МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Кафедра українознавства, культури та документознавства

Кваліфікаційна бакалаврська робота

СПЕЦИФІКА РОБОТИ З ДОКУМЕНТАМИ ОБМЕЖЕНОГО ДОСТУПУ

(на прикладі діяльності військової частини)

Студентки 3 курсу групи 3пГД
Спеціальності 029 «Інформаційна, бібліотечна та архівна справа»

_____ Новікова Дарія Олександрівна

Науковий керівник
к. філол. н., доцент _____ Акіншина Ірина Миколаївна

Завідувач кафедри _____ Передерій Ірина Григоріївна

Полтава 2024

Деканові факультету філології, психології та педагогіки
Національного університету
«Полтавська політехніка
імені Юрія Кондратюка
Анні АГЕЙЧЕВІЙ
студентки групи ЗпГД
спеціальності 029 «Інформаційна, бібліотечна та архівна справа»
Новікової Дарії Олекснадрівни

ЗАЯВА

Прошу затвердити тему кваліфікаційної роботи: Специфіка роботи з документами обмеженого доступу (на прикладі діяльності військової частини).

Науковим керівником прошу призначити кандидата філологічних наук, доцента, доцента кафедри українознавства, культури та документознавства Акіншину Ірину Миколаївну.

12.02.2024 _____

Завідувач кафедри _____ Ірина ПЕРЕДЕРІЙ

Керівник _____ Ірина АКІНШИНА

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Факультет філології, психології та педагогіки
Кафедра українознавства, культури та документознавства
Спеціальність 029 «Інформаційна, бібліотечна та архівна справа»

ЗАТВЕРДЖУЮ
Завідувач кафедри українознавства, культури та документознавства_____ Ірина ПЕРЕДЕРІЙ
“___” _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРУ

Новіковій Дарії Олександрівні

1. Тема роботи: Специфіка роботи з документами обмеженого доступу (на прикладі діяльності військової частини).

Керівник роботи: к. філол. н., доц. Акіншина Ірина Миколаївна.

2. Термін подання роботи 12.06.2024 р.

3. Мета та завдання бакалаврської роботи: вивчення теоретичних аспектів та розроблення практичних рекомендацій щодо впровадження захищеної автоматизованої системи електронного документообігу військової частини; розкрити теоретичні основи конфіденційного діловодства та визначити особливості його автоматизації; дослідити організаційну структуру, напрями діяльності та провести аналіз особливостей обігу документів обмеженого доступу військової частини; надати практичні рекомендації для впровадження та захисту автоматизованої системи електронного документообігу військової частини.

Дата видачі завдання: 20.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітки
1	Теоретична частина	11.03.24– 30.03.24	25%
2	Аналітична частина	01.04.24 – 25.04.24	50%
3	Проєктна частина	26.04.24 – 18.05.24	25%
4	Виготовлення ілюстративного матеріалу та підготовка до захисту	20.05.24 – 04.06.24	100%
5	Захист роботи	25.06.20224	

Студентка _____ Дарія НОВІКОВА

Керівник роботи _____ Ірина АКІНШИНА

АНОТАЦІЯ

Новікова Д. О. Специфіка роботи з документами обмеженого доступу (на прикладі діяльності військової частини). Спеціальність 029 «Інформаційна, бібліотечна та архівна справа», спеціалізація «Документознавство та інформаційна діяльність». Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, 2024.

У кваліфікаційній роботі сформульовано теоретичні основи роботи з документами обмежено доступу. Визначено нормативно-правові та організаційні аспекти роботи з конфіденційною інформацією. Схематично відтворено режими доступу до інформації. Розглянуто основні принципи захисту інформації обмежено доступу. Висвітлено основні недоліки правового регулювання в інформаційній сфері.

Проведено порівняльний аналіз технологій конфіденційного електронного документообігу. Встановлено особливості конфіденційного діловодства, визначено основні джерела загрози безпеці конфіденційних документів та методи їхнього захисту. Описано основні операції технологічного процесу обліку конфіденційних документів.

У роботі схарактеризовано діяльність військової частини, схематично відтворено її організаційну структуру управління. Схарактеризовано специфіку організації діловодного обслуговування військових підрозділів. З'ясовано основні принципи військового документування, описано документний склад військової частини, сформульовано способи захисту електронних документів.

Подано загальну класифікацію програмних рішень для систем електронного документообігу. Розроблено практичні рекомендації щодо забезпечення захисту інформації обмеженого доступу в СЕД військової частини.

Ключові слова: військова частина, система електронного документообігу, конфіденційна інформація, служба діловодства, документи обмеженого доступу

54 с., 8 рис., 1 табл., 49 джерел.

ABSTRACT

Novikova Dariia. Specifics of working with restricted documents (on the example of a military unit activity). Speciality 029 «Information, Library and Archives», specialisation «Documentation and Information Activity». National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, 2024.

In the qualification work, the theoretical foundations of handling restricted access documents are formulated. The regulatory, legal, and organizational aspects of working with confidential information are defined. The access modes to information are schematically depicted. The main principles of protecting restricted access information are considered. The main shortcomings of legal regulation in the information sphere are highlighted.

