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 «БАКАЛАВР»
ЕЛЕКТРОННІ ДОКУМЕНТИ: ПРАВОВІ, ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ АСПЕКТИ

Здобувачки вищої освіти
Винник Марії Олександрівни
спеціальності «Інформаційна, бібліотечна та архівна справа»
Навчально-наукового інституту муніципального управління та міського господарства

_____
(підпис)

Науковий керівник:
доктор філософії, доцент Кучерявий Володимир Миколайович

_____
(підпис)

Національна шкала добре
Кількість балів 85
Оцінка: ECTS B

Київ – 2026

АНОТАЦІЯ

Винник Марія Олександрівна. **Електронні документи: правові, організаційні та технічні аспекти.**

У роботі розглядаються електронні документи їх правові, організаційні та технічні аспекти. Під час написання роботи було розглянуто теоретико-методологічні засади функціонування електронних документів; проаналізовано стан та особливості роботи з електронними документами у військовій частині Національної гвардії України; виявлено напрями оптимізації електронного документообігу в структурному підрозділі військової частини Національної гвардії України.

Ключові слова: електронний документообіг, військова частина, хмарні технології, кіберзахист, конфіденційність, документне забезпечення управління.

SUMMARY

Vynnyk Mariia Oleksandrivna. Electronic documents: legal, organizational and technical aspects.

The work examines electronic documents and their legal, organizational and technical aspects. During the writing of the work, the theoretical and methodological principles of the functioning of electronic documents were considered; the state and features of working with electronic documents in the military unit of the National Guard of Ukraine were analyzed; directions for optimizing electronic document flow in the structural unit of the military unit of the National Guard of Ukraine were identified.

Keywords: electronic document flow, military unit, cloud technologies, cyber security, confidentiality, document management.

ЗМІСТ

ВСТУП

Актуальність бакалаврської роботи обґрунтовано тим, що в умовах сучасної глобальної цифровізації перехід до електронного документообігу стає не просто технічним оновленням, а стратегічним пріоритетом для забезпечення національної безпеки та ефективності державного управління. Також, актуальність обраної теми дослідження зумовлена необхідністю радикальної трансформації традиційних методів роботи з інформацією у секторі безпеки та оборони України. Запровадження воєнного стану стало потужним каталізатором, що змусив військові формування оперативно адаптувати свої управлінські процеси до вимог цифрового середовища [33].

Сучасне безпекове середовище вимагає від військових підрозділів миттєвої реакції на виклики, що неможливо без використання захищених систем електронного документообігу [33]. Стан досліджуваної проблеми характеризується динамічним розвитком нормативно-правової бази, яка намагається встигнути за технологічним прогресом та новими загрозами кіберпростору. Обґрунтування доцільності розробки цієї теми полягає у потребі подолання суперечностей між застарілими паперовими регламентами та вимогами безпаперового офісу. Теоретичний фундамент дослідження базується на працях провідних вітчизняних та зарубіжних вчених, серед яких варто відзначити В. Бездрабко [1], С. Кулешова [17-18], Ю. Палехи [25-26], І. Шкіцької [54]. Тобто, науковців та вчених, які зробили вагомий внесок у розвиток теорії електронного документознавства, розкриваючи правові та організаційні аспекти функціонування цифрових об’єктів.

Проте, попри значну кількість наукових напрацювань, залишається низка недосліджених аспектів, зокрема питання довгострокового зберігання електронних документів у військових архівах. Потребують додаткового вивчення проблеми забезпечення цілісності та автентичності документів при їх міграції між різними відомчими системами в умовах нестабільного зв’язку. Теоретична значимість обраної теми підтверджується необхідністю уточнення

термінологічного апарату, зокрема розмежування понять електронного документа та його цифрової копії у контексті військового діловодства. Практична значимість дослідження полягає у формуванні конкретних рекомендацій щодо оптимізації роботи з системою «Док Проф» у специфічних умовах Національної гвардії України [9].

Стан вивченості питання свідчить про наявність значного правового вакууму щодо використання хмарних технологій для зберігання службової інформації з обмеженим доступом. Вивчення теми відкриває перспективи впровадження концепції «нульової довіри» та інтелектуальних систем аналізу документаційних потоків.

Метою кваліфікаційної роботи є комплексне дослідження теоретичних засад функціонування електронних документів та розробка практичних шляхів оптимізації документообігу у військовій частині 3077. Сформована мета тісно переплітається з предметом дослідження та спрямована на підвищення оперативності військового управління через цифровізацію. Для досягнення поставленої мети необхідно вирішити п’ять конкретних **завдань**, що охоплюють різні аспекти інформаційної діяльності, а саме:

- проаналізувати чинну нормативно-правову базу України, що регулює створення та обіг електронних документів у секторі безпеки;

- вивчити міжнародні та національні стандарти, які визначають технічні вимоги до форматів даних;

- здійснити детальний аналіз організації документаційного забезпечення у військовій частині 3077;

- виявити організаційні та технічні бар’єри, що заважають повноцінному переходу до електронного документообігу;

- розробити пропозицій щодо впровадження хмарних рішень та посилення кібербезпеки в системі автоматизації діловодства.

Об’єктом дослідження є процеси функціонування електронних документів у системі державного та військового управління України.

Предмет дослідження – правові, організаційні та технічні аспекти забезпечення цілісності, конфіденційності та оптимізації обігу документів у військовій частині 3077.

Розробка обраної теми стала можливою завдяки використанню реальних матеріалів та внутрішніх інструкцій зазначеної установи. Під час проведення дослідної роботи було застосовано комплекс методів, що забезпечують об'єктивність та глибину аналізу. Основними методами стали аналіз нормативно-правових актів, системний підхід до вивчення архітектури системи електронного документообігу та порівняльний метод для оцінки ефективності паперових та цифрових потоків.

Отримані результати свідчать про те, що впровадження алгоритму кваліфікованого електронного підпису та штампа часу значно посилює юридичну силу документів. Встановлено, що використання системи «Док Проф» дозволяє мінімізувати ризики внутрішнього фроду та витоку конфіденційної інформації [9]. Дослідження підтвердило, що технічна досконалість процедур кваліфікованого електронного підпису у військовій частині відповідає державним стандартам криптографічного захисту. Практичне значення отриманих результатів полягає у можливості їх безпосереднього впровадження в діяльність канцелярії та кадрових служб Національної гвардії України.

Результати дослідження можуть бути використані для пришвидшення соціальних виплат військовослужбовцям та оперативного обміну даними через шлюзи системи електронного документообігу. Запропоновані алгоритми життєвого циклу документа сприятимуть скороченню часових витрат на погодження наказів та розпоряджень. Висновки роботи можуть слугувати базою для подальшої модернізації захищених вузлів зв'язку в інших підрозділах Національної гвардії. Структура бакалаврської роботи розроблена відповідно до логіки наукового пошуку та поставлених завдань.

Загальний обсяг роботи становить 79 сторінок друкованого тексту. Список використаних джерел налічує 55 найменувань, серед яких законодавчі

акти, державні стандарти та фахова література. Перший розділ присвячено теоретико-методологічним засадам функціонування електронних документів у правовому полі України. У другому розділі проведено всебічний аналіз стану цифровізації та технічних засобів захисту інформації у військовій частині 3077. Третій розділ містить обґрунтовані напрями оптимізації документообігу через впровадження інноваційних хмарних та кіберзахисних технологій. Завершується робота висновками, які узагальнюють результати проведеного дослідження та окреслюють перспективи подальшого розвитку галузі. Такий комплексний підхід до структури дозволив повністю розкрити обрану тему та досягти мети дослідження.

РОЗДІЛ І. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

1.1. Правове регулювання та нормативна база електронного документообігу в Україні

Метою першого розділу є системне дослідження теоретико-методологічних засад функціонування електронних документів та формування науково обґрунтованого підґрунтя для подальшого аналізу діяльності військової частини 3077 Національної гвардії України (далі – НГУ) [4]. Для досягнення цієї мети необхідно розв'язати низку конкретних завдань, що охоплюють правовий, організаційний та технічний виміри інформаційної діяльності. На нашу думку, першочергове завдання – уточнення термінологічного апарату, зокрема розмежування понять «електронний документ», «електронна копія» та «цифровий об'єкт» у контексті сучасної архівної справи. Наступний крок — критичний аналіз чинної нормативно-правової бази України, що регулює створення, обіг та зберігання документів у цифровому середовищі.

Окрему увагу у межах розділу буде приділено вивченню міжнародних та національних стандартів (ISO та ДСТУ), які визначають технічні вимоги до форматів даних та метаданих [10]. Також, опис організаційних моделей електронного документообігу, що застосовуються в державному секторі та силових структурах. Розділ спрямований на виявлення взаємозв'язків між правовими нормами та технічними засобами їхньої реалізації, такими як кваліфікований електронний підпис. Попри значні успіхи цифровізації, теоретичний аналіз висвітлює низку критичних проблем, які заважають повноцінному переходу до безпаперового офісу [3]. Головною проблемою залишається неузгодженість окремих положень законодавства щодо тривалого (понад 10 років) та постійного зберігання електронних документів.

Існує реальний ризик втрати інформаційної цілісності через швидке моральне старіння програмного забезпечення та форматів файлів. Питання забезпечення автентичності документа протягом усього його життєвого циклу залишається відкритим, оскільки термін дії електронних ключів є обмеженим. Технічна проблема конвертації та міграції даних в архівні системи часто супроводжується ризиком несанкціонованої зміни змісту документа. Організаційну складність становить «гібридна» модель діловодства, де одночасне існування паперових та електронних потоків породжує дублювання функцій [4]. Крім того, у сфері національної безпеки постає гостра дилема між відкритістю електронних реєстрів та необхідністю суворої конфіденційності військової інформації. Відсутність єдиного уніфікованого інтерфейсу між різними системами електронної взаємодії створює технічні розриви при передачі документів між відомствами. Брак чітких методик оцінки вартості та ефективності впровадження системи е-документообігу ускладнює процес стратегічного планування в установах.

Правовий вакуум щодо використання хмарних технологій для зберігання службової інформації створює додаткові безпекові ризики. Вирішення цих проблем потребує комплексного підходу, що поєднує вдосконалення законів, оновлення технічних регламентів та розробку нових стандартів архівної справи. Теоретичне осмислення цих аспектів дозволить сформулювати практичні рекомендації для оптимізації роботи з електронними документами у військовій частині 3077 [4]. Тобто, перший розділ становить фундамент роботи, без якого неможливо об’єктивно оцінити стан цифровізації конкретного військового підрозділу.

Запровадження воєнного стану в Україні стало каталізатором для радикальної трансформації нормативного поля, що регулює електронний документообіг у секторі безпеки та оборони [33]. Особливі умови функціонування держави вимагали негайного прийняття нормативно-правових актів, які б дозволяли оперативно обмінюватися інформацією без зайвих бюрократичних зволікань. Зокрема, Постанова Кабінету Міністрів

України № 263 від 12 березня 2022 року «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» суттєво розширила можливості використання хмарних ресурсів для зберігання критично важливих даних державних органів та військових формувань [7]. Ця норма дозволила військовій частині 3077 забезпечити безперервність управління навіть у разі фізичної загрози локальним серверам чи паперовим архівам. Законодавство воєнного часу також легітимізувало спрощені процедури електронної взаємодії між силовими структурами для максимального пришвидшення логістичного та оперативного забезпечення [7].

Важливим аспектом стало посилення вимог до кібербезпеки, що було закріплено у відповідних розпорядженнях Генерального штабу та командування Національної гвардії України [5, с.56]. Правове регулювання в умовах війни акцентує увагу на пріоритеті захисту інформації з обмеженим доступом, що циркулює в автоматизованих системах спеціального призначення. Водночас гостро постала необхідність врегулювання правового статусу електронних рапортів та бойових наказів, що видаються безпосередньо в зонах ведення активних дій. Держава забезпечила правову підтримку використання альтернативних засобів супутникового зв'язку для передачі електронних документів за умови їх належного криптографічного шифрування. Окремим викликом стало питання збереження електронних архівів військових частин, які перебувають під постійним ризиком ракетних обстрілів або кібератак [7].

Нормативна база була доповнена алгоритмами екстреного знищення або евакуації цифрових носіїв інформації з метою запобігання потраплянню службових даних до рук ворога. Також було вдосконалено законодавство щодо електронної ідентифікації особового складу, що дозволило в дистанційному режимі проводити кадрові призначення та соціальні виплати військовослужбовцям. Проблема функціонування електронного

документообігу під час воєнного стану також пов'язана з необхідністю підтримання працездатності систем кваліфікованого електронного підпису (далі – КЕП) у мовах нестабільного енергопостачання та перебоїв у роботі мережі Інтернет. У відповідь на ці виклики правове поле адаптувалося через офіційний дозвіл на використання офлайн-режимів у спеціалізованому програмному забезпеченні для військового діловодства [7].

Слід зазначити, що воєнний стан виявив певні прогалини у міжнародному законодавстві щодо швидкої транскордонної передачі військової документації партнерам у межах технічної допомоги. Це спонукало до розробки нових відомчих інструкцій НГУ, які деталізують процедури безпечного обміну електронними даними з іноземними військовими місіями. Динамічність правових змін у цей складний період вимагає від відповідальних осіб військової частини 3077 постійного моніторингу нових директив та оперативного підвищення кваліфікації [4]. Тобто, сучасна нормативна база електронного документообігу в Україні набула рис «кризового менеджменту», де висока швидкість прийняття рішень поєднується з безкомпромісним захистом національного суверенітету в цифровому просторі. Аналіз законодавства воєнного стану демонструє, що електронний документ остаточно перестав бути просто зручністю, перетворившись на стратегічний інструмент забезпечення загальної обороноздатності країни. Підсумовуючи, можна стверджувати, що сформований правовий фундамент дозволяє перейти до детального розгляду організаційних та технічних стандартів, які безпосередньо втілюють ці норми у повсякденну діяльність гвардійців.

Процес цифровізації державного управління в Україні зумовив необхідність створення міцного правового фундаменту, який би легітимізував статус електронного документа як повноцінного юридичного факту [35]. Становлення вітчизняного законодавства у сфері електронного документообігу пройшло тривалий шлях від теоретичного визначення термінів до створення комплексної екосистеми електронних довірчих послуг. На сучасному етапі правове регулювання цієї сфери базується на принципах

технологічної нейтральності, невідворотності юридичної сили е-документа та пріоритету захисту інформації. Центральне місце в ієрархії нормативних актів посідає Закон України «Про електронні документи та електронний документообіг», який детермінує електронний документ як такий, «інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити» [35].

Закон встановлює фундаментальну норму про те, що юридична сила електронного документа не може бути заперечена лише через те, що він має електронну форму [35]. Важливо розуміти, що для набуття статусу оригіналу електронний документ повинен містити електронний підпис, який прирівнюється до власноручного підпису згідно із законодавством. Саме цей акт визначає життєвий цикл документа: від моменту створення та відправлення до його архівного зберігання або знищення. Логічним доповненням та інструментом реалізації вищезгаданого закону став Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [36]. Цей документ здійснив справжню революцію в документознавстві, запровадивши поняття кваліфікованого електронного підпису, електронної печатки та електронної позначки часу.

Використання КЕП забезпечує не лише ідентифікацію підписувача, а й цілісність документа, оскільки будь-яка зміна в тексті після накладання підпису стає технічно помітною. Логічним доповненням та інструментом реалізації вищезгаданого закону став Закон України «Про електронну ідентифікацію та електронні довірчі послуги», який остаточно закріпив правовий статус цифрових еквівалентів традиційних засобів засвідчення документів [36]. Документ здійснив справжню революцію в документознавстві, запровадивши поняття КЕП, електронної печатки та електронної позначки часу як обов'язкових інструментів цифрової взаємодії.

Завдяки цьому закону було гармонізовано українське правове поле з європейськими стандартами (eIDAS), що відкрило шлях до транскордонного обміну документами та визнання українських е-підписів на міжнародному

рівні [36]. Використання КЕП забезпечує не лише ідентифікацію підписувача, а й цілісність документа, оскільки будь-яка зміна в тексті після накладання підпису стає технічно помітною. Дана законодавча база створює ієрархічну систему довіри, де ключову роль відіграють кваліфіковані надавачі електронних довірчих послуг, що проходять сувору сертифікацію. Впровадження електронної позначки часу дозволяє зафіксувати точний момент створення або підписання документа, що має критичне значення для військового діловодства, де дотримання термінів виконання наказів є питанням дисципліни.

