої оптимізації. Виявлено проблеми, пов'язані з недостатнім рівнем автоматизації, відсутністю централізованого сховища даних, недосконалою системою резервного копіювання та обмеженою інтеграцією з хмарними сервісами. Аналіз діловодних процесів засвідчив, що частина документів досі зберігається у змішаному — паперово-електронному форматі, що створює ризики втрати інформації та ускладнює контроль за життєвим циклом документів.

На основі дослідження розроблено рекомендації щодо удосконалення системи електронного архівування на підприємстві, які передбачають впровадження централізованої платформи управління документами з функціями пошуку, ідентифікації, класифікації, автоматичного резервного копіювання та моніторингу доступу. Запропоновано використання технологій шифрування даних та багаторівневої аутентифікації користувачів, що забезпечить високий рівень інформаційної безпеки. Визначено необхідність розроблення внутрішнього нормативного акта, який регламентуватиме процеси створення, оброблення, зберігання, передавання та знищення електронних документів.

У процесі дослідження електронного архівування в умовах воєнного стану було встановлено, що питання кіберзахисту та резервного копіювання мають критичне значення для стабільності функціонування підприємств. Виявлено, що відсутність єдиної державної системи резервних центрів зберігання даних збільшує ризики втрати важливої інформації у випадку технічних збоїв або кібератак. Запропоновано створення захищеного хмарного сховища на базі сертифікованих дата-центрів, що відповідають вимогам ISO/IEC 27001, із можливістю дублювання архівів на альтернативних майданчиках.

Важливим результатом дослідження стало виявлення залежності між рівнем нормативно-правового регулювання та ефективністю впровадження електронних архівних систем. Підтверджено, що чітка правова основа є

передумовою для створення надійної інфраструктури електронного архівування, яка гарантує автентичність, довіру та юридичну силу електронних документів. Проведений порівняльний аналіз свідчить, що Україні необхідно посилити стандартизацію метаданих, форм документів та форматів зберігання відповідно до міжнародних вимог, зокрема OAIS та PDF/A.

Наукова новизна одержаних результатів полягає у комплексному підході до вивчення електронного архівування як багаторівневої системи, що поєднує правові, організаційні та технічні механізми збереження інформації. У роботі запропоновано модель удосконалення електронного архіву підприємства, яка базується на принципах інтегрованості, безперервності, автентичності та захищеності даних. Розроблені рекомендації спрямовані на практичне підвищення ефективності документообігу, зниження ризиків втрати інформації та зміцнення довіри до електронних ресурсів.

У роботі доведено, що електронне архівування є не лише технічним процесом, а й важливим елементом управлінської культури, який визначає якість прийняття рішень і правову захищеність організації. Підприємствам рекомендовано розробляти власні політики електронного архівування, інтегровані в загальну систему інформаційної безпеки, а також здійснювати постійний моніторинг стану збереженості цифрових документів. Застосування сучасних архівних технологій дозволить підвищити ефективність діловодства, скоротити витрати часу та ресурсів, а також забезпечити довгостроковий доступ до даних.

У результаті проведеного аналізу встановлено, що в Україні вже сформовано базові передумови для створення національної системи електронного архівування, однак необхідна координація дій між державними органами, архівними установами та приватним сектором. Підвищення рівня інформаційної культури працівників та підготовка фахівців з архівної справи нового покоління є важливою умовою для ефективного функціонування електронних архівів. Теоретичне значення результатів дослідження полягає в

уточненні понять «електронний архів», «електронне архівування» та «електронна ділова документація» у контексті сучасного правового поля України. Практичне значення визначається можливістю застосування отриманих висновків для модернізації архівних процесів у державних та приватних структурах, розроблення навчальних курсів із цифрової архівної справи та створення методичних матеріалів для працівників діловодства.

Підсумовуючи результати, слід зазначити, що всі поставлені завдання дослідження виконано. Проаналізовано правові засади електронного документообігу в Україні та міжнародний досвід його регулювання, охарактеризовано систему діловодства ПП «ВК Нафтогазпромбуд», визначено особливості електронного архівування на підприємстві, з'ясовано проблеми захисту персональних даних і подано практичні рекомендації з їх вирішення. Визначено перспективи розвитку електронного архівування в Україні, зокрема впровадження хмарних технологій, систем штучного інтелекту для класифікації документів та формування національного електронного архівного простору.