A comparative analysis of confidential electronic document circulation technologies is conducted. The peculiarities of confidential record-keeping are established, the main sources of threats to the security of confidential documents and methods of their protection are identified. The main operations of the technological process of accounting for confidential documents are described.

The work characterizes the activities of a military unit, and its organizational management structure is schematically depicted. The specifics of organizing record-keeping services for military units are characterized. The main principles of military documentation are clarified, the document composition of the military unit is described, and methods for protecting electronic documents are formulated.

A general classification of software solutions for electronic document management systems is provided. Practical recommendations for ensuring the protection of restricted access information in the EDMS of a military unit are developed.

Keywords: military unit, electronic document management system, confidential information, record-keeping service, restricted access documents

54 pp., 8 pic., 1 tab., 49 sources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АІС	–	автоматизована інформаційна система
ДЗУ	–	документаційне забезпечення управління
ДСТУ	–	Державний стандарт України
ЗСУ	–	Збройні Сили України
ЕД	–	електронний документ
ЕП	–	електронний підпис
СЕД	–	система електронного документообігу

ВСТУП

Актуальність теми дослідження. Документи обмеженого доступу є важливим елементом функціонування, управління та оперативної діяльності військових частин. Вони містять важливу інформацію, яка має стратегічне значення для національної безпеки та оборони.

Захист документів обмеженого доступу військової частини вимагає використання сучасних технологій шифрування та розмежування доступу до інформації, які не лише запобігають несанкціонованому доступу до конфіденційних матеріалів, але й забезпечують збереження цілісності та достовірності військової інформації.

Саме системи електронного документообігу відіграють ключову роль у автоматизації спеціального діловодства, зокрема і у військових структурах. Вони забезпечують швидкий та ефективний обмін документами з високим рівнем захисту конфіденційної інформації.

Загалом, успішна реалізація основних процесів роботи з конфіденційною інформацією є важливим складником надійного захисту національної безпеки країни від потенційних загроз та ефективного управління військовими структурами усіх рівнів.

Об’єктом дослідження є документи обмеженого доступу.

Предмет дослідження – особливості роботи з документами обмеженого доступу військової частини.

Мета дослідження – вивчення теоретичних аспектів та розроблення практичних рекомендацій щодо впровадження захищеної автоматизованої системи електронного документообігу військової частини.

Сформована мета передбачає розв’язання таких **дослідницьких завдань**:

1. Розкрити теоретичні основи конфіденційного діловодства та визначити особливості його автоматизації.

2. Дослідити організаційну структуру, напрями діяльності та провести аналіз особливостей обігу документів обмеженого доступу військової частини.

3. Надати практичні рекомендації для впровадження та захисту автоматизованої системи електронного документообігу військової частини.

Методи дослідження. Зазначені завдання, особливості об'єкта й предмета дослідження зумовили застосування *описового методу* для розгляду особливостей роботи з документами обмеженого доступу; *методу порівняння*, завдяки якому визначено переваги та недоліки технологій автоматизованих систем електронного документообігу; *методів аналізу і синтезу* застосовано для з'ясування основних складників структури військової частини, встановлення зв'язків між ними для формування цілісного уявлення про систему управління; *методу систематизації*, що уможливив визначення результатів захисту документів обмеженого доступу у роботі служби діловодства військової установи; *методу системно-компонентного аналізу* для визначення основних складників автоматизованої системи електронного документообігу; *методу узагальнення*, що уможливив формулювання висновків та обґрунтування практичних рекомендацій щодо захисту конфіденційних документів військової частини за допомогою технологій СЕД.

Джерельну базу дослідження становлять нормативно-правові акти, наукові статті, навчально-методичні видання, матеріали ЗМІ, вебресурси.

Питанням захисту конфіденційної інформації приділяли увагу вчені О. Загорецька, А. Гуз, О. Довгань, А. Марущак, С. Сельченкова., Є. Скулиш, Х. Ярмакі, С. Музика. Інформаційні технології захисту документаційного забезпечення розглянули у своїх працях вчені Г. Полішко, О. Рибальський, В. Хахановський, В. Кудінов, В. Фастовець, В. Сирцов, М. Цілина.

Питання документування та обліку військових документів досліджували І. Кузьмич, С. Литвинська, А. Сібрук, С. Мельник, П. Фівкін, Є. Пащенко, Л. Зіняк, В. Юрчак.

Наукова новизна кваліфікаційної роботи полягає в тому, що в ній досліджено способи захисту конфіденційної інформації та визначено інструментальні засоби впровадження системи електронного документообігу військової частини, що дозволить автоматизувати основні процеси роботи з документами обмеженого доступу.

Практичне значення одержаних результатів полягає у можливості впровадження та подальшої експлуатації системи електронного документообігу Google Workspace, яка забезпечує захист конфіденційної інформації, працівниками служби діловодства військової частини.

Апробація результатів дослідження. Окремі положення кваліфікаційної роботи, а також одержані узагальнення було апробовано на 76-ій науковій конференції професорів, викладачів, наукових працівників, аспірантів та студентів Національного університету «Полтавська політехніка імені Юрія Кондратюка». Результати дослідження висвітлено в тезах доповіді «Організація електронного документообігу при роботі з конфіденційною інформацією у військових частинах України». *Тези 76-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів Національного університету «Полтавська політехніка імені Юрія Кондратюка»*. Т. 2 (Полтава, 14 травня – 23 травня 2024 року). Полтава: Національний університет імені Юрія Кондратюка, 2024. С. 301-302 [32].