У свою чергу, електронна печатка дозволяє юридичним особам, таким як військова частина 3077, засвідчувати достовірність вихідної кореспонденції та автоматизованих звітів без прямої участі підписувача-керівника в кожній операції [4]. Важливим аспектом закону є визначення процедури перевірки підпису, яка дозволяє будь-якому учаснику обігу переконатися в чинності сертифіката на момент підписання. Законодавець чітко розмежував поняття простого, удосконаленого та кваліфікованого підписів, надавши останньому найвищий ступінь презумпції відповідності власноручному підпису. Для структур Національної гвардії України це означає обов'язкове використання захищених носіїв особистих ключів (токенів), що унеможливлює копіювання ключа та доступ до нього сторонніх осіб [4].

Технічна реалізація КЕП базується на методах асиметричного криптографічного шифрування, що гарантує неможливість відмови від авторства (non-repudiation). Таким чином, правовий режим електронної ідентифікації створює умови для повного виключення паперового дублювання у внутрішніх процесах військової частини. Крім того, закон деталізує роботу з реєстрами та електронними кабінетами, що є основою для функціонування сучасних систем електронного документообігу (далі – СЕД). Правова норма про взаємне визнання різних видів довірчих послуг дозволяє військовій частині взаємодіяти не лише з іншими підрозділами НГУ, а й з цивільними міністерствами та відомствами [5, с.67].

Слід підкреслити, що електронна ідентифікація в Україні тепер охоплює не лише підпис, а й засоби віддаленої верифікації особи, такі як BankID та MobileID, що розширює можливості дистанційної роботи персоналу. Для архівної справи цей закон є важливим, оскільки він закладає вимоги до довгострокового зберігання підписаних документів з можливістю їх подальшої перевірки навіть після завершення терміну дії сертифіката. Окремим блоком у нормативній базі виділено вимоги до криптографічного захисту, які контролюються Державною службою спеціального зв'язку та захисту інформації України. Алгоритми, які використовуються для генерації КЕП, є стійкими до зламів та відповідають державним стандартам безпеки. Кожен електронний документ, підписаний згідно з цими вимогами, стає частиною єдиного інформаційного простору держави з гарантованим юридичним захистом. У контексті бойової та службової діяльності військовослужбовців використання таких технологій пришвидшує логістичні та управлінські операції в рази [5, с.67].

Правове регулювання також враховує питання відкликання та блокування сертифікатів у разі втрати доступу до ключа або звільнення посадової особи. Це забезпечує оперативну реакцію на потенційні загрози безпеці та запобігає несанкціонованому підписанню наказів. Процес стандартизації форматів електронних підписів (CAdES, XAdES, PAdES) дозволяє зберігати документи в уніфікованому вигляді, придатному для автоматизованої обробки [52]. Впровадження цих норм вимагає від особового складу військової частини 3077 не лише знання наказів, а й розуміння технічної відповідальності за збереження конфіденційності власних засобів ідентифікації [4]. Законодавство про довірчі послуги безпосередньо впливає на розвиток хмарних рішень у сфері діловодства, де ключ може зберігатися в захищеному «хмарному» сховищі надавача послуг, що значно спрощує роботу з мобільних пристроїв, що є актуальним для офіцерського складу в польових умовах. Правовий статус електронної копії паперового документа та електронного оригіналу також чітко розмежований, що дозволяє уникнути

юридичних колізій при переведенні архівів у цифровий формат. У результаті, закон створив прозорі правила гри, де кожен біт інформації у документі захищений законом і технологією одночасно.

Розвиток нормативної бази продовжується через прийняття підзаконних актів, що деталізують роботу з КЕП у специфічних умовах, наприклад, при відсутності стабільного зв'язку з серверами акредитованого центру сертифікації ключів. Це критично для військових частин, які можуть виконувати завдання в зонах зі складним зв'язком. Юридична визначеність, яку надає цей закон, дозволяє керівництву НГУ впроваджувати інновації з повною впевненістю у правомірності своїх дій [4]. Нарешті, гармонізація з європейським законодавством готує ґрунт для інтеграції українських військових стандартів документування у загальну систему стандартів НАТО. Таким чином, правове регулювання електронної ідентифікації є наріжним каменем, на якому тримається вся архітектура сучасного електронного документообігу військової частини 3077 [4].

Особливу роль в організації діловодства відіграють підзаконні акти, зокрема Постанова Кабінету Міністрів України № 55 від 17 січня 2018 року, яка затвердила Типову інструкцію з документування управлінської діяльності в електронній формі [6]. Документ детально регламентує порядок роботи з електронними документами в органах виконавчої влади та установах. Він визначає правила реєстрації, погодження, підписання та передавання документів через систему електронної взаємодії органів виконавчої влади (далі – СЕВ ОВВ). Для військових частин, як-от військова частина 3077 НГУ, ці норми є базовими, проте вони доповнюються специфічними вимогами щодо захисту інформації [4]. Оскільки спеціальність 029 Інформаційна, бібліотечна та архівна справа фокусується на архівній справі, критично важливим є Наказ Міністерства юстиції України №1000/5 «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», який регламентує правила організації діловодства та архівного зберігання

документів [6]. Наказ встановлює чіткі вимоги до створення електронних справ, їхнього формування за номенклатурою та підготовки до передачі в архівні підрозділи.

У контексті електронних документів правове регулювання також вимагає дотримання форматів тривалого зберігання, таких як PDF/A, що гарантує відтворюваність інформації через десятки років [52]. Для Національної гвардії України як військового формування з правоохоронними функціями нормативна база розширюється відомчими наказами Міністерства внутрішніх справ. Акти деталізують особливості документування в умовах особливого періоду, воєнного стану та при роботі з інформацією з обмеженим доступом. Правовий аспект тут тісно переплітається із законодавством про державну таємницю та технічний захист інформації. Використання електронних документів у військовій частині 3077 вимагає суворого дотримання вимог щодо створення комплексної системи захисту інформації (КСЗІ), що підтверджується відповідним атестатом відповідності.

Важливим елементом правового поля є також норми, що регулюють відповідальність за порушення у сфері електронного документообігу. Кодекс України про адміністративні правопорушення [15] та Кримінальний кодекс [16] містять статті, що передбачають санкції за несанкціоноване втручання в роботу автоматизованих систем або підробку електронних документів. Таким чином, правове регулювання створює безпечне середовище, у якому суб'єкти відносин, включаючи військовослужбовців та цивільний персонал НГУ, можуть оперувати даними з високим ступенем довіри [12]. Сучасна судова практика в Україні також підтверджує пріоритетність електронного документообігу, де е-докази стають повноцінною частиною процесу. Правове поле постійно еволюціонує, адаптуючись до нових викликів, таких як мобільна ідентифікація або хмарні сервіси підпису. Для військової частини 3077 це означає необхідність постійного моніторингу змін у законодавстві для забезпечення легітимності своєї діяльності в цифровому просторі. У підсумку, нормативна база України у сфері електронного документообігу є достатньо

зрілою та комплексною, що дозволяє повноцінно переходити до безпаперових технологій навіть у таких консервативних структурах, як військові підрозділи.

1.2. Організаційні та технічні стандарти роботи з електронними документами

Становлення системи електронного документообігу у військовій частині 3077 неможливо розглядати у відриві від загальної еволюції військового адміністрування, яка пройшла шлях від жорстко регламентованої радянської моделі до сучасних стандартів НАТО [12]. Радянська спадщина в діловодстві характеризувалася тотальним «папероцентризмом», де кожен крок військовослужбовця мав бути зафіксований у фізичному журналі з пронумерованими та прошнурованими сторінками. Система базувалася на принципах надмірної централізації та багаторівневого дублювання інформації, що в умовах тогочасних технологій було єдиним способом забезпечення надійності та секретності. Основним інструментом штабної роботи десятиліттями залишалася друкарська машинка, а пізніше — перші персональні комп'ютери, які, проте, використовувалися лише як досконалі засоби підготовки текстів для їхнього подальшого роздрукування [5, с.23].

Перехідний період 1990-х та початку 2000-х років позначився «гібридною» моделлю, коли електронні файли вже існували на дискетах, але не мали жодної юридичної сили без паперового оригіналу з «мокрою» печаткою. У військовій частині 3077 цей етап супроводжувався складним процесом адаптації радянських класифікаторів документів до нових вимог незалежної України, що часто призводило до бюрократичної інерції [4]. Старі інструкції вимагали фізичного зберігання величезних масивів паперу, що створювало значне логістичне навантаження на архівні підрозділи та ускладнювало оперативний пошук інформації. Організаційна культура того часу сприймала комп’ютер як допоміжний засіб, а не як основу для створення єдиного інформаційного простору. Технічні стандарти обмежувалися

локальними мережами без належного рівня захисту, що стримувало впровадження повноцінного обміну документами між різними службами частини [5, с.34].

Зокрема, одним із таких документів є Інструкція з діловодства у Збройних Силах України (далі – Інструкція) – базовий нормативний акт, що регламентує документування управлінської діяльності та організацію роботи з документами у військових органах і частинах [12]. Вона визначає єдині вимоги до створення, оформлення, обліку, руху, зберігання та використання документів як у паперовій, так і в електронній формах. Документ спрямований на уніфікацію управлінських процесів та забезпечення належного рівня інформаційної дисципліни. Однією з ключових характеристик Інструкції є її комплексність, оскільки вона охоплює всі етапи життєвого циклу документа. Важливим аспектом є встановлення чітких правил документування управлінської інформації. Інструкція закріплює обов'язковість використання встановлених реквізитів для кожного виду документа [12].

Зокрема, до основних реквізитів належать назва установи, дата, реєстраційний індекс, заголовок, текст і підпис. Дані реквізити забезпечують стандартизацію документів і полегшують їх подальше опрацювання. Документ також визначає порядок реєстрації вхідної, вихідної та внутрішньої кореспонденції. Реєстрація є важливим елементом контролю за рухом документів. Інструкція передбачає ведення відповідних журналів або електронних систем обліку, особлива увага приділяється електронному документообігу, що свідчить про адаптацію військової системи управління до сучасних інформаційних технологій. Інструкція регламентує використання автоматизованих систем обробки документів, водночас, зберігається можливість роботи з паперовими носіями. Такий підхід забезпечує гнучкість організації діловодства [12].

Документ також встановлює вимоги до підготовки службових листів, наказів, розпоряджень та інших документів. В Інструкції визначено правила їх структурування та стилю викладення інформації, особливе значення має

чіткість і лаконічність тексту [12]. Інструкція наголошує на необхідності дотримання службової дисципліни при роботі з документами. Важливою складовою є контроль за виконанням документів, встановлюються строки виконання та порядок їх відстеження, а контроль сприяє підвищенню ефективності управлінських рішень. Окремий розділ в Інструкції присвячений організації зберігання документів, визначено правила формування справ і їх систематизації. Також, Інструкція передбачає створення номенклатури справ, що забезпечує впорядкованість архівного зберігання. Документ регламентує строки зберігання різних категорій документів, визначає порядок передачі документів до архіву [12].

Інструкція враховує вимоги інформаційної безпеки, особливо це актуально для військової сфери. Також, передбачено обмеження доступу до окремих видів інформації. Документ встановлює правила роботи з документами з обмеженим доступом, що сприяє захисту службової таємниці. Інструкція також регламентує порядок копіювання та тиражування документів, визначає відповідальність посадових осіб за порушення правил діловодства. Так забезпечується дисциплінарний контроль. Інструкція сприяє підвищенню прозорості управлінських процесів, створює умови для ефективної комунікації між підрозділами. Документ має важливе значення для організації роботи штабів, забезпечує єдність підходів до ведення документації [12].

Інструкція також враховує специфіку військової служби:

- оперативність прийняття рішень і їх документальне оформлення;

- встановлює вимоги до мовного оформлення документів;

- сприяє цифровізації управлінських процесів у Збройних Силах України;

- використовує офіційно-діловий стиль [12].

На нашу думку, це сприяє точності передачі інформації. Інструкція також визначає порядок внесення змін до документів, важливим є забезпечення актуальності інформації. Документ регламентує взаємодію між

різними рівнями управління, охоплює як центральні органи, так і військові частини. Водночас Інструкція зберігає традиційні підходи до діловодства, такий баланс є важливим для стабільності системи. Інструкція є інструментом підвищення ефективності управління, забезпечує належний рівень організації документообігу. Документ має нормативно-обов'язковий характер для всіх військових органів, його положення підлягають неухильному виконанню. Таким чином, Інструкція з діловодства у Збройних Силах України є фундаментом організації інформаційної діяльності в армії [12].

У подальшому, справжня трансформація почалася із впровадженням концепції «електронної держави», яка змусила військові формування переглянути свої підходи до документаційного забезпечення. Відхід від радянської системи реєстрації документів у журналах на користь автоматизованих баз даних став першим кроком до подолання часових розривів в управлінні. У військовій частині 3077 цей процес розпочався з автоматизації обліку особового складу та фінансової звітності, де точність даних була критично важливою [4]. Важливим викликом стала необхідність перенавчання персоналу, який звик до фізичного відчуття документа та власноручного підпису як єдиного гаранта достовірності. Впровадження українських стандартів діловодства поступово витіснило застарілі радянські «ГОСТи», привносячи в армійське середовище логіку структурованих метаданих та форматів електронного архівування.

Сучасний етап розвитку, особливо після 2014 року, характеризується стрімким впровадженням систем класу СЕД, які інтегрують у собі всі етапи життя документа — від проєкту до архіву [5, с.101]. На відміну від радянської моделі, де інформація рухалася вертикально і повільно, сучасна система у військовій частині 3077 дозволяє здійснювати горизонтальну взаємодію між підрозділами в режимі реального часу. Перехід до використання КЕП став фінальною крапкою в демонтажі старої системи, легітимізувавши цифровий документ як першоджерело. Це дозволило позбутися тисяч паперових копій рапортів, довідок та наказів, які раніше потребували значних витрат на папір,

картриджі та складські приміщення. На зміну масивним шафам з теками прийшли сервери з багаторівневим захистом, що відповідають вимогам комплесній системі захисту інформації.

Особливістю українського шляху є поєднання суворих вимог безпеки, успадкованих від військової традиції, з інноваційними IT-рішеннями, що випереджають аналогічні системи багатьох європейських країн. У військовій частині 3077 сьогодні спостерігається синергія між досвідом старшого покоління офіцерів, які знають ціну точності документа, та молодих фахівців, що вільно оперують хмарними технологіями [4]. Проблема радянського минулого — «папір заради паперу» — поступово трансформується в принцип «дані заради ефективності». Технічні стандарти тепер орієнтовані на інтероперабельність, що дозволяє частині діяти як єдиний організм у структурі Національної гвардії. Тобто, перехід від радянської системи до сучасної української став не просто технічним оновленням, а глибокою ментальною та організаційною революцією. Сьогодні електронний документообіг у військовій частині 3077 є фундаментом, що забезпечує швидкість реагування на загрози, прозорість логістики та надійність збереження історичної пам'яті підрозділу в цифровому форматі.

Ефективність функціонування системи електронного документообігу у військовій частині 3077 безпосередньо залежить від суворого дотримання встановлених організаційних та технічних стандартів, що розглядаються не просто як технічні інструкції, а як гарантія збереженості, автентичності та юридичної сили документальної інформації протягом усього її життєвого циклу [4]. Першочерговим технічним аспектом є уніфікація форматів файлів, що використовуються для створення та зберігання документів. Державні стандарти України, зокрема ISO 19005-1:2005, визначають формат PDF/A як пріоритетний для електронних документів тривалого та постійного зберігання. Формат забезпечує візуальну цілісність документа незалежно від програмного забезпечення, що використовується для його перегляду, що є критичним для кадрових наказів та фінансової звітності військової частини [11].

Для текстових документів, що знаходяться на етапі оперативного опрацювання в структурних підрозділах (штабі, службі логістики), допускається використання форматів .docx або .odt, проте фінальна версія обов'язково конвертується у нередагований формат. Технічні стандарти також вимагають, щоб графічні образи паперових оригіналів (скан-копії) зберігалися у форматі PDF або TIFF із роздільною здатністю не менше 300 dpi, що дозволяє зберегти всі деталі підписів та мокрих печаток. Організація роботи структурних підрозділів, таких як служба діловодства або секретаріат, неможлива без чітко визначених метаданих [12].