Отже, загальні висновки роботи свідчать, що ефективне електронне архівування є ключовою умовою цифрової трансформації управлінської діяльності. Його впровадження забезпечує прозорість, безперервність і надійність інформаційних процесів, сприяє підвищенню рівня правової культури в організаціях і створює передумови для інтеграції України у світовий інформаційний простір. Розвиток цієї сфери відкриває нові можливості для оптимізації діловодства, зміцнення інформаційної безпеки та формування надійної цифрової платформи держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. AES шифрування: надійний захист цифрових даних. URL: https://avolutech.com/blog/aes. (дата звернення: 22.10.2025)

2. Акуленко В. І. Міжнародне право охорони культурних цінностей та його імплементація у внутрішньому праві України: монографія /НАН України, Ін-т держави і права ім. В. М Корецького. Київ, 2019. 616 с.

3. ВК НАФТОГАЗПРОМБУД, ПП. URL: https://www.ua-region.com.ua/33661328 (дата звернення: 20.10.2025)

4. Дашко І. В., Михайліченко Л. О. Особливості використання штучного інтелекту в діяльності підприємств. Сталий розвиток економіки. №2. 2024. URL: https://www.semanticscholar.org/paper/16f903385e242c5fe377a77cb9b70e57d974a767 (дата звернення: 31.10.2025)

5. Держава в смартфоні: що це та які переваги для бізнесу і громадян? URL: https://intelserv.net.ua/news/material/id/623 (02.10.2025)

6. Державний класифікатор управлінської документації ДК 010-98. Документ v1024217-98, втратив чинність, поточна редакція — скасування від 19.04.2021, підстава - v0526915-21. URL: https://zakon.rada.gov.ua/rada/show/v1024217-98#Text (дата звернення: 28.09.2025)

7. Дія: Цифрова держава. URL: https://ua/projects/diya-cifrova-derzhava#:~:text=%D0%9A% (дата звернення: 18.09.2025)

8. Документне забезпечення управлінської діяльності організацій : навч.-метод. посіб. / уклад. О. В. Попчук; Рівнен. держ. гуманітар. ун-т. Рівне, 2016. 116 с.

9. ДСТУ 4163 – 2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. URL: https://buhgalter.com.ua/upload/news/2021/9/DSTU_4163.pdf (дата звернення: 09.09.2025)

10. ДСТУ ISO 15489-1:2018. (ISO 15489-1:2016, IDT). Інформація та документація. Керування записами. Частина 1. Поняття та принципи. Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») Наказ від 05.12.2018 № 464. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_15489-1_2018.pdf (дата звернення: 15.09.2025)

11. ДСТУ 4423-2:2005. Частина 2. Настанови Інформація та документація (ISO/TR 15489-2:2001, MOD). Керування документаційними процесами. Київ: Держспоживстандарт України. 2007. 44 с.

12. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 26.10.2025)

13. Єдиний державний веб-портал електронних послуг «ДІЯ». URL: https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia (дата звернення: 31.10.2025)

14. Закон України «Про адміністративні послуги». Документ 5203-VI, чинний, поточна редакція — редакція від 01.01.2025, підстава - 4170-IX, 3586-IX.URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text (дата звернення: 01.10.2025)

15. Закон України «Про доступ до публічної інформації» 2939-VI, редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text(дата звернення: 23.10.2024)

16. Закон України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 18.09.2025)

17. Закон України «Про електронні документи та електронний документообіг». Документ 851-IV, чинний, поточна редакція — редакція від

31.12.2023, підстава - 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 28.09.2025)

18. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». Документ 2155-VIII, чинний, поточна редакція — редакція від 18.12.2024, підстава - 3911-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 28.09.2025)

19. Закон України «Про затвердження Указу Президента України "Про введення надзвичайного стану в окремих регіонах України"» 2101-IX, від 23. 02. 2022. URL: https://zakon.rada.gov.ua/laws/show/2101-20#Text (дата звернення: 19.09.2025)