Структура кваліфікаційної бакалаврської роботи підпорядкована меті та завданням дослідження і складається з переліку умовних скорочень, вступу, двох розділів, висновків, списку використаних джерел, що містить 46 найменувань. Обсяг роботи – 54 сторінки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РОБОТИ З ДОКУМЕНТАМИ ОБМЕЖЕНОГО ДОСТУПУ

1.1. Принципи роботи з конфіденційною інформацією: нормативно-правові та організаційні аспекти

Відомо, що нові інформаційні технології активно впроваджують у різні сфери виробництва та послуг. З поступовим розвитком та ускладненням засобів, методів автоматизації процесів оброблення інформації підвищується залежність суспільства від рівня безпеки інформаційних технологій. Недотримання вимог безпеки інформації від випадкових чи навмисних впливів природного чи штучного характеру може спричинити шкоду суб'єктам інформаційних відносин, зокрема власникам та користувачам інформації.

Безумовно, у процесі своєї діяльності суб'єкти можуть бути один з одним у різних інформаційних відносинах, що стосуються питань отримання, зберігання, оброблення, поширення та використання певної інформації. Для успішного здійснення своєї діяльності з управління об'єктами певної предметної галузі суб'єкти інформаційних відносин можуть бути зацікавлені у забезпеченні:

– своєчасного доступу до необхідної інформації та певних автоматизованих служб;

– конфіденційності певної інформації;

– достовірності, зрозумілості, достатності, цілісності та цінності документної інформації;

– захисту від дезінформації, незаконного поширення, зміни чи розповсюдження інформації;

– розподілу відповідальності за порушення законних інтересів усіх суб'єктів інформаційних відносин та встановлених правил поводження з інформацією;

– постійного контролю та управління процесами оброблення та передавання інформації тощо.

Кожна організація забезпечує захист цінної інформації, що є предметом її власності, відповідно до вимог законодавства або вимог, що встановлює власник інформації.

Загальновідомо, що вся інформація є відкритою, окрім тієї, яка згідно з законом належить до інформації з обмеженим доступом. Згідно з законом України «Про інформацію» [7], «інформацією з обмеженим доступом є: конфіденційна інформація, таємна інформація, службова інформація». Загальну характеристику режимів доступу до інформації подано на рис. 1.1.

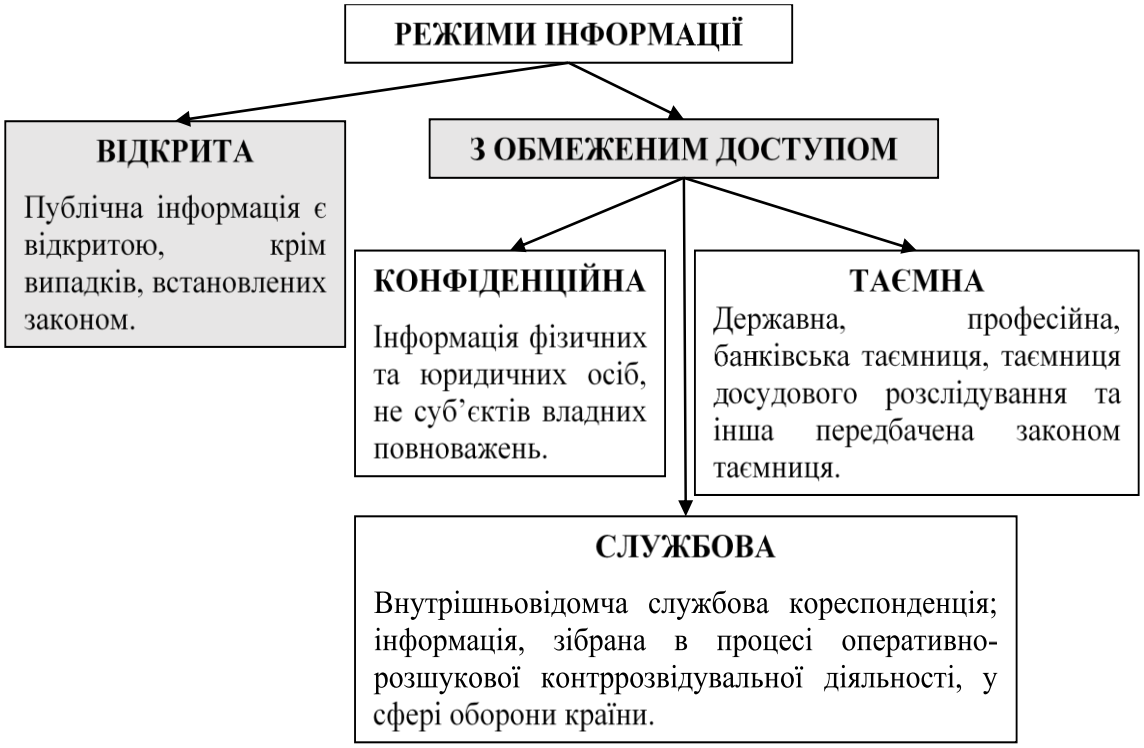

Рисунок 1.1. Режими інформації

Розроблено автором за матеріалами [7]

Сьогодні проблема роботи з конфіденційними документами набуває все більшої актуальності у зв'язку з тим, що «розвиток нових інформаційних технологій підвищує рівень пошкодження або/чи знищення інформації, що становить конфіденційні відомості. Внаслідок цього виникає необхідність документування процесу захисту конфіденційної інформації» [21, с. 234].