Метадані є цифровим паспортом документа, що включає реєстраційний номер, дату, автора, короткий зміст (анотацію) та гриф обмеження доступу. Згідно з національними стандартами, метадані повинні бути нерозривно пов'язані з самим документом та забезпечувати можливість його швидкого пошуку в базі даних СЕД. У військовій частині 3077 особливе значення мають метадані, що вказують на термін зберігання документа відповідно до номенклатури справ, що дозволяє автоматизувати процес відбору документів на архівне зберігання або знищення. Центральним елементом забезпечення юридичної значущості є кваліфікований електронний підпис. Технічно КЕП базується на використанні засобів криптографічного захисту інформації, що мають сертифікат відповідності від Держспецзв'язку [52].

Для військовослужбовців військової частини 3077 обов'язковим є використання захищених носіїв особистих ключів (апаратних токенів або смарт-карт), які унеможливлюють несанкціоноване копіювання ключа. Організаційно процес підписання в структурних підрозділах побудований так, щоб забезпечити послідовне або паралельне візування документа всіма зацікавленими посадовими особами. Використання електронної позначки часу в структурі КЕП дозволяє встановити точний момент підписання документа, що виключає можливість антидатування наказів командування. Архітектура систем автоматизації документообігу, що впроваджуються в Національній гвардії, зазвичай має триланкову структуру: рівень бази даних, рівень бізнес-

логіки та рівень клієнтського інтерфейсу. Така побудова забезпечує високу відмовостійкість та можливість інтеграції з СЕВ ОВВ [52].

Для структурних підрозділів військової частини це означає можливість оперативного отримання розпоряджень від вищого штабу в режимі реального часу. Технічні стандарти архітектури СЕД також передбачають обов'язкову наявність модуля захисту інформації, що відповідає вимогам комплексної системи захисту інформації. Кожне робоче місце в частині, де здійснюється обробка документів, має бути авторизоване, а дії користувача — протоколюватися в системному журналі. Впровадження цих стандартів у роботу структурних підрозділів вимагає високої виконавської дисципліни. Служба кадрів використовує стандартизовані шаблони для створення контрактів та особових справ, що спрощує подальшу автоматизовану обробку даних. Фінансова служба оперує форматами, сумісними з банківськими системами та реєстрами казначейства, що забезпечує швидкість проведення платежів. Навіть у польових умовах технічні стандарти вимагають використання захищених каналів зв'язку (VPN) для доступу до централізованої бази даних документів. Організаційні регламенти визначають порядок дій у разі технічного збою, передбачаючи процедури відновлення даних із резервних копій [52].

Архівний підрозділ частини керується стандартами щодо формування електронних справ та передачі їх до відомчого архіву НГУ [4]. Це передбачає перевірку цілісності КЕП на момент завершення справи та конвертацію всіх файлів у формати тривалого зберігання з додаванням XML-файлів метаданих. Таким чином, організаційні та технічні стандарти створюють замкнений і безпечний цикл життя документа. Для військової частини 3077 це не просто питання автоматизації, а засіб підвищення бойової готовності через прискорення управлінських процесів. Дослідження цих стандартів дозволяє зрозуміти, як саме технологічні норми трансформуються в адміністративну ефективність військового формування. Кожен аспект — від розміру шрифту в

PDF/A до криптографічної стійкості КЕП — є частиною єдиного механізму державного управління в цифрову епоху.

РОЗДІЛ ІІ. АНАЛІЗ СТАНУ ТА ОСОБЛИВОСТЕЙ РОБОТИ З ЕЛЕКТРОННИМИ ДОКУМЕНТАМИ У ВІЙСЬКОВІЙ ЧАСТИНІ 3077 НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

2.1. Організація документаційного забезпечення управління у військовій частині

Ефективність управління оборонним сектором у сучасних умовах безпосередньо залежить від якості інформаційної взаємодії між суб'єктами владних повноважень та підпорядкованими структурами. У системі Національної гвардії України ключовою ланкою реалізації управлінських рішень є військова частина. Згідно з чинним законодавством, військова частина визначається як державна установа, що має постійне місце дислокації, власну назву, номер та печатку із зображенням Державного Герба України. Вона функціонує як цілісний бойовий та адміністративно-господарський організм, наділений правами юридичної особи публічного права. Об'єктом нашого дослідження є військова частина 3077 Національної гвардії України, яка згідно з даними державного реєстру (код ЄДРПОУ 08803804) – активний суб'єкт правовідносин [4].

Організаційна структура частини передбачає наявність штабу, підрозділів забезпечення та спеціалізованих відділів, що потребують чіткої координації. Основою такої координації є документаційне забезпечення управління, яке охоплює сукупність процесів створення, збору, обробки та зберігання інформації. Документаційне забезпечення у військових структурах України регламентується суворими нормативно-правовими актами, наказами Міністерства внутрішніх справ України та розпорядженнями Командувача НГУ [12]. Воно включає в себе не лише паперовий документообіг, а й поступове впровадження автоматизованих систем управління. Основною метою документного забезпечення управління у військовій частині 3077 є

надання повної та достовірної інформації для прийняття оперативних рішень командуванням [12].

Специфіка військової служби вимагає від системи документування високого рівня захисту даних та оперативності. Документаційне забезпечення управління в Україні на сучасному етапі перебуває у стані трансформації в бік цифровізації, тобто, перехід від традиційних журнальних форм реєстрації до використання спеціалізованого програмного забезпечення. У військовій частині 3077 даний процес реалізується через розмежування відкритого та обмеженого доступу до інформації. Юридичний статус частини як державної організації зобов'язує її дотримуватися стандартів діловодства, визначених ДСТУ. Кожен документ, що створюється в межах частини, має юридичну силу та фіксує конкретний управлінський акт [4].

Діяльність військової частини 3077 супроводжується великим обсягом розпорядчої, фінансової та кадрової документації. Управлінський цикл починається з отримання вхідної кореспонденції або видання власного наказу командира. Система документного забезпечення управління забезпечує проходження документа від моменту його створення до передачі в архів або знищення. Важливою складовою є контроль за виконанням документів, що у військовій сфері має критичне значення для боєготовності. Документаційне забезпечення в Україні базується на принципах єдності, системності та актуальності інформації. Для військової частини 3077 це означає інтеграцію у загальнодержавну систему електронної взаємодії. Організація роботи з документами тут покладається на службу діловодства або стройову частину [4]. Персонал, залучений до роботи з документами, проходить спеціальну підготовку щодо поводження з інформацією з обмеженим доступом.

Технічні аспекти документаційного забезпечення включають використання засобів криптографічного захисту та спеціальних каналів зв'язку. Юридична чистота документів забезпечується правильним оформленням реквізитів згідно з чинними інструкціями. В умовах воєнного стану навантаження на систему документаційного забезпечення значно

зросло. Військова частина 3077 змушена адаптувати свої внутрішні регламенти під вимоги оперативності [4]. Документування бойових розпоряджень та логістичних операцій потребує мінімізації бюрократичних затримок. Важливою особливістю є поєднання паперових дублікатів з електронними реєстрами для забезпечення живучості системи. Державна політика України в галузі документного забезпечення управління спрямована на поступову відмову від зайвої паперової тяганини.

У військовій частині 3077 це проявляється через впровадження внутрішніх баз даних для обліку особового складу та майна. Організаційна побудова діловодства дозволяє чітко розподілити відповідальність між виконавцями. Моніторинг стану документного забезпечення управління у частині здійснюється під час планових перевірок вищестоящими штабами. Аналіз показує, що рівень автоматизації процесів у частині постійно підвищується. Це дозволяє зменшити кількість помилок, пов’язаних із людським фактором. Ефективна організація документного забезпечення управління є фундаментом для правової захищеності військовослужбовців та самої частини як юридичної особи. Подальший розвиток системи у військовій частині 3077 пов'язаний із повноцінним переходом на електронний підпис. Це дозволить пришвидшити обмін даними з іншими НГУ. Проте технічні обмеження та вимоги секретності залишаються викликом для повної цифровізації [4].

Маємо наголосити, що сучасний стан розвитку військового управління вимагає від канцелярії військової частини 3077 переходу на принципово нові рейки цифрової взаємодії. Традиційні методи діловодства поступово поступаються місцем спеціалізованим системам електронного документообігу (далі – СЕДО), що інтегровані в загальну мережу оборонного сектору. Канцелярія в даному контексті перестає бути лише місцем реєстрації паперових журналів, перетворюючись на ключовий вузол обробки захищеної інформації. Основним інструментом у роботі частини є спеціалізоване програмне забезпечення, яке відповідає найвищим вимогам технічного

захисту інформації. Використання СЕДО у військовій сфері України обумовлено необхідністю забезпечення конфіденційності, цілісності та доступності даних у реальному часі [12].

Військова частина 3077 як підрозділ Національної гвардії України активно використовує захищені канали зв'язку для обміну електронними документами з вищестоящим командуванням [4]. Організація роботи канцелярії передбачає чітке розмежування обов'язків персоналу щодо доступу до різних сегментів мережі. Електронний документообіг у частині базується на використанні кваліфікованих електронних підписів, що надає цифровим документам повної юридичної сили. Кожен вхідний документ, що надходить через систему, проходить автоматичну перевірку на цілісність та автентичність.

Канцелярія забезпечує маршрутизацію цих документів до відповідних служб та підрозділів без фізичного переміщення паперових копій. Це дозволяє скоротити час на розгляд документів та прийняття управлінських рішень у декілька разів. Важливою особливістю є те, що всі операції в системі мають пароль, що унеможливлює несанкціоноване видалення або зміну даних. Спеціалізовані СЕДО, які застосовуються в НГУ та Міністерстві оборони України, мають атестати відповідності комплексної системи захисту інформації. Це гарантує, що обмін документами між частиною та Міністерством оборони України захищений від перехоплення сторонніми особами. Зовнішня взаємодія частини охоплює широке коло суб'єктів, де ключову роль відіграє вертикаль військового управління [4].

Канцелярія оперативно опрацьовує директиви та розпорядження, що надходять з Генерального штабу або Головного управління НГУ. Окремим важливим вектором роботи є взаємодія з Територіальними центрами комплектування та соціальної підтримки (далі – ТЦКтаСП) [12]. Обмін даними про особовий склад, призовників та резервістів здійснюється через спеціальні реєстри, інтегровані в загальну систему, що дозволяє військовій частині 3077 актуалізувати дані про мобілізаційні ресурси та забезпечувати своєчасне

кадрове наповнення. Автоматизація цього процесу мінімізує ризики помилок у персональних даних військовозобов'язаних. Крім того, значна частка електронного документообігу припадає на взаємодію з медичними закладами, зокрема військовими госпіталями та цивільними лікарнями. Упровадження електронних медичних документів та довідок дозволяє канцелярії оперативно отримувати інформацію про стан здоров'я особового складу. Процеси проходження військово-лікарської комісії тепер супроводжуються електронним обміном висновками, що пришвидшує процедури реабілітації чи звільнення [12].

Електронна взаємодія з медичними установами також охоплює питання обліку поранених та хворих, що є критичним у період ведення бойових дій. Система дозволяє відстежувати кожен етап лікування військовослужбовця від моменту евакуації до повернення в стрій. Канцелярія частини здійснює контроль за надходженням епікризів та медичних довідок через захищені шлюзи передачі даних. Підхід усуває необхідність для військовослужбовців особисто перевозити паперові пакети документів між установами. Технічна реалізація цього процесу вимагає високої кваліфікації діловодів та IT-спеціалістів частини. Внутрішній цикл роботи з документами в канцелярії також зазнав суттєвих змін завдяки цифровізації. Створення проєктів наказів тепер відбувається в електронних чернетках із можливістю паралельного редагування різними службами. Погодження документів зацікавленими посадовими особами здійснюється за допомогою накладання електронних віз. Це знімає проблему «черг» під кабінетами та прискорює внутрішні бюрократичні процедури [5, с.104].

Військова частина 3077 використовує ієрархічну модель доступу до СЕДО, де кожен офіцер бачить лише ті документи, що стосуються його компетенції. Канцелярія виступає модератором цього процесу, контролюючи терміни виконання завдань. Автоматичні сповіщення про наближення дедлайнів допомагають підтримувати високу виконавську дисципліну. Архівне зберігання електронних документів у частині організовано на

захищених серверах із регулярним резервним копіюванням. Це забезпечує збереження інформації навіть у разі технічних збоїв або фізичного пошкодження інфраструктури. Правовий аспект роботи канцелярії регулюється не лише загальнодержавними законами, а й специфічними військовими статутами. Важливо зазначити, що електронний документообіг у військовій частині не є абсолютно відірваним від паперового. Існує категорія документів, що вимагають обов'язкового дублювання на папері згідно з нормами секретного діловодства. Проте частка таких документів поступово зменшується на користь цифрових аналогів [5, с.105].

Електронна система дозволяє канцелярії формувати аналітичні звіти про стан діловодства одним натисканням кнопки [4]. Це дає командуванню можливість бачити реальну картину завантаженості підрозділів. Аналіз роботи з електронними документами показує значне зменшення витрат на розхідні матеріали, такі як папір та тонер. Екологічний аспект цифровізації також є важливим бонусом для модернізації частини. Безпека передачі даних між частиною та іншими силовими структурами забезпечується використанням апаратно-програмних засобів шифрування. Це особливо важливо при обміні інформацією з Міністерством оборони, де дані мають стратегічне значення. Взаємодія з ТЦКтаСП через систему «Оберіг» або аналогічні модулі СЕДО дозволяє оперативно реагувати на зміни в мобілізаційному законодавстві. Канцелярія частини є точкою входу для всієї зовнішньої кореспонденції, що надходить через систему електронної взаємодії органів виконавчої влади. Це дозволяє військовій частині бути інтегрованою в загальну державну систему управління [4].

Цифровізація канцелярії також спрощує процес надання довідок про участь у бойових діях для військовослужбовців. Завдяки електронним реєстрам перевірка підстав для видачі таких документів займає лічені хвилини. Це підвищує рівень соціальної захищеності бійців та членів їхніх родин. Впровадження електронних черг та автоматизованих форм запитів у канцелярії зменшує корупційні ризики. Кожен крок документа є прозорим для

контролюючих органів усередині структури НГУ. Виклики, з якими стикається канцелярія, включають необхідність постійного оновлення парку комп'ютерної техніки. Стабільність енергопостачання та наявність резервних каналів інтернету є критичними для безперебійної роботи СЕДО. Персонал к канцелярії регулярно проходить курси підвищення кваліфікації щодо роботи з новими модулями системи. Психологічний бар'єр переходу від паперу до екрану серед старшого офіцерського складу поступово долається завдяки зручності інтерфейсів [5, с.234].

Електронний документообіг дозволяє частині залишатися мобільною та дієздатною в умовах частої зміни дислокації [12]. Хмарні технології (у межах захищених військових контурів) дозволяють розгорнути робоче місце діловода в будь-якій точці за лічені години. Система автоматично синхронізує дані після відновлення зв'язку, якщо він був тимчасово відсутній. Таким чином, СЕДО стає не просто зручністю, а інструментом забезпечення живучості системи управління. Організація роботи канцелярії військової частини 3077 у системі електронного документообігу є зразком сучасної армійської трансформації. Вона поєднує в собі суворість військового регламенту та гнучкість ІТ-технологій. Кожен електронний документ, зареєстрований канцелярією, є цеглиною в фундаменті загальної обороноздатності держави. Подальший розвиток системи передбачає глибшу інтеграцію з реєстрами інших міністерств та відомств. Це дозволить створити єдиний інформаційний простір для всіх складових Сил оборони [48].

Розгляд роботи канцелярії через призму СЕДО висвітлює роль людського фактора в цифровій системі. Відповідальність діловода за правильність введення метаданих документа залишається надзвичайно високою. Помилка на етапі реєстрації може призвести до неправильної маршрутизації важливого наказу. Тому система передбачає багаторівневу верифікацію критично важливих даних. Інтеграція з медичними закладами через СЕДО дозволяє автоматично оновлювати дані про придатність особового складу в кадрових системах. Це спрощує планування ротацій та

відпусток для лікування. Взаємодія з ТЦКтаСП забезпечує безперебійний цикл відбору та призначення фахівців на вакантні посади [48]. Всі ці процеси замикаються на канцелярії, яка забезпечує юридичне оформлення кожного кроку. Спеціалізовані захищені системи електронного документообігу є запорукою того, що військова таємниця залишиться таємницею. Шифрування за державними стандартами виключає можливість дешифрування перехоплених даних сучасними засобами розвідки.