20. Закон України «Про захист персональних даних» 2297-VI від 16.09.2022. Документ 2297-VI, чинний, поточна редакція — редакція від 14.06.2025, підстава - 4240-IX. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 19.09.2025)

21. Закон України «Про захист інформації в автоматизованих системах». Документ 80/94-ВР, чинний, поточна редакція — редакція від 20.04.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.11.2025)

22. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Документ 80/94-ВР, чинний, поточна редакція — редакція від 20.04.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.09.2025)

23. Закон України «Про інформацію». Документ 2657-XII, чинний, поточна редакція — редакція від 14.06.2025, підстава - 4240-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 29.09.2025)

24. Закон України «Про Національний архівний фонд та архівні установи». Документ 3814-XII, чинний, поточна редакція — редакція від 21.06.2024, підстава - 3683-IX. URL: https://zakon.rada.gov.ua/laws/show/3814-12#Text (дата звернення: 03.11.2025)

25. Закон України «Про критичну інфраструктуру». Документ 1882-IX, чинний, поточна редакція — редакція від 21.09.2024, підстава - 3931-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення6 21.10.2025)

26. Закон України «Про оборону України». Документ 1932-XII, чинний, поточна редакція — редакція від 09.07.2025, підстава - 4497-IX. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 21.10.2025)

27. Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII, чинний, поточна редакція — редакція від 19.10.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (21.10.2025)

28. Закон України «Про правовий режим надзвичайного стану» 1550-III . Документ 1550-III, чинний, поточна редакція — редакція від 18.05.2024, підстава - 3633-IX. URL: https://zakon.rada.gov.ua/laws/show/1550-14#Text(дата звернення: 27.09.2025)

29. Закон України «Про правовий режим воєнного стану» 389-VIII. Документ 389-VIII, чинний, поточна редакція — редакція від 14.05.2025, підстава - 4391-IX. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 27.09.2025)

30. Закон України «Про основні засади забезпечення кібербезпеки України». Документ 2163-VIII, чинний, поточна редакція — редакція від 20.04.2025, підстава - 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 27.09.2025)

31. Закон України «Про санкції». Документ 1644-VII, чинний, поточна редакція — редакція від 01.08.2025, підстава - 4537-IX. URL: https://zakon.rada.gov.ua/laws/show/1644-18#Text (дата звернення: 05.09.2025)

32. Захист від сучасних загроз: модель «нульової довіри». URL: https://www.microsoft.com/uk-ua/security/business/zero-trust (дата звернення: 22.10.2025)

33. Ковальська Л. А. Документ в діловодстві та архівній справі: комунікація інформаційної діяльності. Бібліотекознавство. Документознавство. Інформологія. 2021. № 3. С. 29–37.

34. Ковальова В. І., Михайленко Д. Г., Куц Н. В. Особливості реалізації процесу автоматизації діловодства на підприємствах України. Проблеми сучасних трансформацій. Серія: економіка та управління. 2025. (17). DOI: https://doi.org/10.54929/2786-5738-2025-17-04-10 (дата звернення: 31.10.2025)

35. Конституція України. Документ 254к/96-ВР, чинний, поточна редакція — редакція від 01.01.2020, підстава - 27-IX. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 05.09.2025)

36. Кукарін О. Б. Електронний документообіг та захист інформації : навч. посіб. Київ: НАДУ, 2015. 84 с.

37. Кучеренко І.А. Офіційно-ділова комунікація: чинні вимоги і стандарти: електронний навчальний курс. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2024. 70 с.