Загалом, *конфіденційна інформація* – це відомості, що становлять комерційну, виробничу, особисту таємницю, та не підлягають широкому розголошенню.

Варто зазначити, що категорії конфіденційної інформації можуть включати:

1. Персональні дані фізичних осіб.

2. Комерційну таємницю (інформація про комерційну діяльність, яка не підлягає розголошенню і має комерційну цінність).

3. Відомості, що становлять професійну таємницю.

4. Інші види інформації, що обмежують в доступі законодавством [7].

Порушення правил зберігання конфіденційної інформації призводить до значних матеріальних і моральних збитків організації, а саме:

– втрата можливостей підписання вигідних контрактів, угод;

– відмова від рішень, що стали економічно неефективними через розголошення інформації, що призводить до додаткових фінансових витрат на прийняття нових управлінських рішень;

– зниження вартості продукції чи послуг, а також суттєве зниження обсягів продажу;

– значне погіршення ділових комунікацій із партнерами;

– втрата можливості продажу патентів, авторських свідоцтв і ліцензій;

– погіршення умов для кредитування;

– збільшення витрат на проведення науково-дослідницьких робіт.

На думку дослідників, для кожної одиниці інформації, що захищають, є кілька параметрів, які необхідно враховувати: статичність; розмір та тип доступу; час життя; вартість створення; вартість втрати конфіденційності; вартість прихованого порушення цілісності; вартість втрати.

Статичність визначає рівень змінності захищеної інформації процесі нормального використання. Розмір та тип доступу (послідовний або довільний) також накладають обмеження на засоби захисту. Час життя

інформації – це важливий параметр, який визначає час актуальності інформації. Вартість створення є чисельним виразом сукупності ресурсів (фінансових, людських, тимчасових), витрачених на створення інформації (собівартість). Вартість втрати конфіденційності виражає можливі збитки, які зазнає власник інформації, якщо до неї отримають неавторизований доступ сторонні особи. Як правило, вартість втрати конфіденційності багаторазово перевищує собівартість інформації. Вартість прихованого порушення цілісності виражає збитки, які можуть виникнути внаслідок внесення змін до інформації, якщо факт модифікації не був виявлений. «Порушення цілісності може бути як випадковими, так і навмисним. Вартість втрати визначає збитки від повного чи часткового руйнування інформації. При виявленні порушення цілісності та неможливості отримати ту саму інформацію з іншого джерела інформація вважається втраченою» [25].

Розглянемо спосіб формування списку конфіденційних документів фірми (організації) з урахуванням розглянутих раніше властивостей інформації.

Варто підкреслити, що для формування переліку конфіденційних документів та визначення ступеня їх важливості необхідно виконати такі етапи: вивчити нормативно-правові документи щодо питань визначення інформації, яку відносять до конфіденційної; сформувати приблизний список документів організації; визначити приблизну цінність інформації, що міститься у документах, з врахуванням таких критеріїв, як вартість створення, вартість розголошення, час життя документа тощо; сформувати список конфіденційних документів компанії (організації); оцінити важливість документа.

Розглянемо основні принципи захисту інформації обмеженого доступу:

1. Створення нормативно-правової бази чи вдосконалення вже існуючої для чіткого регулювання цієї сфери.

2. Визначення кола осіб, які відповідають за безпеку документів.

3. Визначення переліку відомостей, що підлягають захисту.

4. Укладання переліку осіб, які мають доступ до цієї інформації.

5. Побудова системи інформаційної безпеки захисту цих документів.

6. Використання програмно-апаратних засобів захисту носіїв інформації.

7. Проведення профілактичних бесід та ознайомлення співробітників з правилами техніки безпеки [26, с. 49].

Безумовно, у системі управління організацією застосовують такі види таємниць: комерційна таємниця, персональні дані, службова таємниця. Для захисту інформації в організаціях та установах проводять такі заходи:

1. Розроблення локальних нормативних актів, у яких визначено порядок поводження з інформацією конфіденційного характеру та особливості контролю за дотриманням такого порядку (наприклад, інструкція про конфіденційне діловодство).

2. Розроблення та визначення переліку інформації, що становить конфіденційні відомості. Цей перелік має затверджувати керівник організації або установи. З ним мають ознайомитися всі співробітники, які допущені до роботи з цими відомостями.

3. Надання грифів обмеження доступу на документах, що містять конфіденційну інформацію. Наприклад, на документах конфіденційного та комерційного характеру проставляють позначку «Конфіденційно», а на документах, що містять службові відомості, – гриф «Для службового користування».

4. Регулювання відносин щодо використання інформації, що становить комерційну таємницю, працівниками на підставі трудових договорів та контрагентами на підставі цивільно-правових договорів. Крім цього, слід вносити певні доповнення до посадових інструкцій цієї групи співробітників.