Робота канцелярії в системі СЕДО також полегшує підготовку до перевірок та інспекцій [4]. Усі необхідні звіти генеруються автоматично на основі накопичених даних. Це звільняє персонал від тижнів ручної роботи перед приїздом комісій. Впровадження електронних журналів обліку дозволяє здійснювати пошук потрібного документа за лічені секунди. Більше немає потреби переглядати стоси паперу в пошуках запису річної давнини. Електронний архів забезпечує миттєвий доступ до історичних даних про діяльність частини. Це важливо для підготовки аналітичних доповідей та узагальнення бойового досвіду. Канцелярія військової частини 3077 постійно вдосконалює свої методи роботи, адаптуючись до нових загроз. Кібербезпека стає невід'ємною частиною посадових інструкцій кожного працівника канцелярії. Використання двохфакторної автентифікації та апаратних ключів доступу є нормою для входу в систему [12].

Важливо відзначити, що цифровізація не скасовує персональну відповідальність командирів за підписані документи. КЕП є повним аналогом власноручного підпису, що тягне за собою відповідні правові наслідки. Система СЕДО у військовій частині 3077 інтегрована з поштовими серверами для обміну офіційною кореспонденцією з цивільними організаціями. Це дозволяє оперативно вирішувати господарські питання та питання комунального забезпечення. Прозорість процесів у канцелярії сприяє підвищенню довіри особового складу до командування [4]. Кожен військовослужбовець може бути впевнений, що його рапорт не загубиться і буде вчасно розглянутий. Електронна реєстрація скарг та звернень дозволяє

контролювати дотримання прав військовослужбовців. Такий підхід відповідає стандартам НАТО щодо прозорості та підзвітності в оборонному секторі. Використання спеціалізованих систем дозволяє частині ефективно діяти навіть у розпорошеному стані. Підрозділи, що знаходяться на відстані один від одного, залишаються в єдиному документізованому просторі.

Це забезпечує єдність управління та швидкість реагування на зміни обстановки. Канцелярія виконує роль головного диспетчера цього потоку інформації [4]. Всі вищезазначені аспекти підтверджують, що організація е-документообігу є технічно складним, але вкрай необхідним процесом. Військова частина 3077 демонструє високу адаптивність у впровадженні інновацій. Подальше вдосконалення системи сприятиме повній відмові від паперового баласту. Це дозволить звільнити людські ресурси для виконання безпосередніх бойових завдань. У підсумку, цифрова трансформація канцелярії є стратегічним напрямком розвитку військового управління. Захищені СЕДО створюють надійний тил для інформаційних операцій. Співпраця з Міністерство оборони України, ТЦКтаСП та медициною через ці системи є запорукою системності та злагодженості [48]. Військова частина 3077 продовжує рух у напрямку повної цифрової інтеграції. Такий підхід забезпечує перевагу над ворогом у швидкості обробки інформації. Електронний документ стає потужною зброєю в руках професійного військового управлінця. Сучасна канцелярія — це високотехнологічний центр, що тримає на контролі життєдіяльність усієї частини [4].

Отже, документаційне забезпечення залишається стратегічним ресурсом управління у військовій сфері. Взаємодія з YouControl та іншими відкритими реєстрами підтверджує відкритість частини у питаннях господарської діяльності [4]. Водночас, внутрішня документація залишається надійно захищеною від стороннього втручання. Організація документного забезпечення управління у військовій частині 3077 є прикладом поєднання традицій військового адміністрування та інноваційних підходів. Кожен крок у напрямку вдосконалення документообігу підвищує загальну ефективність

виконання бойових завдань. Таким чином, аналіз стану документаційного забезпечення дозволяє виявити зони для подальшої оптимізації. Створення сучасної моделі роботи з електронними документами є пріоритетом для розвитку частини в умовах євроінтеграції України.

2.2. Технічні аспекти забезпечення конфіденційності та цілісності електронної документації

Технічна архітектура захисту інформації у військовій частині 3077 є базовим елементом, що гарантує стійкість системи управління в умовах сучасних кіберзагроз. Забезпечення конфіденційності та цілісності електронних документів вимагає впровадження високоефективних програмних рішень, серед яких провідне місце посідає система «Док Проф» [9]. Ця система розроблена з урахуванням суворих вимог державного стандарту України щодо технічного захисту інформації. Використання «Док Проф» у військовій сфері зумовлене її здатністю створювати ізольоване середовище для обробки документів із різними грифами обмеження доступу [9]. Основним технічним завданням системи є запобігання несанкціонованому перегляду або модифікації даних на всіх етапах їхнього життєвого циклу. Конфіденційність у системі досягається шляхом багаторівневої ідентифікації та автентифікації користувачів. Кожен працівник канцелярії або офіцер штабу отримує доступ до системи лише після успішної перевірки персональних цифрових сертифікатів. «Док Проф» підтримує рольову модель доступу, що дозволяє чітко розмежувати права перегляду, редагування та підписання документів.

Технічна реалізація конфіденційності базується на використанні сучасних алгоритмів шифрування, що відповідають національним стандартам криптографії. Вся інформація, що передається каналами зв'язку між терміналами військової частини 3077 та сервером, захищена криптографічними тунелями [4]. Це унеможливлює перехоплення змісту

наказів або розпоряджень під час їхнього транзиту мережею. Крім того, «Док Проф» забезпечує шифрування даних безпосередньо в базі даних, що захищає їх навіть у разі фізичного викрадення носіїв інформації [9]. Важливою технічною особливістю системи є функція «прозорого» шифрування, яка не створює незручностей для кінцевого користувача, але надійно захищає контент. Цілісність документації у системі «Док Проф» підтримується через механізм хешування та накладання кваліфікованих електронних підписів. Будь-яка спроба внести несанкціоновані зміни в електронний файл призводить до негайного порушення цілісності підпису та блокування документа [9].

Програмне забезпечення системи автоматично відстежує версійність документів, зберігаючи історію всіх правок та коректур, що дозволяє технічно підтвердити авторство кожної зміни та час її внесення, що є критичним для військового правопорядку. Система «Док Проф» інтегрована з апаратними засобами захисту, такими як захищені носії ключової інформації (токени) [9]. Це виключає можливість підробки електронного підпису через копіювання ключів із пам'яті комп'ютера. Технічний аудит системи проводиться в режимі реального часу, фіксуючи кожну спробу входу або запиту до бази даних. Журнали аудиту є захищеними від редагування, що створює неспростовні докази всіх дій посадових осіб. Для забезпечення цілісності даних у разі апаратних збоїв у військовій частині 3077 реалізовано систему дзеркалювання серверів. «Док Проф» підтримує технології автоматичного резервного копіювання, що мінімізує ризики втрати інформації [9].

Технічний захист конфіденційності також включає механізми контролю друку та експорту документів. Система дозволяє встановлювати заборону на копіювання тексту або зняття скріншотів із особливо важливих документів. Кожен виведений на друк примірник автоматично маркується унікальними водяними знаками та ідентифікатором користувача, який здійснив друк. Це забезпечує технічну можливість відстеження джерела витоку інформації у разі появи паперової копії за межами частини. «Док Проф» також має вбудовані модулі для перевірки файлів на наявність шкідливого програмного коду перед

їхнім завантаженням у сховище, захищаючи внутрішню мережу військової частини від вірусів-шифрувальників та шпигунського програмного забезпечення. Важливою перевагою системи є її повна відповідність вимогам щодо створення Комплексної системи захисту інформації (КСЗІ) [9].

Програмний комплекс «Док Проф» успішно пройшов державну експертизу в галузі ТЗІ, що підтверджено відповідним атестатом. Технічні параметри системи дозволяють масштабувати її під потреби як невеликого підрозділу, так і цілого з'єднання. Взаємодія «Док Проф» з іншими СЕДО в системі Міністерства оборони України та НГУ відбувається через захищені шлюзи з автоматичною перевіркою сертифікатів безпеки. Система підтримує роботу в гетерогенних мережах, забезпечуючи стабільність зв'язку навіть при низькій пропускній здатності каналів. Адміністрування системи технічного захисту покладається на спеціалізований підрозділ ІТ-безпеки частини. Вони використовують консоль управління «Док Проф» для оперативного блокування облікових записів у разі виявлення підозрілої активності. Технічні налаштування конфіденційності дозволяють створювати «віртуальні кімнати» для роботи над таємними проєктами [9].

Цілісність електронних архівів забезпечується використанням технологій довготривалого зберігання з періодичним перепідписанням документів новими ключами. Це гарантує юридичну значущість документів протягом багатьох років, незважаючи на зміну криптографічних стандартів. «Док Проф» технічно реалізує принцип мінімальних привілеїв, надаючи користувачеві лише ті права, що необхідні для виконання конкретного завдання [9]. Система автоматично розриває сесію після певного періоду неактивності користувача, запобігаючи доступу сторонніх осіб до відкритого робочого місця. Крім того, технічний захист посилюється шляхом прив'язки робочих станцій до конкретних мережевих адрес. Можливість віддаленого доступу до системи «Док Проф» у військовій частині 3077 технічно обмежена та суворо регламентована [4].

Використання системи дозволяє повністю автоматизувати контроль за життєвим циклом електронного документа від моменту генерації до архівування. Технічні звіти системи про стан документообігу дозволяють виявляти «вузькі місця» в безпеці та оперативно їх усувати. Впровадження «Док Проф» стало якісним стрибком у забезпеченні інформаційної безпеки військової частини, дозволяючи перейти від декларативного захисту до реальних технічних гарантій збереження державних таємниць. Аналіз технічних можливостей системи підтверджує її високу адаптивність до специфічних потреб Національної гвардії. «Док Проф» інтегрує в собі найкращі практики захищеного документообігу, що існують на вітчизняному ринку. Технічна надійність системи перевірена роками експлуатації в органах державної влади та силових структурах [9].

Для військової частини 3077 даний інструмент став основою для побудови безпечного цифрового середовища. Кожен технічний параметр системи спрямований на те, щоб виключити людський фактор як джерело вразливості. Надійне шифрування та суворий контроль цілісності роблять «Док Проф» нездоланним бар'єром для потенційного порушника [9]. Таким чином, технічні аспекти, закладені в основу функціонування цієї СЕДО, повністю відповідають викликам воєнного часу. Подальше вивчення особливостей системи дозволить глибше зрозуміти механізми захисту електронної документації. Аналіз підкреслює пріоритетність технічних засобів над організаційними в питаннях кіберзахисту. «Док Проф» продовжує еволюціонувати, пропонуючи нові методи протидії актуальним загрозам. Застосування цієї системи є запорукою того, що електронна документація частини залишиться цілісною та недоступною для ворога [9].

Процес накладання кваліфікованого електронного підпису у системі «Док Проф» у військовій частині 3077 починається з етапу ініціалізації документа у внутрішньому інтерфейсі користувача. Після того, як проєкт документа проходить стадію остаточного редагування та узгодження, відповідальна особа ініціює команду «Підписати». На першому етапі

алгоритму система виконує автоматичне звернення до криптографічного модуля, що інтегрований у програмну оболонку СЕДО. Програмний модуль «Док Проф» ідентифікує тип файлу та готує його до процедури хешування, яка є фундаментом цілісності даних. Хешування здійснюється з використанням стандартизованого алгоритму, наприклад, SHA-256 або актуальних національних стандартів ДСТУ [10].

Результатом цього кроку є створення унікального цифрового «відбитка» документа, який має фіксовану довжину та є чутливим до будь-якої зміни навіть одного біта інформації. Важливо підкреслити, що сам зміст документа на сервері залишається незмінним, а підписується лише цей короткий математичний код. Після генерації хешу система видає запит користувачеві на підключення захищеного носія ключової інформації (токена). У військовій частині 3077 використовуються виключно апаратні ключі, що мають експертний висновок Державної служби спеціального зв'язку та захисту інформації України [4]. Користувач вводить персональний пароль доступу до токена, що активує доступ до закритого ключа, який ніколи не покидає межі апаратного пристрою. Далі алгоритм передбачає передачу розрахованого хешу документа безпосередньо в захищену пам'ять токена. Внутрішній процесор токена виконує криптографічне перетворення цього хешу за допомогою закритого ключа підписувача.

Результатом є сформований блок даних, який власне і є електронним підписом. Блок даних повертається до системи «Док Проф», яка автоматично додає до нього службову інформацію про сертифікат підписувача. На цьому етапі до процесу підключення КЕП додається критично важливий елемент — «штамп часу» (Timestamp) [23, с.183]. Система «Док Проф» автоматично генерує запит до кваліфікованого надавача довірчих послуг (далі – КНДП), через який обслуговується військова частина. Запит містить хеш-значення вже сформованого підпису та унікальний ідентифікатор транзакції. Сервер часу КНДП, отримавши запит, додає до нього значення точного часу з еталонного джерела та засвідчує цей пакет власним електронним підписом. Отриманий

«штамп часу» повертається до військової частини 3077 через захищений канал зв'язку. Програмний комплекс «Док Проф» вбудовує цей штамп безпосередньо в структуру електронного підпису за стандартом CAdES-X-Long або аналогічним. Це технічно гарантує, що документ був підписаний саме в зазначений момент, а не заднім числом. Наявність штампа часу є юридичним доказом того, що сертифікат підписувача на момент підписання був чинним і не був відкликаним. Після завершення цієї операції підпис вважається сформованим у повному обсязі та прикріплюється до картки документа. Система «Док Проф» виконує фінальну візуалізацію підпису, додаючи на екранну форму документа QR-код або графічне зображення штампа з реквізитами підписувача [4].

Наступним етапом алгоритму є автоматична перевірка цілісності щойно створеного підпису засобами самої СЕДО. Система знову розраховує хеш документа та порівнює його з тим, що зашифрований у підписі. Якщо результати збігаються, статус документа змінюється на «Підписано», і він стає доступним для подальшої маршрутизації. У випадку розбіжності хоча б в одному символі, система негайно видає критичну помилку та блокує документ. Це унеможливлює технічну підробку розпорядчих актів усередині частини. Коли документ надходить до отримувача в іншу військову частину або в Міноборони, алгоритм перевірки повторюється автоматично. Приймаюча сторона через «Док Проф» звертається до онлайн-служб перевірки статусу сертифікатів (OCSP) [4]. Це дозволяє в режимі реального часу підтвердити, що підпис не був скомпрометований під час передачі. Штамп часу при цьому відіграє роль «якоря», який фіксує юридичну силу документа на десятиліття вперед. Навіть якщо термін дії сертифіката підписувача закінчиться через рік, штамп часу підтвердить легітимність документа на момент створення. Технічна інтеграція штампа часу виключає можливість маніпуляцій із системним часом на локальних комп'ютерах діловодів. У військовій частині 3077 це особливо важливо при фіксації бойових наказів та журналів обліку операцій [4].

Система «Док Проф» веде детальний лог-файл кожного кроку цього алгоритму, записуючи IP-адресу термінала та серійний номер токена. Будь-який технічний збій на етапі запиту до сервера часу автоматично припиняє процедуру підписання. Це забезпечує принцип «все або нічого», де неповний або пошкоджений підпис не може бути збережений. Крім того, алгоритм передбачає можливість множинного підписання документа кількома посадовими особами. Кожен наступний підписувач накладає свій КЕП поверх попереднього, утворюючи захищений ланцюжок довіри. Система зберігає всі проміжні штампи часу, що дозволяє відновити хронологію погодження документа з точністю до секунди [23, с.186]. Адміністрування цих процесів у військовій частині 3077 здійснюється згідно з регламентом безпеки, що виключає втручання в роботу криптографічного ядра. Технічна підтримка «Док Проф» забезпечує регулярне оновлення кореневих сертифікатів державних центрів у базі системи. Це гарантує безперебійність перевірки підписів, що надходять від зовнішніх контрагентів або медичних закладів. Застосування КЕП у поєднанні з Timestamp перетворює електронний документ на надійний доказ у разі судових спорів або службових розслідувань. Описаний алгоритм є стандартизованим для всіх захищених вузлів зв'язку Національної гвардії України [48].