38. Наказ державної архівної служби України від 22.04.2019 № 40 «Про затвердження та впровадження методичних рекомендацій "Організація роботи архівних установ, заснованих фізичними та/або юридичними особами приватного права"». Документ v0040843-19, поточна редакція — прийняття від 22.04.2019. URL: https://zakon.rada.gov.ua/rada/show/v0040843-19#Text (дата звернення: 28.09.2025)

39. Наказ Міністерства юстиції України «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях» від 18.06.2015 № 1000/5. Документ z0736-15, чинний, поточна редакція — редакція від 30.11.2024, підстава - z1643-24. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 19.10.2025)

40. Наказ Міністерства юстиції України «Про затвердження Змін до Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання». Документ z1252-22, чинний, поточна редакція — прийняття від 14.10.2022. URL: https://zakon.rada.gov.ua/laws/show/z1252-22?utm#Text (дата звернення: 19.10.2025)

41. Наказ Міністерства юстиції України № 1000/5 від 18 червня 2015 року «Про затвердження Типової інструкції з діловодства в міністерствах, інших центральних органах виконавчої влади, місцевих державних адміністраціях». Документ z0736-15, чинний, поточна редакція — редакція від 30.11.2024, підстава - z1643-24. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 29.09.2025)

42. Наказ державної судової адміністрації України від 13.04.2018 № 168 «Про затвердження Концепції Єдиної судової інформаційно-телекомунікаційної системи». URL: https://zakon.rada.gov.ua/rada/show/v0168750-18#Text. (дата звернення: 28.09.2025)

43. Орлов О. В., Нестеренко В. О. Використання штучного інтелекту в документообігу: перспективи та виклики. State Formation. No. 1 (37)/2025. С. 548-568

44. Палеха Ю. Документування в підприємницькій сфері (зі зразками сучасних документів) : навч. посіб. Київ: Ліра-К, 2016. 512 с.

45. Постанова Кабінету Міністрів України «Деякі питання документування управлінської діяльності». Документ 55-2018-п, чинний, поточна редакція — редакція від 03.10.2025, підстава - 1003-2025-п. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text (дата звернення: 07.10.2025)

46. Постанова Верховної Ради України «Про прийняття за основу проєкту Закону України про внесення змін до Закону України "Про електронну ідентифікацію та електронні довірчі послуги" щодо

удосконалення окремих положень та забезпечення безперебійності надання електронних довірчих послуг». Документ 4202-IX, чинний, поточна редакція — прийняття від 09.01.2025. URL: https://zakon.rada.gov.ua/laws/show/4202-IX#Text (дата звернення: 13.09.2025)

47. Постанова Кабінету Міністрів України № 1453 від 28 жовтня 2004 року «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади». Документ 1453-2004-п, втратив чинність, поточна редакція — втрата чинності від 07.03.2018, підстава - 55-2018-п. URL: https://zakon.rada.gov.ua/laws/show/1453-2004-%D0%BF#Text (дата звернення: 12.10.2025)

48. Постанова Кабінету Міністрів України від 8 вересня 2016 р. № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів». Документ 606-2016-п, чинний, поточна редакція — Редакція від 03.10.2025, підстава - 1244-2025-п. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF#Text. (дата звернення: 27.09.2025)

49. Постанова Кабінету Міністрів України від 28 червня 2024 р. № 764 «Деякі питання електронної ідентифікації та електронних довірчих послуг». Документ 764-2024-п, чинний, поточна редакція — прийняття від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/764-2024-%D0%BF#Text (дата звернення: 28.09.2025)

50. Постанова Кабінету Міністрів України від 16 січня 2024 р. № 48 «Про внесення змін до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109». Документ 48-2024-п, чинний, поточна редакція — прийняття від 16.01.2024. URL: https://zakon.rada.gov.ua/laws/show/48-2024-%D0%BF#Text (дата звернення6 18.10.2025)

51. Приватне підприємство «ВК Нафтогазпромбуд». URL: https://clarity-project.info/edr/33661328 (дата звернення: 20.10.2025)

52. Про затвердження національного класифікатора НК 010:2021 та скасування національного класифікатора ДК 010-98. Документ v0526915-21, поточна редакція — прийняття від 12.03.2021. URL:

https://zakon.rada.gov.ua/rada/show/v0526915-21#Text (дата звернення: 27.09.2025)

53. Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС. Документ 984_016-14, чинний, поточна редакція — редакція від 18.10.2024, підстава - 9a3_001-22 URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 14.09.2025)

54. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації». Документ 67-2018-р, чинний, поточна редакція — редакція від 17.09.2020, підстава - 826-2020-п. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 14.09.2025)