5. Документування обліку осіб, які отримали доступ до інформації, що становить комерційну або службову таємницю, та (або) осіб, яким така інформація була надана або передана [33, с. 54].

Загальновідомо, що обмеження доступу до конфіденційної інформації визначаються законодавством, і порушення встановлених обмежень може тягти за собою юридичну відповідальність.

Нормативно-методичне забезпечення системи захисту конфіденційної інформації призначене для регламентації процесів забезпечення безпеки інформації підприємства, зокрема під час роботи персоналу з конфіденційними відомостями, документами, справами та базами даних. Воно включає низку обов'язкових організаційних, інструктивних та інформаційних документів, що встановлюють принципи, вимоги та способи запобігання пасивним та активним загрозам цінної інформації, які можуть виникнути з вини персоналу, конкурентів, зловмисників та інших осіб.

Система захисту цінної, конфіденційної інформації підприємства реалізується у «комплексі нормативно-методичних документів, які деталізують та доводять її у вигляді конкретних робочих вимог до кожного працівника» [36, с. 6]. Критерії ідентифікації конкретної інформації для віднесення її до категорії обмеженого доступу мають бути визначені чинним законодавством.

У науковій літературі конфіденційну інформацію визначають як «інформацію, що складається з сукупності отриманих із різних джерел будь-яких секретних відомостей, що не підлягають розголосу, доступ до яких обмежений чинним законом, за виключенням інформації, що становить державну таємницю».

Основні нормативно-правові акти, які забезпечують захист конфіденційної інформації, відображено у таблиці 1.1.

Таблиця 1.1

Нормативно-правові аспекти захисту конфіденційної інформації

Назва нормативно-правового акту	*Характеристика*
Основні закони	
Конституція України	Гарантує право на захист особистих даних та особистої інформації (стаття 32).

Продовження таблиці 1.1

Назва нормативно-правового акту	*Характеристика*
Закон України «Про інформацію»	Визначає загальні принципи інформаційних відносин, включаючи категорії інформації з обмеженим доступом, до яких належить конфіденційна інформація (стаття 21).
Закон України «Про захист персональних даних»	– регулює обробку та захист персональних даних; – встановлює права суб'єктів персональних даних і обов'язки осіб, які здійснюють їх оброблення; – визначає механізми захисту персональних даних.
Закон України «Про доступ до публічної інформації»	– визначає порядок доступу до публічної інформації та встановлює обмеження щодо доступу до конфіденційної інформації; – встановлює, що інформація з обмеженим доступом надають у передбачених законом випадку.
Закон України «Про державну таємницю»	– регулює питання захисту інформації, що становить державну таємницю; – встановлює категорії державної таємниці та порядок її захисту.
Підзаконні акти	
Постанови Кабінету Міністрів України	– регламентують порядок захисту конфіденційної інформації в різних сферах діяльності; – встановлюють процедури та вимоги до захисту інформації в державних органах та установах.
Накази міністерств та центральних органів виконавчої влади	Видаються з метою виконання законів та постанов Кабінету Міністрів.
Інструкції та положення державних органів	– визначають внутрішні процедури захисту конфіденційної інформації; – регулюють питання доступу співробітників до конфіденційної інформації, облік і зберігання такої інформації.
Додаткові регулюючі документи	
Постанови органів місцевого самоврядування	Встановлюють правила захисту конфіденційної інформації на місцевому рівні.
Положення про конфіденційність у договорах	– включають умови щодо захисту конфіденційної інформації у трудові договори; – забезпечують юридичне зобов'язання з боку співробітників та партнерів щодо нерозголошення конфіденційної інформації.

Продовження таблиці 1.1

Назва нормативно-правового акту	*Характеристика*
Стандарти та рекомендації	– вказівки з технічного захисту інформації, що надаються, наприклад, Державної служби спеціального зв'язку та захисту інформації України; – міжнародні стандарти, такі як ISO/IEC 27001, що встановлюють вимоги до системи управління інформаційною безпекою.

Розроблено автором за матеріалами [1–14]

Варто наголосити, що захист конфіденційної інформації в Україні забезпечується через комплекс нормативно-правових актів, які регулюють різні аспекти оброблення, зберігання та доступу до такої інформації. Виконання цих нормативних вимог дозволяє забезпечити належний рівень захисту конфіденційної інформації та мінімізувати ризики несанкціонованого доступу або витоку даних.

Обмеження доступу до інформації встановлюється законами України «Про інформацію» [7], «Про захист персональних даних» [6], «Про захист інформації в інформаційно-телекомунікаційних системах» [5], «Про державну таємницю» [2] з метою захисту основ конституційного ладу, моральності, здоров'я, правових і законних інтересів, забезпечення оборони та безпеки держави. Обов'язковим є дотримання конфіденційності інформації, доступ якої обмежений законом України «Про доступ до публічної інформації». До того ж законом можуть встановлюватися умови віднесення інформації до відомостей, що становлять комерційну таємницю, службову таємницю та іншу таємницю, обов'язковість дотримання конфіденційності такої інформації.