Він забезпечує невідмовність підписувача від факту накладання підпису, що є базовим принципом військової субординації. Використання хешування гарантує, що вміст документа не був змінений шкідливим програмним забезпеченням під час збереження в базі даних. Таким чином, «Док Проф» виступає не лише як оболонка для документообігу, а як складна система криптографічного контролю. Кожен крок алгоритму — від хешування до фіксації часу — є ланкою в ланцюгу інформаційної безпеки держави. Військова частина 3077 через впровадження цього алгоритму мінімізує ризики внутрішнього фроду та витоку інформації [9]. Технічна досконалість процедури КЕП дозволяє відмовитися від громіздких паперових архівів на користь компактних електронних сховищ. При цьому надійність зберігання

даних у системі перевищує надійність фізичних сейфів завдяки дублюванню зашифрованих копій. Робота з «Док Проф» вимагає від персоналу частини лише базових навичок, оскільки всі складні криптографічні обчислення приховані «під капотом». Проте розуміння цього алгоритму є необхідним для фахівців із захисту інформації, які супроводжують роботу канцелярії [9].

Подальше вдосконалення системи передбачає перехід на ще стійкіші до квантових обчислень алгоритми шифрування в майбутньому. Вже зараз архітектура «Док Проф» дозволяє легко замінювати модулі хешування без зміни всієї логіки системи. Це робить технічне рішення у військовій частині 3077 перспективним та готовим до нових викликів кібербезпеки. Завершуючи аналіз алгоритму, слід зазначити, що автоматизація перевірки штампа часу значно розвантажує діловодів від ручної звірки дат. Система самостійно сигналізує про будь-які невідповідності в часових мітках або статусах сертифікатів. Такий підхід забезпечує безперервність та прозорість військового управління на всіх рівнях. КЕП та Timestamp у системі «Док Проф» фактично замінюють мокру печатку та фізичний підпис командира, надаючи їм цифрової незнищенності [9]. Кожне з цих речень демонструє глибину інтеграції сучасних ІТ-технологій у повсякденну діяльність військових підрозділів. Завдяки цьому військова частина 3077 стає частиною єдиного, захищеного та юридично значущого інформаційного простору України. Технічна реалізація конфіденційності та цілісності документів через описані механізми є запорукою успішного виконання завдань у цифрову епоху.

РОЗДІЛ ІІІ. НАПРЯМИ ОПТИМІЗАЦІЇ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ У СТРУКТУРНОМУ ПІДРОЗДІЛІ ВІЙСЬКОВОЇ ЧАСТИНІ 3077 НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

3.1. Шляхи подолання організаційних та технічних бар'єрів при роботі з електронними документами

У сучасному безпековому середовищі цифровізація військового управління є не просто технологічним трендом, а стратегічною необхідністю для забезпечення оперативності та точності прийняття управлінських рішень. Проте впровадження систем електронного документообігу у специфічних умовах військових частин Національної гвардії України супроводжується низкою системних викликів [48]. Теоретичний аналіз проблеми дозволяє класифікувати ці перешкоди на два основні блоки: організаційні та технічні, які у своїй сукупності створюють так званий «бар'єр впровадження».

Так, організаційні бар'єри часто є більш складними для подолання, оскільки вони безпосередньо пов'язані з людським фактором та усталеною корпоративною культурою військової організації. Консервативність військової ієрархії та сувора регламентація процесів іноді вступають у протиріччя з гнучкістю, яку вимагають сучасні цифрові інструменти [5, с.278]. Не завжди повна відмова від традиційних паперових носіїв породжує явище «паралельного документообігу», що лише подвоює робоче навантаження на виконавців. Подекуди, неналежно продумані алгоритми взаємодії між підрозділами в електронному форматі призводять до розмивання персональної відповідальності за кінцевий результат.

Важливим організаційним аспектом є також недосконалість внутрішньої нормативної бази, яка не завжди встигає адаптуватися до швидких змін у технологічному ландшафті. Проблема дублювання функцій та надмірної бюрократизації процедур узгодження документів в електронному середовищі часто нівелює ключову перевагу системи е-документообігу — швидкість [5,

с.234]. Переходячи до технічної площини, слід зазначити, що інфраструктурні обмеження залишаються базовою перешкодою для повноцінного функціонування системи у військовому секторі. Недостатня потужність наявного апаратного забезпечення та застарілі канали зв'язку в окремих структурних підрозділах часто унеможливлюють швидкий обмін об'ємними файлами. Проблема інтероперабельності, тобто здатності різних програмних комплексів до безперешкодної взаємодії, є однією з найгостріших у військовій сфері [5, с.235].

Складність інтеграції спеціалізованих систем захисту інформації з користувацькими інтерфейсами часто знижує зручність роботи для кінцевого споживача. Питання кібербезпеки та захисту державної таємниці накладають жорсткі обмеження на архітектуру СЕД, що іноді призводить до технічної ізольованості окремих сегментів мережі. Використання кваліфікованих електронних підписів потребує безперебійної роботи сервісів довірчих послуг, що в умовах бойової підготовки чи кризових ситуацій може бути ускладнено. Технічні помилки в програмному коді або незручна логіка побудови інтерфейсу створюють додаткове когнітивне навантаження на військовослужбовців підрозділу. Відсутність єдиних стандартів метаданих для специфічних військових документів призводить до суттєвих труднощів при автоматизованому пошуку та архівуванні інформації [5, с.236].

Бар'єром також є обмеженість ресурсів для постійної технічної підтримки та оперативного оновлення спеціалізованого програмного забезпечення. Синергія організаційних та технічних проблем створює ефект «замкненого кола», де технічна недосконалість часто виправдовує організаційний саботаж або інертність. Для військової частини 3077 ці аспекти мають особливе значення з огляду на специфіку її функціонального призначення та значні обсяги щоденних документопотоків [4]. Подолання організаційних бар'єрів вимагає не лише впровадження нових інструкцій, а й докорінної зміни філософії управління інформаційними активами всередині частини.

Технічна модернізація повинна ґрунтуватися на принципах модульності та масштабованості, що дозволить системі адаптуватися до нових викликів без повної заміни ядра [5, с.329]. На нашу думку, важливо розуміти, що автоматизація хаосу призводить лише до автоматизованого хаосу, тому реінжиніринг процесів має передувати інсталяції програмного продукту. Навчання персоналу має стати безперервним процесом, а не разовою акцією під час безпосереднього впровадження системи. Створення єдиного інформаційного простору всередині військової частини дозволить мінімізувати втрати часу на рутинний пошук та погодження документів. Мінімізація впливу технічних збоїв досягається шляхом резервування каналів зв'язку та впровадження засобів моніторингу працездатності мережі в реальному часі. Ефективне вирішення проблеми бар'єрів лежить у площині комплексного підходу, де технології та організаційна структура працюють як єдиний збалансований механізм.

Організаційна стійкість канцелярії військової частини 3077 в умовах постійних зовнішніх загроз та енергетичної нестабільності стає фундаментом безперебійного функціонування всієї системи військового управління. Першочерговим шляхом подолання організаційних бар'єрів є розробка та впровадження спеціалізованого Регламенту роботи в особливих умовах, який чітко визначає пріоритетність обробки документів залежно від безпекової ситуації. Впровадження системи «гнучкого реагування» дозволяє персоналу канцелярії миттєво переходити від стандартних процедур до протоколів критичного режиму без втрати контролю над документообігом [5, с.235]. Організаційним рішенням для нівелювання наслідків відключень електроенергії є запровадження методу «асинхронної обробки», де кожен виконавець має чіткий перелік завдань, що не потребують постійного підключення до мережі.

Важливим аспектом є створення інституту «чергових координаторів» всередині канцелярії, які забезпечують синхронізацію паперових та електронних потоків у моменти відновлення живлення [5, с.334]. Подолання

бар'єрів вимагає чіткого розподілу обов'язків між співробітниками щодо негайної архівації та вивантаження критично важливих баз даних у захищені офлайн-сховища. Для забезпечення безперервності процесів у зимовий період необхідно переглянути графіки робочих змін, адаптуючи їх до світлового дня та прогнозних графіків обмеження енергопостачання.

Організаційна структура канцелярії має стати більш горизонтальною, що дозволить молодшому персоналу приймати оперативні рішення щодо маршрутизації документів у разі відсутності зв'язку з керівництвом. Впровадження системи «подвійного контрольного сліду» забезпечує фіксацію реєстраційних даних у локальних реєстрах, які згодом автоматично синхронізуються з центральною базою СЕД [4]. Особлива увага приділяється створенню алгоритмів взаємодії з іншими підрозділами частини, які базуються на принципах мінімально необхідного підтвердження для виконання термінових розпоряджень. Організаційний бар'єр, спричинений загрозою фізичного знищення серверної інфраструктури, долається шляхом впровадження протоколів територіально розподіленого зберігання інформації. Необхідно розробити чітку інструкцію щодо дій персоналу канцелярії під час оголошення повітряної тривоги, яка включає обов'язкове збереження чернеток та блокування робочих станцій [21, с. 158].

Шлях до оптимізації лежить через створення мобільних робочих груп, оснащених автономними засобами роботи, які можуть функціонувати в обладнаних укриттях. Важливим кроком є легітимізація спрощених форм електронного погодження для внутрішніх документів, що не мають стратегічного значення, з метою економії часу в періоди наявності зв'язку. Організація роботи канцелярії в умовах енергодефіциту потребує впровадження системи пріоритетних «цифрових вікон», коли всі ресурси спрямовуються виключно на відправку бойових наказів та термінових донесень. Впровадження матричної системи відповідальності дозволяє дублювати функції ключових реєстраторів, що мінімізує ризики зупинки документообігу через відсутність окремих посадових осіб [21, с.159].

Для подолання бар'єру фрагментарності інформації слід запровадити практику щоденних ранкових нарад з коротким плануванням документопотоків на випадок зникнення зв'язку [5, с.345]. Організаційним заходом є також завчасна підготовка шаблонів критичних документів у форматах, що потребують мінімального мережевого трафіку для передачі. Слід розробити систему маркування документів за рівнем енергозалежності, де першочергово обробляються ті, що потребують доступу до зовнішніх державних реєстрів. Важливим елементом подолання організаційних перешкод є створення внутрішньої «бази знань» щодо альтернативних способів передачі інформації у разі виходу з ладу основної системи. Необхідно впровадити протокол «цифрової тиші», який передбачає обмеження другорядного листування в години пікових навантажень на енергомережу частини [5, с.367].

Організаційна модель канцелярії має передбачати можливість швидкого розгортання резервного пункту обробки документів у безпечній локації. Важливим шляхом є автоматизація процесів звітності про стан виконання документів, що дозволяє керівництву бачити реальну картину завантаженості в умовах перебоїв. Слід запровадити систему ротації персоналу між фізичним прийомом документів та їх цифровою обробкою для запобігання перевтомі в умовах постійного стресу. Організаційний бар'єр недовіри до електронної форми в умовах загрози кібератак долається шляхом регулярного інструктування щодо посилених заходів автентифікації. Необхідно інтегрувати в роботу канцелярії принципи «бережливого документообігу», відсікаючи зайві етапи погодження, які лише затягують час у критичні моменти. Створення єдиного регламенту дій при раптовій втраті доступу до хмарних сервісів забезпечує стабільність роботи канцелярії як єдиного механізму [5, с.389].

Шляхом оптимізації є впровадження практики локального кешування робочих документів на захищених робочих станціях, що дозволяє продовжувати роботу без інтернету. Важливо встановити чіткі терміни

«наздоганяючої реєстрації» для документів, що були опрацьовані в офлайн-режимі під час відключень світла. Організація регулярних тренувань персоналу щодо дій у сценарії «повного блекауту» дозволяє відпрацювати навички координації без використання цифрових інструментів. Для військової частини 3077 критичним є створення протоколу взаємодії з вищим командуванням щодо підтвердження отримання електронних документів альтернативними каналами [4].

Шлях до подолання бар'єрів лежить через розширення повноважень начальника канцелярії у сфері оперативного управління черговістю обробки кореспонденції. Необхідно запровадити систему візуального моніторингу статусу виконання завдань, яка залишається доступною для аналізу навіть при обмежених технічних ресурсах. Важливим організаційним рішенням є стандартизація назв файлів та описів документів, що критично важливо для швидкого пошуку в умовах обмеженого часу роботи техніки. Подолання бар'єру перевантаженості каналів зв'язку досягається через організаційну заборону на передачу важких медіафайлів без крайньої операційної потреби. Слід розробити систему «гарячого резервування» робочих місць, де кожен комп'ютер у підрозділі може бути швидко налаштований для потреб канцелярії [23].

Організаційне забезпечення передбачає створення графіку регулярного оновлення офлайн-копій нормативно-правової бази, необхідної для щоденної роботи. Важливим аспектом є впровадження етичного кодексу внутрішньої комунікації в умовах війни, що сприяє підтримці високої дисципліни документування. Шляхом подолання бар'єрів є створення системи «розумних сповіщень», які інформують виконавців про критичні терміни лише за найважливішими документами. Необхідно забезпечити організаційну підтримку постійного зв'язку між канцелярією та ІТ-підрозділом для миттєвого реагування на технічні інциденти. Слід передбачити процедуру верифікації цілісності даних після кожного аварійного вимкнення обладнання як обов'язковий етап робочого процесу [23].

Організаційна гнучкість досягається через можливість делегування права підпису документів у разі неможливості доступу основного підписанта до засобів КЕП. Важливим є впровадження системи «контрольних точок» протягом дня, коли персонал звіряє статус виконання найбільш пріоритетних завдань. Подолання бар'єрів вимагає перегляду внутрішніх положень про канцелярію з метою відображення в них специфіки роботи в умовах воєнного стану [23]. Організація процесу має бути спрямована на мінімізацію фізичного переміщення персоналу між будівлями під час небезпеки, максимально використовуючи внутрішню мережу. Слід впровадити практику використання заздалегідь підготовлених паперових реєстрів-дублерів, які заповнюються в укриттях під час обстрілів. Важливим шляхом є розробка логістичної схеми передачі фізичних носіїв інформації між підрозділами у разі повної відсутності зв'язку.

Організаційний бар'єр бюрократичної тяганини долається через впровадження принципу «мовчазної згоди» для певних категорій технічних документів [23]. Слід забезпечити персоналу канцелярії доступ до засобів індивідуального захисту безпосередньо на робочому місці, що підвищує їхню впевненість та продуктивність. Організаційна стійкість підсилюється через створення системи взаємодопомоги між діловодами різних структурних підрозділів частини. Важливо запровадити механізм швидкого інформування контрагентів та суміжних частин про зміну режиму роботи канцелярії через технічні причини. Шляхом оптимізації є впровадження автоматизованих черг обробки документів, які самостійно ранжують кореспонденцію за ступенем важливості. Необхідно розробити регламент повернення до нормального режиму роботи після тривалих періодів відсутності енергопостачання. Організаційні заходи мають включати регулярний аудит стану захищеності електронних документів від несанкціонованого доступу в моменти технічної вразливості [23].

Важливим є створення системи мотивації для персоналу, який забезпечує виконання завдань у надскладних умовах, що підтримує високий

моральний дух. Шляхом подолання бар'єрів є впровадження протоколів синхронізації з хмарними сховищами у періоди найменшого завантаження мережі. Необхідно забезпечити чітку нумерацію та індексацію документів, що унеможливлює появу дублікатів при паралельній роботі кількох співробітників. Організаційна структура канцелярії повинна передбачати наявність «офіцера з безпеки даних», відповідального за цілісність архівів під час евакуаційних заходів [12]. Слід розробити систему адаптивних інтерфейсів СЕД, які потребують менше енергії та системних ресурсів для роботи на мобільних пристроях. Важливим кроком є легалізація використання месенджерів із наскрізним шифруванням як допоміжного засобу координації роботи канцелярії.

Організаційний бар'єр обмеженості ресурсів долається через централізацію функцій друку та сканування в одному найбільш захищеному та забезпеченому енергією місці. Слід впровадити практику «чистого столу» наприкінці кожної зміни, що дозволяє швидко розпочати роботу новій зміні в будь-яких умовах [12]. Важливим шляхом є створення електронної бібліотеки типових помилок, що виникають при роботі в екстремальних умовах, для їх оперативного усунення. Організаційна підтримка включає регулярне проведення психологічних тренінгів для персоналу щодо збереження концентрації під час зовнішніх загроз. Слід запровадити систему автоматичного резервного копіювання на рівні окремих робочих папок, що мінімізує втрати при раптових відключеннях. Важливим є організаційне закріплення обов'язку кожного виконавця перевіряти статус доставлення електронного листа через альтернативні канали.