55. Розпорядження Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках». Документ 1351-2024-р, чинний, поточна редакція — редакція від 14.07.2025, підстава - 704-2025-р. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (дата звернення: 14.09.2025)

56. Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні». Документ 649-2017-р, чинний, поточна редакція — прийняття від 20.09.2017. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (дата звернення: 14.09.2025)

57. Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні». Документ 386-2013-р, чинний, поточна редакція — прийняття від

15.05.2013. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (дата звернення: 28.09.2025)

58. Смірнов О. А., Конопліцька-Слободенюк О. К., Смірнов С. А., Буравченко К. О., Смірнова Т.В ., Поліщук Л. І. Інформаційна безпека в комп'ютерних мережах: навч. посіб. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.

59. Створіть свій план реагування на інциденти. URL: https://blog.colobridge.net/uk/2025/05/comprehensive-guide-steps-to-build-an-incident-response-plan-ua/#:~:text2 (дата звернення: 22.10.2025)

60. У 2024 році кількість кібератак на Україну зросла на 70%. URL: https://imi.org.ua/news/u-2024-rotsi-kilkist-kiberatak-na-ukrayinu-zrosla-na-70-i65931#:~:text (дата звернення6 10.09.2025)

61. Хмарні сервіси: як вони працюють та чому стали стандартом. URL: https://denovo.ua/resources/cloud-services-how-they-work (дата звернення: 01.11.2025)

62. Як побудувати та запустити центр безпеки (SOC). URL: https://oleg-dubetcky.medium.com/%D1%8F%D0%BAB8-soc-504266cefa53 (дата звернення: 22.10.2025)

63. April 1 - 5, 2024. Procedure for exchanging e-documents with control bodies has been clarified. URL: https://devisu.ua/en/stattia/01-05-kvitnya-2024-roku-utochneno-poryadok-obminu-e_dokumentami-z-kontrolyuyuchimi-organami. (дата звернення6 19.10.2025)

64. BAS документообіг. URL: https://www.ksoft.com.ua/index.php/bas/rishennia-dlia-korporatyvnoho-rynku/bas-dokumentoobih-korp?gad_source=1&gad_campaignid=22509748053&gbraid=0AAAAA-db05KRTK-AQuXkATArDx_-AEDqq&gclid (дата звернення: 28.10.2025)

65. DMS – Ефективні системи управління документами для бізнесу. URL: https://xpro.com.ua/dms-system (дата звернення: 27.10.2025)

66. Electronic Records at the National Archives. URL: https://www.archives.gov/research/electronic-records. (дата звернення: 15.09.2025).

67. ISO 14721:2025. URL: https://www.iso.org/ru/standard/87471.html (дата звернення: 01.10.2025)

68. ISO 23081-1:2017 Information and documentation — Records management processes — Metadata for records. URL: https://www.iso.org/ru/standard/73172.html (дата звернення: 02.10.2025)

69. ISO/IEC 27001. Система менеджменту інформаційної безпеки. URL: ertification.com.ua/iso27001?gad_source=1&gad_campaignid=22638344346&gbraid=0AAAAAo4yQR0_QLI5nfTYoLpagxVQgvybx&gclid=EAIaIQobChMIsb_KtZO3kAMVlZyDBx14PBFpEAAYASAAEgIervD_Bw (дата звернення: 22.10.2025)

70. The International Council on Archives (ICA). URL: https://www.ica.org/ (дата звернення: 02.10.2025)

71. United Nation E-Government Survey (2018). URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/ 2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf. (дата звернення6 01.10.2025)

72. National Archives Electronic Records Archives (ERA). URL: https://www.archives.gov/era. (дата звернення: 15.09.2025).