Нормативну технічну базу утворюють документи, що безпосередньо визначають організаційні та технічні вимоги щодо захисту інформації, порядок їх виконання та контролю ефективності заходів захисту. До таких документів відносять: державні стандарти України (ДСТУ); вимоги та

рекомендації щодо захисту інформації; нормативні та методичні документи, що визначають критерії ефективності захисту інформації та порядок їх контролю.

На законодавчому рівні створено систему правових актів, які регламентують режим інформації конфіденційного характеру, проте взагалі відсутній єдиний підхід у розумінні її сутності і змісту. При цьому не достатнього врегульовано питання захисту інформації обмеженого доступу.

Основними недоліками правового регулювання в інформаційній сфері є: різне тлумачення ключових понять та термінів, відсутність узгодженого понятійного апарату, «різні підходи до забезпечення інформаційної безпеки та елементів інформаційної сфери у законодавстві та державних стандартах, неактуальність джерел, відставання нормотворення від темпів розвитку інформаційних технологій» [38].

Отже, доходимо висновку, що обсяг відомостей, що становлять конфіденційну інформацію, у конкретній організації визначається керівниками виходячи зі специфіки діяльності організацій. Керівник має право самостійно встановлювати правила роботи з конфіденційною інформацією, у тому числі призначати співробітників, відповідальних за облік та зберігання конфіденційних документів, передавання документів до інших підрозділів.

Варто підкреслити, що найважливішим постулатом для документування конфіденційної інформації є те, що вона не підлягає розголошенню в будь-якому вигляді і в будь-якій формі, а також не може стати надбанням третіх осіб.

Сьогодні найбільш рекомендованою системою захисту конфіденційної інформації є комплексна система захисту інформації, що включає всі види компонентів захисту, а саме: програмну, технічну, внутрішньомережеву і об’єктну, що має централізовано-розподілену архітектуру, вона найбільш повно відповідає сучасним вимогам захисту інформації. Такий підхід

дозволяє забезпечити високий рівень захисту даних і мінімізувати ризики несанкціонованого доступу або витоку інформації.

1.2. Система конфіденційного діловодства в умовах розвитку інформаційних технологій

Безумовно, реальний механізм, який може забезпечити захист документованої конфіденційної інформації, – це створення в організації системи конфіденційного діловодства або, як мінімум, застосування у відкритому діловодстві засобів та методів, які використовують під час роботи із закритими документами.

Конфіденційне діловодство – це діяльність, що забезпечує документування конфіденційної інформації, організацію роботи з конфіденційними документами, їхній захист та оперативне зберігання.

Відповідно до цього, метою конфіденційного діловодства є «забезпечення захисту конфіденційної інформації, що міститься в документах, від несанкціонованого доступу, витоку, втрати або пошкодження» [23, с. 18].

Система конфіденційного діловодства – це сукупність методів, засобів та заходів, спрямованих на забезпечення збереження конфіденційності та безпеки інформації, що міститься в документах організації. Такі системи мають забезпечувати захист інформації на всіх етапах її життєвого циклу, починаючи від створення документа і до його знищення або архівації.

Зазначимо, що внаслідок цього система оброблення та захисту конфіденційних документів включає низку заходів, а саме:

– жорстке регламентування складу документів і контроль процесів документування зі стадії підготовки чернеток і проєктів документів;

– створення дозвільної системи доступу до документів та справ, що забезпечує правомірне та санкціоноване ознайомлення з ними;

– обов’язковий поекземплярний та полистовий облік усіх документів, проєктів та чернеток, облікових форм;

– фіксація проходження та місцезнаходження кожного документа, зокрема письмове фіксування всіх звернень персоналу до документів;

– контроль копіювання та розмноження документів;

– регламентація обов’язків співробітників, зокрема запровадження персональної відповідальності щодо роботи з документами та захисту довіреної конфіденційної інформації;

– проведення систематичних перевірок наявності конфіденційних документів, їх збереження та цілісності;

– проведення постійної інформаційно-аналітичної роботи, спрямованої на виявлення потенційних загроз, визначення найбільш оптимальних заходів, що сприяють зміцненню та оновленню системи захисту документованої інформації відповідно до змінних внутрішніх і зовнішніх обставин.

Відповідно до специфіки діяльності організація має самостійно вибрати найефективніший програмний продукт захисту секретної інформації.

Технології конфіденційного електронного документообігу належать до групи інформаційних. Інформаційні технології – це процеси, методи пошуку, збирання, зберігання, оброблення, надання, розповсюдження інформації та способи здійснення таких процесів та методів. Технології оброблення, зберігання, передавання інформації входять до переліку технологій, що мають велике соціально-економічне значення, а також відіграють важливу роль у забезпеченні захисту як окремого підприємства, так і безпеки держави вцілому [34, с. 83].

На думку дослідників, проблеми захисту інформації стали ще більш складними і значущими у зв’язку з переходом життєвого циклу документованої інформації на безпаперову, електронну основу з одночасним застосуванням як паперових технологій діловодства та документообігу, так і електронних з використанням автоматизованих інформаційних систем.

Відповідно технології конфіденційного діловодства та документообігу багато в чому збігаються з технологіями організації роботи з документованою інформацією обмеженого доступу.