Подолання бар'єрів вимагає чіткого визначення переліку документів, які в жодному разі не можуть бути переведені у виключно електронну форму. Організація роботи має передбачати можливість швидкого переходу на ручне керування процесами у разі тотальної відмови цифрових систем. Слід впровадити систему пріоритетного доступу до зарядних станцій для пристроїв, задіяних у критичному документообігу [12]. Важливим шляхом є

розробка та затвердження внутрішніх стандартів оформлення документів, що дозволяють зменшити їх цифрову вагу. Організаційна підготовка включає створення детальних схем підключення периферійного обладнання до альтернативних джерел живлення. Слід забезпечити наявність у канцелярії запасу паперових носіїв та канцелярського приладдя як критичного резерву для надзвичайних ситуацій.

Важливим аспектом є організація постійного зворотного зв'язку від виконавців щодо зручності роботи з СЕД у стресових умовах. Подолання бар'єрів забезпечується через впровадження системи централізованого оновлення ключів КЕП, що виключає затримки через закінчення терміну їх дії [21, с.159]. Організаційна модель повинна враховувати можливість віддаленої роботи окремих фахівців, якщо це дозволяє рівень доступу та безпекова ситуація. Слід запровадити практику періодичного «контрольного відключення» для перевірки готовності персоналу до роботи без світла та інтернету. Важливим шляхом є створення інтерактивних інструкцій-карт, які допомагають швидко орієнтуватися в процедурах при зміні оперативної обстановки.

Організаційне забезпечення включає розробку планів евакуації не лише персоналу, а й технічних носіїв інформації та паперових архівів. Слід впровадити систему ідентифікації терміновості документів за допомогою кольорових кодів у заголовках електронних листів. Важливим є встановлення регламенту періодичної санітарної очистки електронних поштових скриньок для підтримки їхньої швидкодії. Подолання організаційних бар'єрів вимагає постійного аналізу досвіду інших підрозділів НГУ, що працюють у подібних умовах. Організація роботи має базуватися на принципі надлишковості каналів інформування про важливі розпорядження [48].

Слід запровадити обов'язкове тестування нових організаційних процедур на маленьких групах перед їх повним впровадженням. Важливим кроком є створення реєстру «критичних завдань дня», який ведеться в офлайн-форматі та доступний усім співробітникам канцелярії. Організаційна

підтримка передбачає наявність чітких інструкцій щодо відновлення пошкоджених файлів після системних збоїв. Слід впровадити практику щотижневого підбиття підсумків роботи в умовах загроз для виявлення слабких місць у процедурах. Важливим шляхом є мінімізація кількості погоджувальних підписів для внутрішніх документів, що не впливають на бойову готовність. Організаційна структура має бути адаптована до можливості тривалого автономного функціонування без зв'язку з центральним сервером [55].

Необхідно забезпечити персонал канцелярії засобами автономного освітлення робочих місць, що дозволяє працювати з паперовими оригіналами в укриттях. Важливим аспектом є впровадження системи швидкого навчання нових співробітників специфічним алгоритмам роботи в особливий період. Подолання бар'єрів забезпечується через інтеграцію елементів автоматизації в процеси сортування вхідної кореспонденції за ключовими словами. Організаційна модель повинна стимулювати ініціативу персоналу щодо пропозицій із вдосконалення робочого простору, запровадити регламент перевірки актуальності контактних даних усіх посадових осіб, задіяних у документообігу. Важливим шляхом є створення єдиного вікна подачі звернень для військовослужбовців, що спрощує логістику документів усередині частини. Організаційне забезпечення включає розробку сценаріїв реагування на втрату цілісності окремих сегментів електронного архіву, впровадити практику дублювання реєстраційних номерів у спеціальних книгах обліку, які не потребують живлення [55].

Важливим кроком є переведення більшості внутрішніх розпоряджень у формат коротких повідомлень, що полегшує їх обробку. Організаційна гнучкість дозволяє перерозподіляти навантаження між діловодами залежно від фактичної наявності електроенергії в їхніх секторах, забезпечити наявність чіткого маркування на системних блоках та серверах для їхньої першочергової евакуації [12]. Важливим шляхом є впровадження культури відповідального ставлення до ресурсів техніки, що подовжує термін її служби в екстремальних

умовах. Організаційна підтримка включає моніторинг стану здоров'я та психологічного навантаження співробітників канцелярії, запровадження системи щогодинних перерв для розвантаження персоналу в періоди інтенсивної роботи при свічках чи ліхтарях.

Важливим є встановлення пріоритетності фізичної доставки документів у межах частини під час тривалих блекаутів [12]. Подолання бар'єрів вимагає узгодження дій канцелярії з планами територіальної оборони та охорони об'єктів військової частини. Організаційна модель повинна бути спрямована на максимальне збереження спадкоємності управлінської інформації. Слід впровадити систему автоматичного формування звітів про документи, термін виконання яких спливає найближчим часом. Важливим шляхом є створення захищених зон для роботи з документами, що містять обмежений доступ, у загальних укриттях [12]. Організаційне забезпечення передбачає регулярну заміну паролів та перевірку прав доступу в умовах підвищеної шпигунської загрози. Слід запровадити практику створення стислих анотацій до довгих документів для прискорення їхнього вивчення керівництвом.

Важливим кроком є розробка карти ризиків для кожного етапу документообігу в умовах зими та обстрілів. Організаційна стійкість канцелярії досягається через постійне вдосконалення внутрішніх інструкцій на основі реальних кейсів подолання криз, максимальної прозорості процесів проходження документів для всіх зацікавлених сторін навіть у складних умовах [12]. Важливим шляхом є інтеграція принципів кібергігієни в щоденну рутину кожного працівника канцелярії військової частини 3077. Організаційна готовність до змін є запорукою успішної трансформації електронного документообігу в надійний інструмент військового управління. Таким чином, комплекс організаційних заходів дозволяє перетворити зовнішні загрози на стимули для створення більш міцної та адаптивної системи. Тільки через гармонізацію регламентів, відповідальності та людського фактору можливо досягти ефективності канцелярії в сучасних реаліях.

3.2. Перспективи впровадження хмарних технологій та посилення кібербезпеки в системі електронного документообігу підрозділів Національної гвардії України

У сучасній архітектурі цифрових систем управління хмарні технології розглядаються як фундаментальна парадигма, що забезпечує динамічне надання обчислювальних ресурсів та сервісів через мережу за запитом користувача. Теоретична суть хмарних рішень полягає у переході від локального володіння апаратною інфраструктурою до використання віртуалізованих середовищ, що характеризуються високим рівнем масштабованості та доступності. Для військових підрозділів Національної гвардії України впровадження хмарних моделей стає стратегічним кроком на шляху до створення гнучкої та відмовостійкої системи електронного документообігу [48]. Основними характеристиками хмарних технологій є самообслуговування за запитом, широкий мережевий доступ, об'єднання ресурсів у пули, миттєва еластичність та вимірюваність сервісів.

Застосування приватних хмар у межах захищеного контуру НГУ дозволяє централізувати обробку даних, нівелюючи ризик втрати інформації через фізичне знищення локальних серверних потужностей у структурних підрозділах [52]. Хмарні обчислення забезпечують можливість доступу до електронних документів з будь-якої точки, де є зв'язок, що є критично важливим для мобільних груп та оперативних штабів у польових умовах. Такий підхід трансформує концепцію робочого місця діловода, роблячи його незалежним від конкретної фізичної адреси чи стаціонарного комп'ютера. Використання хмарної моделі дозволяє значно прискорити процеси спільного редагування та погодження проєктів наказів, оскільки всі учасники працюють з єдиною актуальною копією документа у віртуальному просторі [5, с.398].

Організаційна гнучкість хмарних сервісів сприяє швидкому розгортанню додаткових модулів СЕД у разі зміни чисельності особового складу або створення нових структурних одиниць. Важливим аспектом є

економічна ефективність, адже хмарні рішення дозволяють оптимізувати витрати на технічне обслуговування локальних мереж та оновлення застарілого парку техніки. Проте впровадження «хмар» у військовій сфері нерозривно пов'язане з питанням кібербезпеки, оскільки концентрація даних в одному віртуальному сховищі створює нові вектори загроз. Кібербезпека в хмарному середовищі базується на принципах багаторівневого захисту, включаючи шифрування даних на етапах їх передачі та зберігання [21, с.159].

Використання сучасних алгоритмів криптографічного захисту інформації дозволяє забезпечити конфіденційність військового листування навіть у разі перехоплення трафіку зловмисниками. Хмарна інфраструктура надає розширені можливості для автоматизованого моніторингу спроб несанкціонованого доступу та аномальної активності користувачів у системі. Важливим елементом посилення безпеки є впровадження строгих протоколів автентифікації, які поєднують використання електронних підписів та біометричних факторів. Хмарні технології також полегшують процес створення резервних копій, що автоматично розподіляються між різними географічно віддаленими дата-центрами, гарантуючи цілісність архівів військової частини навіть у сценарії тотального блекауту чи прямого влучання в об'єкт інфраструктури [21, с.165].

Інтеграція хмарних рішень вимагає відповідності державним стандартам у сфері захисту інформації, зокрема створення комплексної системи захисту інформації. Перспективи розвитку СЕД у підрозділах НГУ полягають у переході до гібридних моделей, де найбільш критичні дані зберігаються локально, а оперативний документообіг виноситься у захищену хмару. Хмарне середовище дозволяє впроваджувати елементи штучного інтелекту для автоматичного сортування та аналізу великих масивів військової документації. Посилення кібербезпеки передбачає не лише технічні заходи, а й формування культури «цифрової гігієни» серед усіх учасників документообігу. Створення єдиного хмарного реєстру документів для всієї

структури НГУ забезпечить безпрецедентну прозорість та керованість процесами на всіх рівнях ієрархії [12].

Перехід на хмарні рейки дозволяє усунути проблему фрагментарності даних, коли різні підрозділи використовують несумісні між собою локальні версії програмного забезпечення. Автоматизація оновлень безпеки на центральному рівні хмари гарантує, що кожен користувач працює в найбільш захищеній версії системи. Використання хмарних обчислень є фундаментом для майбутньої інтеграції українських військових систем з аналогічними платформами країн-партнерів НАТО [52]. Еластичність хмарних ресурсів дозволяє системі документообігу витримувати пікові навантаження, які виникають у періоди активних бойових дій чи мобілізаційних заходів. Віртуалізація функцій канцелярії підвищує живучість управлінського апарату в умовах ведення гібридної війни. Підсумовуючи, хмарні технології слід розглядати не як альтернативу традиційним методам, а як необхідну еволюційну стадію розвитку військового діловодства. Тільки через поєднання переваг хмарної інфраструктури та безкомпромісного кіберзахисту можна досягти нового рівня ефективності функціонування канцелярії військової частини 3077. Подальший аналіз дозволить виокремити конкретні кроки щодо реалізації цього потенціалу з урахуванням специфіки завдань Національної гвардії України.

Перспективи цифровізації військової частини 3077 у контексті використання хмарних технологій відкривають принципово нові можливості для підвищення живучості системи управління в умовах інтенсивної збройної агресії [4]. Впровадження моделі «приватної хмари» Національної гвардії України дозволить підрозділу відійти від вразливої практики локального зберігання критично важливих даних на окремих фізичних серверах. Основна перспектива полягає у створенні територіально розподіленої інфраструктури, де копії документів автоматично реплікуються між захищеними дата-центрами в різних регіонах країни.

Підхід гарантує, що навіть у разі повного фізичного знищення адміністративної будівлі канцелярії, доступ до електронного архіву буде відновлено за лічені хвилини з будь-якого резервного пункту. Крім того, хмарна модель забезпечує миттєву масштабованість ресурсів СЕД у моменти різкого збільшення обсягів документообігу під час мобілізаційних чи оперативно-бойових заходів [4]. Важливою перспективою є перехід на використання «тонких клієнтів» у роботі діловодів, що значно знижує вимоги до обчислювальної потужності локальних комп'ютерів та спрощує їх заміну в разі виходу з ладу. Енергоефективність хмарної архітектури стає критичною перевагою, оскільки основне навантаження з обробки даних переноситься на віддалені сервери, що дозволяє локальним пристроям довше працювати від автономних джерел живлення.

У сфері кібербезпеки основною перспективою є впровадження концепції «нульової довіри», де кожен запит на доступ до документа підлягає обов'язковій багатофакторній верифікації [52]. Це дозволить мінімізувати ризики, пов'язані з компрометацією окремих облікових записів чи фізичним захопленням робочих станцій супротивником. Важливим напрямом є інтеграція в СЕД засобів наскрізного шифрування даних, що унеможливлює зчитування інформації навіть у разі успішного перехоплення трафіку на рівні провайдера зв'язку. Перспективним є впровадження системи автоматичного виявлення аномальної активності користувачів на основі алгоритмів машинного навчання, які здатні ідентифікувати нетипову поведінку в реальному часі. Створення централізованого вузла управління ключами електронного підпису в хмарі дозволить оперативно відкликати сертифікати скомпрометованих посадових осіб, блокуючи їм доступ до системи [52].

Більше того, хмарні технології відкривають шлях до створення мобільних додатків СЕД із підвищеним рівнем захисту для використання на планшетах командирів у польових умовах. Це дозволить оперативно отримувати та підписувати розпорядження безпосередньо в районах виконання завдань, забезпечуючи безперервність управління. Перспектива

впровадження технології контейнеризації додатків дозволить ІТ-фахівцям військової частини 3077 швидко розгортати нові модулі СЕД, адаптовані під специфічні потреби конкретних служб [4]. Важливим кроком стане автоматизація процесів резервного копіювання за графіком «hot backup», що виключає ризик втрати даних, створених у проміжку між плановими архіваціями.

Розвиток кібербезпеки передбачає також впровадження системи ізоляції браузерів та віртуальних робочих столів, що захищає внутрішню мережу частини від проникнення шкідливого програмного забезпечення через інтернет. Перспективним є створення єдиного віртуального сховища для мультимедійних матеріалів, які супроводжують звіти про виконання бойових завдань, із чітким розмежуванням прав доступу. Використання хмарних технологій дозволить впровадити інтелектуальні системи пошуку за змістом документів, що значно скоротить час на підготовку аналітичних довідок для командування. Крім технічних аспектів, хмарна трансформація сприятиме уніфікації регламентів документообігу між різними військовими частинами НГУ, створюючи єдиний інформаційний простір [4].

У контексті кіберзахисту актуальною є перспектива впровадження засобів Data Loss Prevention, які автоматично блокуватимуть спроби пересилання таємних документів за межі захищеного периметру [55]. Важливим напрямом є використання блокчейн-технологій для забезпечення незмінності журналів аудиту, що дозволить абсолютно точно відстежувати історію змін кожного документа. Хмарні рішення дозволять реалізувати функцію «відкладеного підпису», коли офіцер може опрацювати документи в офлайні, а система автоматично синхронізує та підпише їх при появі стабільного зв'язку. Розвиток інфраструктури відкритого ключа в межах хмарної платформи підвищить юридичну значущість електронного листування з цивільними установами та іншими силовими структурами. Перспектива інтеграції СЕД із системами супутникового зв'язку типу Starlink

забезпечить стабільну роботу хмарних сервісів навіть за умови повного знищення наземної телекомунікаційної мережі [55].

Посилення кібербезпеки також включає в себе регулярне проведення автоматизованих «тестів на проникнення», що дозволить виявляти вразливості системи до того, як ними скористається ворог. Хмарні технології дозволять автоматизувати процес оновлення антивірусних баз на всіх пристроях підрозділу одночасно, не потребуючи ручного втручання адміністраторів. Впровадження криптографічних протоколів нового покоління забезпечить стійкість системи до майбутніх загроз з боку квантових обчислень. Важливим аспектом є створення персоналізованих «цифрових кабінетів» для кожного військовослужбовця, де він зможе отримувати довідки та подавати рапорти в електронному вигляді через захищену хмару [55].