73. UNESCO. Charter on the Preservation of Digital Heritage. 15 October 2003. URL: http://portal.unesco.org/. (дата звернення: 10.09.2025)

74. Open Archival Information System. ruynzeel-storage.com/applications/archive?gad_source=1&gad_campaignid=19773949176&gbraid=0AAAAApONlvw4L9pAu9qhJQbkWD1UxSMFh&gclid=EAIaIQobChMI85TPjbyukAMVtxiiAx0olwXhEA (дата звернення: 01.10.2025)

75. Supreme court. URL: https://supreme.court.gov.ua/supreme/ (дата звернення6 19.10.2025)

76. Symantec Data Loss Prevention (DLP). URL: https://itbiz.ua/proizvoditeli/symantec/symantec-data-loss-prevention-dlp/#:~:text=Data%20Loss%20Prevention-,SYMANTEC%20DATA%20LOSS% (дата звернення: 22.10.2025)

ДОДАТКИ

Додаток А

(до підрозділу 1.3.)

Порівняльний аналіз українського та зарубіжного законодавства у сфері електронної ділової документації

(створено нами на основі аналізу нормативно-правової бази)

№	Країна / об'єднання	Назва нормативно-правового акта	Рік ухвалення / чинності	Ключові положення	Юридичне значення / сфера дії	Спільні риси з українським законодавством	Відмінності
1	**Україна**	Закон України «Про електронні документи та електронний документообіг» № 851-IV	2003 (чинний)	Визначає поняття електронного документа, принцип рівності електронної та паперової форми, порядок обігу, зберігання, підписання	Базовий акт, що заклав засади електронного документообігу в Україні	Встановлює рівноправ-ність електронного документа з паперовим, визначає реквізити та юридичну силу	Має загальний характер, не регулює детально довірчі послуги, інтеграцію з ЄС
2	**Україна**	Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII	2018	Регламентує електронний підпис, печатку, сертифікацію довірчих послуг, електронну ідентифікацію	Гармонізований із європейським Регламентом eIDAS	Встановлює довірчі послуги, електронну ідентифіка-цію та відповідальність провайдерів	Визнання довірчих послуг діє лише на національному рівні, часткове взаємовизнання з ЄС
3	**Україна**	Закон № 2801-IX «Про внесення змін … щодо укладення Угоди між Україною та ЄС про взаємовизнання кваліфікованих електронних довірчих послуг»	2022	Передбачає взаємне визнання кваліфікованих електронних підписів між Україною та ЄС	Крок до європейської інтеграції у сфері електронної ідентифікації	Узгоджується з eIDAS, забезпечує міжнародне визнання підписів	На етапі реалізації, потребує технічної інтеграції інфраструктур
4	**Європейський Союз**	Регламент (ЄС) № 910/2014 (eIDAS) «Про електронну ідентифікацію та довірчі послуги»	2016	Установлює єдині правила для електронної ідентифікації, підписів, печаток, довірчих послуг;	Основоположний документ ЄС у сфері електронної ідентифікації	Принцип рівності електронної та паперової форми, обов'язковість довірчих послуг	Має пряму дію в усіх державах-членах, забезпечує повне взаємовизнання

№	Країна / об'єднання	Назва нормативно-правового акта	Рік ухвалення / чинності	Ключові положення	Юридичне значення / сфера дії	Спільні риси з українським законодавством	Відмінності
				принцип взаємного визнання між країнами ЄС			
5	**ЄС**	Регламент (ЄС) 2024/1183 (оновлений eIDAS 2)	2024	Визначає створення Європей-ського цифрового гаманця (European Digital Identity Wallet), розширює спектр довірчих послуг	Розвиває систему eIDAS, закладає основу для цифрової ідентичності в межах ЄС	Аналогічна мета — уніфікація ідентифікації	Вищий рівень інтеграції, створює спільну електронну ідентичність
6	**Німеччина**	Gesetz über Vertrauensdienste (eIDAS-Durchführungsgesetz)	2017	Національне впровадження eIDAS, визначає нагляд за довірчими сервісами, стандарти безпеки	Забезпечує реалізацію eIDAS на національному рівні	Ідентичні принципи з українськими законами	Має розвинену інституційну систему контролю
7	**Франція**	Décret n° 2017-1416 «relatif à la signature électronique»	2017	Установлює рівність юридичної сили електронного підпису та традиційного	Сумісний із eIDAS, діє в публічному та приватному секторах	Визнає електронний підпис як доказ у суді	Вимагає сертифікації лише європейських провайдерів
8	**США**	Electronic Signatures in Global and National Commerce Act (E-SIGN Act)	2000	Визнає юридичну силу електрон-них підписів і документів у всіх штатах США	Федеральний рівень регулювання електронних документів	Аналогічна норма — рівність електронного документа	Інша технічна модель (менше централізован их довірчих послуг)
9	**Велика Британія**	Electronic Communications Act	2000	Регулює електронні підписи, шифрування, довірчі послуги	Основний закон після виходу з ЄС	Принцип рівності електронної форми документа	Не підпадає під eIDAS, але зберігає сумісність через двосторонні угоди