Забезпечення збереження та конфіденційності документованої інформації вимагає створення та підтримки спеціальних умов зберігання, оброблення та обігу документів, що гарантують надійний захист як самих документів, так і інформації, що міститься в них. Досягається це шляхом організації спеціального режиму зберігання конфіденційної інформації та поводження з нею, встановлення дозвільної системи доступу, розроблення регламентованої технології її створення та оброблення [36, с. 7].

Керівництво конкретної організації у межах своєї компетенції визначає: категорії посадових осіб, уповноважених відносити інформацію (документи) до конфіденційної; коло посадових осіб, які мають доступ до документів та інформації різного ступеня конфіденційності; порядок зняття позначки конфіденційності з документів, включно з електронними, що циркулюють в автоматизованій інформаційній системі; захист АІС.

Виконання завдань документаційного забезпечення управління також передбачає забезпечення управлінської структури повною, своєчасною і достовірною документною інформацією, організацію виконання та використання документів. При організації захисту конфіденційних документів до цих завдань також додають:

1) попередження несанкціонованого доступу будь-якої особи до документа, його частин, варіантів, чернеток, копій;

2) забезпечення фізичного захисту документів;

3) забезпечення захисту інформації, що міститься в документах.

Варто зазначити, що виконання цих завдань дозволяє не тільки уникнути втрати або підміни документів обмеженого доступу, а й запобігти порушенню режиму їх конфіденційності в результаті витоку відомостей, що охороняються, тобто несанкціонованого (неправомірного) поширення цієї інформації серед третіх осіб, які не мають доступ до неї.

До витоку конфіденційної інформації призводить несанкціоноване отримання інформації, що захищається як особами, які безпосередньо не працюють в організації, так і співробітниками, не уповноваженими знайомитися з цією інформацією.

Зазначимо, що конфіденційне діловодство має свій специфічний об’єкт захисту – конфіденційний документ. Специфічність конфіденційних документів у порівнянні з документами відкритого доступу виражається в особливому режимі поводження з ними, що накладає обмеження на ознайомлення, копіювання та розмноження документів, наявність спеціального маркування тощо [40, с. 18].

У конфіденційному діловодстві існує й інше ставлення до документообігу, який розглядають не лише як технологічний процес (сукупність маршрутів руху документів за встановленими пунктами обліку, розгляду, виконання та зберігання), а й як об’єкт захисту, що є сукупністю (мережею) каналів об’єктивного, санкціонованого поширення конфіденційної документованої інформації у процесі управлінської та виробничої діяльності користувачів (споживачів цієї інформації) .

Незалежно від різновидів конфіденційних документів необхідно дотримуватись загальних вимог до порядку роботи з ними (вимоги до порядку руху, ознайомлення з документами, передавання їх до архіву тощо) та в цілому забезпечення конфіденційності інформації.

Витік (розголошення), а також втрата конфіденційної документованої інформації обумовлені проявом різних загроз безпеці конфіденційних документів, до яких належать:

- крадіжка документа, його частини, чернеток, проєкту чи носія;
- втрата документа, його чорнового варіанту, робочих записів;
- несанкціоноване знищення носія чи самої інформації (руйнування);
- заміна документа, його окремих частин чи носія;
- несанкціоноване копіювання інформації;

– несанкціонована модифікація (зміна) інформації, що міститься в документі.

Безумовно, у конфіденційному діловодстві загрози включають різні негативні дії, спрямовані не тільки на сам документ, а й на чернетки та проєкти документів, а також чисті носії, призначені для складання документа або його чернетки (проєкту).

Робочі записи розробників (упорядників, виконавців), що виникли в процесі створення документа, можуть включати більший обсяг конфіденційних відомостей, аніж сам документ, і відповідно ставати каналом витоку інформації, що охороняється. Відповідно, вже з моменту задуму створення того чи іншого документа, що містить конфіденційні відомості організації, виникає потенційна загроза витоку цих відомостей, внаслідок чого повинні вживатися адекватні заходи щодо її запобігання.

Як джерела загроз конфіденційної документованої інформації можуть бути люди, технічні засоби оброблення і передавання інформації, стихійні лиха тощо.

Безпека цінної документованої інформації визначається її рівнем захищеності від екстремальних обставин, а саме від: природніх катаклізмів, а також від пасивних та активних загроз, які створюють зловмисники з метою отримання несанкціонованого доступу до документів через організаційні та технічні канали. До дестабілізуючих факторів належить модифікація, підміна, фальсифікація або знищення інформації для власних цілей зловмисників.

Способами дестабілізуючого впливу на інформацію, що захищається, є порушення технології її оброблення та зберігання, фізичний вплив на носій інформації тощо.

Дослідники визначають такі способи порушення конфіденційності документної інформації:

1) під час відсутності на робочому місці користувач не блокує комп’ютер, внаслідок чого доступ до інформації мають сторонні особи;

2) при включенні комп’ютера до мережі користувач не знає, яка інформація доступна іншим користувачам;

3) зі своїх робочих комп’ютерів користувачі виходять до незахищених мереж загального користування (інтернет), створюючи можливість витоку інформації;

4) користувачі встановлюють на свої комп’ютери стороннє програмне забезпечення, яке знижує продуктивність та збільшує ризик виходу зі системи [37, с. 25].