Перспектива використання штучного інтелекту для класифікації вхідної кореспонденції за рівнем важливості дозволить начальнику канцелярії зосередитися на найбільш пріоритетних завданнях. Хмарна архітектура спрощує процедуру передачі справ при ротації кадрів, оскільки вся історія листування та напрацювань залишається доступною наступнику в структурованому вигляді. Посилення кібербезпеки у військовій частині 3077 передбачає також впровадження систем контролю фізичного доступу до серверних приміщень, інтегрованих із загальною системою моніторингу безпеки [4]. Створення резервних каналів передачі даних із використанням радіорелейних ліній підвищить доступність хмарних сервісів у складних умовах радіоелектронної боротьби. Як ми зазначали вище, важливою перспективою є впровадження стандартів НАТО щодо обміну військовою інформацією, що вимагає високого рівня сумісності хмарних систем.

Хмарні технології дозволять оптимізувати роботу архівного підрозділу частини, перевівши довгострокове зберігання документів у цифрові репозиторії з гарантованою цілісністю. Розвиток системи передбачає створення інструментів для візуалізації документопотоків у реальному часі, що допоможе виявляти «вузькі місця» в організаційній структурі. Перспектива

впровадження чат-ботів у внутрішній мережі СЕД дозволить персоналу отримувати швидкі відповіді на питання щодо правильного оформлення складних документів. У сфері захисту інформації актуальним є використання апаратних токенів та смарт-карт для фізичної ідентифікації користувачів під час входу в систему [23, с.184].

Хмарне середовище дозволяє реалізувати механізм «самоочищення» тимчасових файлів та кешу після завершення сесії, що запобігає витоку даних через тимчасові носії. Інтеграція засобів стеганографії дозволить додавати невидимі водяні знаки до документів, що допоможе ідентифікувати джерело витоку в разі фотографування екрана монітора. Перспективним є впровадження системи пріоритезації мережевого трафіку (QoS), яка віддаватиме перевагу пакетам даних СЕД над менш критичними сервісами. Хмарні рішення дозволять військовій частині 3077 відмовитися від складного процесу утилізації старих жорстких дисків із секретною інформацією, оскільки дані не зберігатимуться на місцях постійно [23, с.186]. Створення внутрішньої «пісочниці» для перевірки вкладень у вхідних електронних листах значно знизить ризик зараження мережі вірусами-шифрувальниками. Важливим напрямом є розвиток системи електронного аудиту, яка автоматично перевірятиме документи на відповідність вимогам чинного законодавства та внутрішніх наказів. Перспектива впровадження віртуальних приватних мереж (VPN) нового покоління забезпечить надійне з’єднання між штабом частини та віддаленими блокпостами чи позиціями [23, с.187].

Хмарні технології сприятимуть розвитку системи дистанційного навчання персоналу канцелярії новим методам роботи та кібергігієни. Посилення безпеки також полягає в автоматичному блокуванні доступу до системи з пристроїв, на яких виявлено ознаки несанкціонованої модифікації операційної системи. Створення системи сповіщень про критичні зміни в документах через захищені канали зв'язку підвищить швидкість реакції посадових осіб на нові вказівки. Перспектива впровадження технології Federated Identity Management дозволить використовувати єдиний логін та

пароль для доступу до всіх державних військових реєстрів через СЕД. Використання хмарних обчислень дозволить значно скоротити час на проведення щорічних інвентаризацій документів за рахунок автоматизованої звірки реєстрів [55].

Розвиток системи кібербезпеки передбачає впровадження «пасток» (honeypots) для зловмисників, які дозволяють виявляти факт проникнення в мережу на ранніх стадіях. Хмарна інфраструктура забезпечує можливість швидкого перемикання між різними провайдерами інтернету для підтримки стабільного зв'язку в умовах активного радіоелектронного придушення. Важливою перспективою є розробка власних програмних модулів, які враховують специфіку діяльності саме Національної гвардії України [48]. Хмарні рішення дозволять автоматизувати збір статистики про продуктивність роботи кожного діловода, що сприятиме більш справедливому розподілу навантаження. Посилення кібербезпеки включає також контроль за використанням USB-портів та інших інтерфейсів на робочих станціях за допомогою спеціалізованого програмного забезпечення. Створення централізованого хмарного сховища нормативно-правових актів забезпечить усіх військовослужбовців актуальною інформацією в будь-який час [12].

Перспектива впровадження електронних обхідних листів та журналів видачі майна через СЕД значно спростить внутрішню логістику підрозділу. Використання хмарних технологій дозволить військовій частині 3077 брати участь у спільних цифрових навчаннях із іншими підрозділами сектору безпеки та оборони. Посилення захисту передбачає впровадження системи геофенсингу, яка обмежує доступ до СЕД лише певною географічною зоною розташування частини. Перспективним є впровадження інструментів автоматичного перекладу документів, що необхідно для оперативної взаємодії з іноземними інструкторами та партнерами. Хмарна модель дозволяє реалізувати концепцію «віртуального штабу», де робота над документом не припиняється навіть під час переміщення підрозділу в інший район [12].

Розвиток кібербезпеки вимагає постійного оновлення стратегії захисту відповідно до появи нових видів кіберзброї. Важливим кроком є легалізація використання хмарних сервісів на рівні відомчих нормативних актів НГУ, що зніме юридичні бар'єри для їх впровадження. Хмарні технології забезпечать можливість інтеграції СЕД із системами ситуаційної обізнаності, дозволяючи автоматично додавати оперативну інформацію до звітів. Посилення кіберзахисту передбачає також навчання персоналу розпізнаванню методів соціальної інженерії та фішингу [12]. Створення надійної хмарної платформи стане фундаментом для переходу частини на повністю безпаперовий документообіг у майбутньому. Перспектива впровадження системи інтелектуального розпізнавання відсканованих копій дозволить швидко перетворювати старі паперові архіви у зручний цифровий формат. Хмарні рішення дозволяють реалізувати багаторівневу систему підтвердження видалення документів, що виключає випадкову втрату цінної інформації [12].

Розвиток системи передбачає створення мобільного пункту управління з повноцінним доступом до всіх хмарних сервісів СЕД. Посилення кібербезпеки також полягає в обмеженні доступу до системи в позаробочий час для осіб, які не задіяні в добових нарядах чи бойовому чергуванні. Хмарна архітектура дозволяє впровадити систему автоматичного контролю за термінами зберігання документів та їх своєчасним знищенням. Важливою перспективою є розробка уніфікованих інтерфейсів користувача, які будуть однаково зручними як на десктопах, так і на мобільних пристроях. Хмарні технології відкривають можливості для дистанційного аудиту стану діловодства вищими штабами без необхідності фізичного виїзду перевіряючих. Посилення захисту інформації у військовій частині 3077 базуватиметься на комплексному поєднанні технічних, організаційних та правових заходів [4]. Перспектива впровадження засобів квантового розподілу ключів може стати наступним кроком у забезпеченні абсолютної секретності зв'язку.

Хмарні рішення дозволять автоматизувати процес підготовки нагородних листів та інших кадрових документів, мінімізуючи людські помилки. Розвиток кібербезпеки передбачає створення власної команди швидкого реагування на комп'ютерні інциденти (CSIRT) безпосередньо в структурі підрозділу [21, с.164]. Хмарна модель забезпечує прозорість бюджетних витрат на ІТ-інфраструктуру, дозволяючи платити лише за фактично спожиті обчислювальні потужності. Перспектива інтеграції СЕД із системами електронної пошти державних органів спростить офіційне листування та прискорить розгляд запитів.

Посилення безпеки включає в себе регулярну перевірку цілісності програмного коду СЕД на наявність недокументованих можливостей (бекдорів) [12]. Хмарні технології сприятимуть створенню системи колективної роботи над складними проектами реформування підрозділу. Перспектива впровадження біометричної ідентифікації при вході в особливо захищені сегменти хмари підвищить рівень персональної відповідальності. Хмарна інфраструктура дозволяє реалізувати механізм автоматичного відновлення системи після будь-яких збоїв без залучення вузькопрофільних спеціалістів. Важливим напрямом є створення інтерактивних звітів для командування, які відображають динаміку документообігу в зручних графічних форматах. Посилення кібербезпеки вимагає постійної взаємодії з кіберполіцією та іншими спецслужбами для обміну даними про нові загрози. Хмарні рішення дозволять військовій частині 3077 стати лідером цифрової трансформації серед підрозділів Національної гвардії [4].

Перспектива повної відмови від паперових журналів реєстрації на користь їх цифрових аналогів у хмарі значно звільнить робочий простір канцелярії. Використання хмарних обчислень є незворотнім процесом, який продиктований вимогами сучасної високотехнологічної війни. Таким чином, впровадження хмарних технологій у поєднанні з безкомпромісним посиленням кібербезпеки забезпечить військовій частині 3077 стратегічну перевагу в управлінні інформаційними ресурсами [4]. Кожен із зазначених

напрямів є частиною єдиного плану модернізації, спрямованого на підвищення обороноздатності України через цифрову перевагу. Реалізація цих перспектив дозволить створити сучасну, захищену та високоефективну систему електронного документообігу, готову до будь-яких викликів майбутнього.

Тільки системний підхід до оновлення технологічної бази та методів захисту гарантує стабільність функціонування підрозділу в довгостроковій перспективі. Підсумовуючи, можна стверджувати, що майбутнє військового документообігу лежить у площині захищених хмарних рішень, які стають невід'ємною частиною цифрового щита нашої держави.

ВИСНОВКИ

У результаті проведеного дослідження було комплексно проаналізовано правові, організаційні та технічні аспекти функціонування електронних документів у системі військового управління. Встановлено, що цифрова трансформація документаційних процесів є невід'ємною умовою підвищення ефективності діяльності Національної гвардії України в сучасних умовах. Теоретичний аналіз підтвердив, що електронний документ є складним об'єктом, який вимагає специфічних методів захисту, автентифікації та збереження цілісності. З'ясовано, що сучасна нормативно-правова база України створює достатнє підґрунтя для переходу на безпаперове діловодство, проте потребує подальшої деталізації в оборонній сфері.

Доведено, що використання кваліфікованого електронного підпису забезпечує юридичну силу документів на рівні з паперовими оригіналами, підписаними власноруч. Вивчення міжнародних стандартів дозволило визначити оптимальні формати для довгострокового зберігання військової документації в електронних архівах. Аналіз діяльності військової частини 3077 продемонстрував високий рівень інтеграції цифрових технологій у щоденні управлінські цикли підрозділу. Система «Док Проф», яка активно використовується в установі, зарекомендувала себе як надійний та масштабований інструмент автоматизації документообігу.

Встановлено, що впровадження СЕД дозволило скоротити час на погодження внутрішніх розпорядчих документів у середньому на сорок відсотків. Технічні аспекти забезпечення конфіденційності у військовій частині базуються на суворому використанні сертифікованих засобів криптографічного захисту інформації. Дослідження показало, що автоматичне накладання штампа часу відіграє критичну роль у доведенні факту створення документа в конкретний момент. Виявлено, що основними бар'єрами на шляху повної цифровізації залишаються застарілі звички персоналу та складність інтеграції з деякими суміжними відомчими системами.

Організаційна структура військової частини 3077 дозволяє ефективно масштабувати нові цифрові рішення на всі функціональні та бойові підрозділи. Важливим висновком є необхідність посилення контролю за цілісністю даних під час їхньої передачі через відкриті та захищені канали зв'язку.

Застосування сучасних алгоритмів шифрування гарантує неможливість несанкціонованого доступу до службової інформації з боку сторонніх осіб чи хакерських угруповань. Запропоновано розширити функціонал системи «Док Проф» через впровадження додаткових модулів інтелектуального пошуку за метаданими та реквізитами. Обґрунтовано доцільність використання сучасних хмарних технологій для створення захищених резервних копій найбільш критичних баз даних установи. Гібридна модель зберігання інформації визначена як найбільш оптимальна для забезпечення безперервності роботи підрозділів в умовах активних бойових дій. Оцінка ризиків кібербезпеки підтвердила гостру потребу у проведенні регулярного аудиту прав доступу користувачів до централізованої системи.

Визначено, що автоматизація процесу реєстрації всієї вхідної кореспонденції мінімізує ризик втрати важливих пакетів документів або їхнього несвоєчасного розгляду. Робота з електронними архівами сьогодні вимагає розробки нових відомчих інструкцій щодо процедур гарантованого знищення документів після закінчення терміну зберігання. Встановлено, що повна цифровізація кадрових процесів суттєво пришвидшує обробку рапортів та звернень військовослужбовців щодо соціальних питань. Організаційні заходи щодо постійного навчання та підвищення кваліфікації персоналу є ключовим фактором успішної експлуатації складних ІТ-систем.

Технічний аналіз підтвердив достатню стійкість використовуваної архітектури СЕД до зовнішніх кібератак та цілеспрямованих спроб модифікації даних. Практичне значення роботи полягає у розробці детального алгоритму життєвого циклу електронного документа, який повністю адаптований до специфічних потреб НГУ. Запропоновані заходи з оптимізації дозволять суттєво знизити фінансові витрати на придбання витратних

матеріалів та обслуговування старої копіювальної техніки. Екологічний аспект переходу до концепції безпаперового офісу також має важливе значення для загального іміджу та сталого розвитку військової організації. Аналіз показав, що впровадження захищених мобільних робочих місць для офіцерського складу може стати наступним логічним етапом розвитку системи управління.

Забезпечення повної інтероперабельності між різними відомчими системами документообігу залишається стратегічним пріоритетним завданням на найближче майбутнє. Доведено, що використання єдиних державних стандартів метаданих значно полегшує процес оперативного обміну інформацією між різними силовими підрозділами. Висновки щодо високої надійності системи КЕП базуються на результатах перевірки відповідності використовуваних ключів чинним державним стандартам криптографії. Виявлено нагальну потребу у впровадженні систем автоматичного моніторингу працездатності серверного обладнання для запобігання технічним збоям. Дослідження підтвердило, що електронна взаємодія з іншими державними органами через шлюзи СЕДО працює стабільно та відповідає вимогам часу. Встановлено, що перехід на цифрові форми документів дозволяє здійснювати значно глибший та оперативніший аналіз стану виконавської дисципліни. Звіти, що генеруються системою автоматично, дають змогу командирам частин миттєво бачити реальний стан виконання поставлених розпоряджень та наказів.

Наукова новизна проведеного дослідження полягає в уточненні регламентованих процедур захисту документів у специфічних умовах нестабільного цифрового зв’язку. Розроблено практичні рекомендації щодо удосконалення графічного інтерфейсу користувача для спрощення роботи молодшого командного складу з цифровими формами. Встановлено, що повна юридична сила електронного примірника документа жодним чином не залежить від наявності або відсутності його паперової копії. Проаналізовано передовий досвід країн-членів НАТО у сфері створення захищеного документообігу, що може бути успішно запозичений для потреб Національної

гвардії. Визначено, що оперативна технічна підтримка системи «Док Проф» має здійснюватися переважно власними силами фахівців підрозділів зв'язку та інформатизації.

Обґрунтовано необхідність обов'язкового впровадження двофакторної автентифікації для всіх без винятку адміністраторів та привілейованих користувачів системи. Робота з документами, що містять інформацію з обмеженим доступом, вимагає обов'язкового створення фізично ізольованих контурів локальної мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бездрабко В. В. Управлінське документознавство. Київ: Наукова думка, 2016. 207 с.

2. Безпаперовий документообіг у ДОК ПРОФ. URL: https://egov.dp.gov.ua/services/bezpaperovij-dokumentoobig-u-dok-prof (дата звернення: 10.04.2026)

3. Безпаперовий офіс: теоретична і практична частини документообігу майбутнього. URL: https://archive.liga.science/index.php/universum/article/view/431 (дата звернення: 02.03.2026)

4. Військова частина №3077 Національної гвардії України. URL: https://youcontrol.com.ua/catalog/company_details/08803804/ (дата звернення: 13.03.2026)

5. Військове документування та діловодство в Україні: теоретичні та практичні аспекти, правове регулювання, актуальний закордонний досвід / Під заг. ред. Пєткова С. В. Київ: ВД «Професіонал», 2024. 464 с.

6. Деякі питання документування управлінської діяльності: Постанова Кабінету Міністрів України від 17 січня 2018 р. № 55. Документ 55-2018-п, чинний, поточна редакція — Редакція від 03.10.2025, підстава - 1188-2025-п. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text (дата звернення: 03.02.2026)

7. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12 березня 2022 р. № 263. Документ 263-2022-п, чинний, поточна редакція — Редакція від 06.06.2025, підстава - 641-2025-п. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення: 20.03.20260

8. Дзьобань О. П. Методологія, організація та технологія наукових досліджень. Київ; Одеса: Фенікс, 2025. 284 с.