№	Країна / об'єднання	Назва нормативно-правового акта	Рік ухвалення / чинності	Ключові положення	Юридичне значення / сфера дії	Спільні риси з українським законодавством	Відмінності
10	**Україна / судова практика**	Закон № 3200-IX «Про внесення змін до … щодо обов`язкової реєстрації електронних кабінетів у ЄСІТС»	2023	Упроваджує електронну комуніка-цію між судами та учасниками процесу	Цифровізація судового документо-обігу	Аналогічно до європейських систем електронного судочинства	Наявна лише на національному рівні

Додаток Б

(до підрозділу 2.3.)

Ризики електронного архівування в умовах воєнного стану

(створено нами на основі аналізу нормативно-правової бази)

№	Категорія ризику	Сутність ризику	Ймовірність виникнення	Потенційний вплив на діяльність	Рівень ризику (низький/середній/ високий)	Заходи мінімізації ризику
1	**Технічний**	Фізичне знищення серверів або пошкодження дата-центрів унаслідок обстрілів	Висока	Повна втрата архівних даних і зупинка операційних процесів	Високий	Створення резервних копій у географічно розподілених сховищах; використання хмарних технологій
2	**Технічний**	Відключення електроенергії, перебої живлення	Висока	Тимчасова втрата доступу до архівів, збої в оновленні баз даних	Середній	Використання UPS, дизель-генераторів, альтернативних джерел живлення
3	**Технічний**	Пошкодження каналів зв`язку або втрати інтернет-доступу	Середня	Неможливість доступу до хмарних архівів або синхронізації копій	Середній	Наявність офлайн-резервів і локальних копій на фізичних носіях
4	**Кібернетичний**	Кібератаки, спроби шифрування або викрадення архівів	Висока	Компрометація даних, зупинка електронного документообігу	Високий	Використання сертифікованих засобів шифрування, багаторівневої авторизації, систем моніторингу подій
5	**Кібернетичний**	Несанкціонований доступ з боку працівників або зовнішніх осіб	Середня	Витік конфіденційної інформації, порушення цілісності архівів	Високий	Аудит дій користувачів, контроль доступу за ролями, політика безпеки паролів

6	**Організаційний**	Недостатня підготовка персоналу в сфері е-архівування	Висока	Помилки під час архівації, видалення або некоректне збереження документів	Середній	Проведення регулярних тренінгів, сертифікація працівників
7	**Організаційний**	Відсутність чіткої політики безперервності бізнес-процесів	Середня	Втрати часу при відновленні архівів, хаос у діях персоналу	Високий	Розроблення Плану аварійного реагування, інструкцій і алгоритмів відновлення даних
8	**Організаційний**	Людський фактор (внутрішній саботаж, помилки, халатність)	Середня	Знищення чи зміна даних, порушення архівної дисципліни	Високий	Контроль доступу, моніторинг активності, внутрішній аудит
9	**Юридичний / нормативний**	Втрата чинності електронних підписів або неможливість перевірки автентичності	Середня	Втрата юридичної сили документів, проблеми у звітності	Середній	Використання LTV-підписів, збереження метаданих і сертифікатів
10	**Системний**	Відсутність моніторингу стану архіву та тестування відновлення	Середня	Несвоєчасне виявлення пошкоджень архіву	Середній	Автоматичні перевірки цілісності, тестові відновлення, ведення журналів подій

Додаток В

(до підрозділу 2.3Рисунок матриці ризиків електронного архівування ПП «Нафтогазпромбуд»

(розроблено нами а основі аналізу джерел)