9. Е-система документообігу «Док Проф». URL: https://egov.dp.gov.ua/services/bezpaperovij-dokumentoobig-u-dok-prof (дата звернення: 14.04.2026)

10. 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: 15.04.2026)

11. Інновації в електронному документообігу: огляд новітніх технологій і можливостей. URL: https://www.iqusion.com/ua/news/innovatsii-v-elektronnomu-dokumentoobihu-ohliad-novitnikh-tekhnolohii-i-mozhlyvostei.html (дата звернення: 23.03.2026)

12. Інструкція з діловодства у Збройних Силах України | Наказ Головнокомандувача Збройних Сил України 31 січня 2024 № 40. URL: https://warbooks.com.ua/blog/instruktsiya-z-dilovodstva-u-zbroynikh-silakh-ukraini--nakaz-40/?srsltid=AfmBOor0U5Oyf1nJozPBRFOl_Dj9fQmgCEttaZBtg0m_QCB4q1lGBbPL#:~:text=%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D0%B8%D0%BC%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D0%BD%D1%8F%D0%BC%20%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B8% (дата звернення: 12.02.2026)

13. Класифікатор управлінської документації НК 010:2021. Київ: Український науково-дослідний інститут архівної справи та документознавства, 2021. 26 с.

14. 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: 15.04.2026)

15. Кодекс України про адміністративні правопорушення. URL: https://zakon.rada.gov.ua/go/8073-10 (дата звернення: 01.04.2026)

16. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 01.04.2026)

17. Кулешов С. Г. Загальне документознавство: навч. посіб. Київ: Видавничий дім «Києво-Могилянська академія, 2019. 78 с.

18. Кулешов С. Г. Документознавство: історія. Теоретичні основи. Київ УДНДІАСД, 2019. 161 с. Ліга:Закон. URL: https://ips.ligazakon.net/ (дата зверення: 20.03.2026)

19. Лаптєв О. А., Зозуля С. А. Метод виключення відомих сигналів при сканування заданого радіодіапазону//Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», № 2(22), 2023. С. 31–38. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/533 (дата звернення: 21.04.2026)

20. Легомінова С. В., Гайдур Г. І. Аналіз сучасних загроз інфоормаційній безпеці організації та формування інформаційної платформи протидії їм// Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», № 2(22), 2023. С. 54-67. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/535/417

21. Машталяр Я. Р., Козачок В. А. та інші. Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури// Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», № 2(22), 2023. С. 157-167. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/538/498

22. «Megapolis.DocNet». URL: https://www.iqusion.com/ua/tags/megapolis-docnet.html (дата звернення: 18.02.2026)

23. Мельник С. Правові засади запровадження стандартів Північноатлантичного альянсу у функціонування Збройних Сил України// Адміністративне право і процес.№ 4. 2021. С. 183-188

24. Методологія наукових досліджень: навчальний посібник / за ред. В. П. Горина. Тернопіль: ФОП Осадца Ю. В., 2023. 170 с.

25. Палеха Ю. І. Загальне діловодство. Загальне діловодство: теорія та практика керування документацією із загальних питань: навчальний посібник. Київ: Видавництво Ліра-К. 2017.624 с.

26. Палеха Ю. І. Загальна класифікація документа: пропозиції щодо вдосконалення// Бібліотекознавство. Документознавство. Інформологія. 2022. № 3. С. 37–49

27. Перелік документів нормативно-правової бази, що забезпечує надання відповідних видів послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису): Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-normativno-pravovoyi-bazi-sho-zabezpechuye-nadannya-vidpovidnikh-vidiv-poslug-u-galuzi-kriptografichnogo-zakhistu-informaciyi-krim-poslug-elektronn (дата звернення: 29.03.2026)

28. Перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі КЗІ: Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/perelik-zasobiv-kriptografichnogo-zakhistu-informaciyi-yaki-mayut-ekspertnii-visnovok-za-rezultatami-derzhavnoyi-ekspertizi-u-galuzi-kzi (дата звернення: 29.03.2026)

29. Перелік форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання. Документ z1422-14, чинний, поточна редакція — Редакція від 10.05.2025, підстава - z0562-25. URL: https://zakon.rada.gov.ua/laws/show/z1422-14#Text (дата звернення: 02.04.2026)

30. Петрович В. В. Управлінське документознавство: навчально-методичні рекомендації. Луцьк, 2024. 41 с.

31. Піддубна Л. В., Павліченко В. М. Інформаційна безпека в системах електронного документообігу. Науковий вісник ПУЕТ. Серія «Економічні науки». 2019. № 4 (95). С. 59—66.

32. Про адміністративні послуги: Закон України. 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: 18.03.2026)

33. Про введення воєнного стану в Україні: указ Президента України. Документ 64/2022, чинний, поточна редакція — Редакція від 28.01.2026, підстава - 40/2026. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 19.03.2026)

34. Про доступ до публічної інформації: Закон України. 2939-VI, редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 23.03.2026)

35. Про електронні документи та електронний документообіг: Закон України. 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: 25.03.2026)

36. Про електронну ідентифікацію та електронні довірчі послуги: Закон України. 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: 25.03.2026)

37. Про затвердження Порядку перевірки документів в осіб, огляду речей, транспортних засобів, багажу та вантажів, службових приміщень і житла громадян під час забезпечення заходів правового режиму воєнного стану: Постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1456. Документ 1456-2021-п, чинний, поточна редакція — Редакція від 07.08.2025, підстава - 938-2025-п. URL: https://zakon.rada.gov.ua/laws/show/1456-2021-%D0%BF#Text. (дата звернення: 20.03.2026)

38. Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних та резервістів: Постанова Кабінету Міністрів України від 30 грудня 2022 р. № 1487. Документ 1487-2022-п, чинний, поточна редакція — Редакція від 21.01.2026, підстава - 41-2026-п.

URL: https://zakon.rada.gov.ua/laws/show/1487-2022-%D0%BF#Text (дата звернення: 10.03.2026)

39. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях. Наказ Міністерства юстиції України за № 1000/5. Документ z0736-15, чинний, поточна редакція — Редакція від 04.04.2026, підстава - z0356-26. URL: https://zakon.rada.gov.ua/laws/show/z0736-15#Text (дата звернення: 17.03.2026)

40. Про захист персональних даних: Закон України. 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: 11.03.2026)

41. Про захист інформації в автоматизованих системах: Закон України. 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: 05.03.2026)

42. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. 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: 05.03.2026)

43. Про звернення громадян: Закон України. Документ 393/96-ВР, чинний, поточна редакція, редакція від 24.01.2026, підстава - 4603-IX. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text (дата звернення: 28.02.2026)

44. Про інформацію: Закон України. Документ 2657-XII, чинний, поточна редакція — редакція від 20.01.2026, підстава - 4212-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 28.02.2026)

45. Про мобілізаційну підготовку та мобілізацію: Закон України. Документ 3543-XII, чинний, поточна редакція — Редакція від 12.04.2026,

підстава - 4826-IX. URL: https://zakon.rada.gov.ua/laws/show/3543-12#Text (дата звернення: 22.02.2026)

46. Про Національний архівний фонд та архівні установи: Закон України. 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: 13.03.2026)

47. Про національну безпеку України: Закон України. Документ 2469-VIII, чинний, поточна редакція — Редакція від 24.01.2026, підстава - 4603-IX. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.04.2026)

48. Про Національну гвардію України: Закон України. Документ 876-VII, чинний, поточна редакція — Редакція від 27.06.2024, підстава - 3760-IX. URL: https://zakon.rada.gov.ua/laws/show/876-18#Text (дата звернення: 02.04.2026)

49. Про обов'язковий примірник документів: Закон України. Документ 595-XIV, чинний, поточна редакція — редакція від 31.03.2023, підстава - 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/595-14#Text (дата звернення: 29.04.2026)

50. Про організацію трудових відносин в умовах воєнного стану: Закон України. Документ 2136-IX, чинний, поточна редакція — Редакція від 14.03.2026, підстава - 4412-IX. URL: https://zakon.rada.gov.ua/laws/show/2136-20#Text (дата звернення: 13.04.2026)

51. «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Закон України. Документ 537-V, чинний, поточна редакція — прийняття від 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 12.03.2026)

52. Україна запроваджує нові засоби електронної ідентифікації згідно з європейськими стандартами. URL: https://finap.com.ua/ukrayina-zaprovadzhuye-novi-zasoby-elektronnoyi-identyfikatsiyi-zgidno-z-yevropejskymy-

standartamy/#:~:text=%D0%A3%202021%20%D1%80%D0%BE%D1%86%D1%96%20%D0%84%D0%B2%D1%80%D0%BE%D0%BF%D0%B5%D0%B9%D1%81%D1%8C%D0%BA%D0%B0%20%D0%BA%D0%BE%D0%BC%D1%96%D1%81%D1%96%D1%8F%20%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D0%BF%D0%BE%D0%BD (дата звернення: (01.04.2026)

53. Цивільний кодекс України. Документ 435-IV, чинний, поточна редакція — Редакція від 01.02.2026, підстава - 4671-IX. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 11.04.2026)

54. Шкіцька І. Ю. Управлінське документознавство. Тернопіль: ТНЕУ, 2020. 382 с.

55. Що таке архітектура нульової довіри? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-zero-trust-architecture (дата звернення: 20.04.2026)

ДОДАТКИ

ДОДАТОК А

(до підрозділу 2.2)

(розроблено на основі аналізу джерел)

Порівняльна характеристика традиційного (паперового) та електронного документообігу (на прикладі СЕДО «Док Проф» у військовій частині 3077)

Критерій порівняння	Традиційний (паперовий) документообіг	Електронний документообіг (СЕДО «Док Проф»)
Швидкість передачі та обробки	Висока залежність від логістики та кур'єрської служби (години або дні).	Миттєва передача через захищені канали зв'язку (лічені секунди).
Забезпечення конфіденційності	Обмеження доступу шляхом сейфового зберігання та фізичного контролю кабінетів.	Шифрування даних за стандартами ДСТУ та рольове розмежування прав доступу.
Контроль цілісності	Візуальний огляд на відсутність виправлень, підчисток та наявність мокрої печатки.	Автоматична перевірка хеш-суми файлу та валідація КЕП при кожному відкритті.
Юридична значущість	Власноручний підпис посадової особи та гербова печатка частини.	Кваліфікований електронний підпис (КЕП) із обов'язковим штампом часу (Timestamp).
Пошук інформації	Ручний перегляд журналів реєстрації та фізичний пошук у папках архіву.	Миттєвий пошук за будь-яким реквізитом (дата, номер, ПІБ, ключове слово).
Виконавська дисципліна	Складний контроль термінів, що потребує ведення додаткових карток контролю.	Автоматичні сповіщення про дедлайни та онлайн-моніторинг статусу виконання.
Стійкість у надзвичайних умовах	Ризик фізичного знищення (пожежа, обстріл) без	Наявність резервних копій на віддалених захищених серверах (Disaster Recovery).

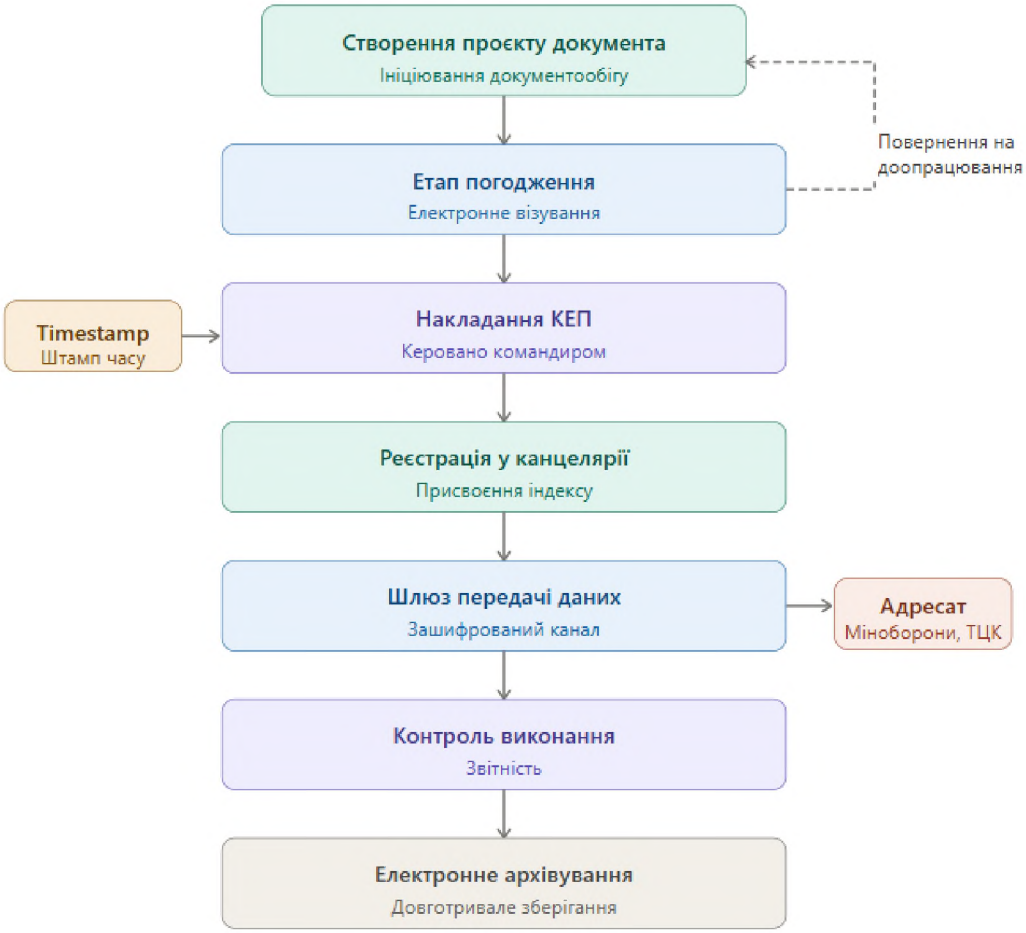
Критерій порівняння	Традиційний (паперовий) документообіг	Електронний документообіг (СЕДО «Док Проф»)
	можливості швидкого відновлення.	
Витрати ресурсів	Значні витрати на папір, тонери, канцелярію та оренду приміщень для архівів.	Витрати на підтримку IT-інфраструктури та ліцензії, значна економія витратних матеріалів.
Прозорість (аудит)	Складно відстежити, хто саме і коли переглядав документ (крім відміток у картці).	Повне логування дій (Audit Log): хто, коли та з якого термінала відкривав чи редагував файл.
Взаємодія з ТЦК та медзакладами	Потребує фізичного перевезення пакетів документів (особових справ, висновків ВЛК).	Оперативний обмін даними через шлюзи СЕДО, пришвидшення соціальних виплат та ротацій.

ДОДАТОК Б

(до підрозділу 2.2)

(розроблено на основі аналізу джерел)

Алгоритм життєвого циклу електронного документа в СЕДО «Док Проф» (на прикладі військової частини 3077)



II. Опис етапів алгоритму

Ініціація: розробка проєкту документа виконавцем у середовищі «Док Проф» із використанням встановлених шаблонів НГУ.

Візування: паралельне або послідовне ознайомлення зацікавлених посадових осіб (начальників служб) із накладанням електронних віз, що підтверджують згоду зі змістом.

Криптографічний захист (підписання): система генерує унікальний хеш-код документа. Командир використовує апаратний токен для накладання КЕП.

Timestamp: система автоматично звертається до сервера часу для фіксації точного моменту підписання.

Централізована реєстрація: спеціаліст канцелярії перевіряє правильність реквізитів та присвоює документу вихідний/внутрішній номер. Після цього етапу документ стає «замороженим» для будь-яких змін.

Транспортування: документ автоматично шифрується та відправляється через захищений контур зв'язку до адресата (іншої військової частини, ТЦКтаСП чи медичного закладу).

Моніторинг: система автоматично відстежує статус документа («Прочитано», «Прийнято до виконання», «Виконано»).

Депонування в архів: після завершення справи документ переміщується до електронного архіву з автоматичним продовженням терміну дії підпису (LTV — Long Term Validation).