Для своєчасного реагування на порушення необхідно проводити моніторинг безпеки інформації, який передбачає постійне спостереження за процесом забезпечення захисту інформації в системі з метою встановлення відповідності вимогам безпеки даних.

Усі організації, які здійснюють оброблення конфіденційної інформації (насамперед персональних даних), повинні виконувати такі вимоги:

1) дотримуватися норм закону України «Про захист персональних даних», забезпечивши при цьому всі необхідні докази законності збирання та оброблення персональної особової інформації;

2) забезпечувати захист від несанкціонованого розповсюдження персональних даних;

3) розробляти нормативні локальні акти й технічну організаційну документацію для забезпечення регламентованого оброблення персональних даних.

Зазначимо, що *конфіденційність* – це форма обмеженням доступу до інформації власником, який встановлює відповідний правовий режим відповідно до чинного законодавства. До категорії конфіденційних не відносять: установчі документи, статути підприємств, фінансову звітність, інформацію про заробітну плату персоналу та іншу документну інформацію, яку обов’язково надають правоохоронним та податковим органам держави для перевірки.

Конфіденційним документом є оформлений носій документованої інформації з відомостями, що належать до недержавної таємниці та становлять інтелектуальну власність юридичної чи фізичної особи. Обов'язковою ознакою конфіденційного документа є наявність у ньому інформації, що підлягає захисту.

До конфіденційних належать такі документи:

1) у державних структурах – документи, проєкти документів, супровідні матеріали, що належать до інформації обмеженого розповсюдження і містять дані службової таємниці, заборонені для опублікування;

2) в установах, організаціях, підприємствах – документна інформація, яку відносять до комерційної таємниці, зокрема патенти, схеми, технічні креслення, технічні специфікації, які містять важливі деталі про виробництво, дизайн або функціонування технологій;

3) незалежно від належності – документи та бази даних, які стосуються особистих даних громадян (ідентифікаційні номери, адреси, медична інформація, фінансова інформація та інші особисті дані, які підлягають захисту від несанкціонованого доступу та використання) [40, с. 21].

Конфіденційний документ є захищеним носієм цінної інформації; основним джерелом поширення такої інформації, а також її неправомірного розголошення чи витоку; обов'язковим об'єктом захисту.

Документообіг – це процес руху паперових, машиночитаних та електронних документів за встановленими пунктами їх обліку, розгляду, виконання та зберігання для виконання творчих, формально-логічних та технічних процедур та операцій. Переміщення конфіденційних документів зі ієрархічними рівнями управління створює серйозні передумови втрати цінної інформації, вимагає здійснення захисних заходів щодо документопотоків і документообігу загалом.

Варто підкреслити, що документообіг як об'єкт захисту є упорядкованою сукупністю (мережею) каналів об'єктивного,

санкціонованого поширення конфіденційної документованої інформації (документів) у процесі управлінської та виробничої діяльності користувачів (споживачів) цієї інформації. Основною характеристикою руху інформації є технологічна комплексність, тобто поєднання завдань, що забезпечують управлінські, діловодні та поштові функції. Документообіг відображає весь життєвий цикл документа.

Загальні принципи руху конфіденційних документів у системі управління установи незмінні під час технологічної системи оброблення, зберігання та поширення документів.

Під час руху конфіденційних документів збільшується кількість джерел інформації (співробітників, баз даних, робочих матеріалів тощо), які мають цінні відомості, і розширюються потенційні можливості для втрати конфіденційної інформації, її розголошення персоналом, витоку технічних каналів, зникнення носія цієї інформації.

Захищеним документообігом є «рух конфіденційної документованої інформації за регламентованими пунктами прийому, оброблення, розгляду, виконання, використання та зберігання в умовах організаційного та технологічного забезпечення захисту як носія, так й інформації» [19, с. 498].

Принципами захищеного документообігу є:

1) забезпечення доступу до документів лише авторизованих осіб, що уможливлює захист інформації від несанкціонованого доступу;

2) систематичне відстеження і фіксація всіх операцій, пов’язаних з опрацюванням документів;

3) використання криптографічних методів захисту документів під час передавання та зберігання для забезпечення конфіденційності та цілісності даних;

4) забезпечення механізмів резервного копіювання та відновлення документів у випадку втрати або пошкодження їх.

Захищеність документопотоків досягається за рахунок: одночасного використання режимних заходів та технологічних прийомів, що входять до

системи оброблення та зберігання конфіденційних документів; нанесення позначки на чистий носій конфіденційної інформації або документ, у тому числі супровідний, що дозволяє виділити їх у загальному потоці документів; формування самостійних, ізольованих потоків конфіденційних документів та додаткового їх поділу на підтоки відповідно до рівня конфіденційності документів, що переміщуються; використання автономної технологічної системи оброблення та зберігання конфіденційних документів.

Відомо, що інформація – це один із найважливіших ресурсів підприємства, який забезпечує чітку та злагоджену роботу кожного підрозділу підприємства. Виходячи з важливості конфіденційної інформації з'являється ризик для організації втратити цінний ресурс. Щоб уникнути проблем, пов'язаних із втратою або розкраданням інформації в організаціях, створюють служби конфіденційного діловодства.

Працівники служби діловодства в організації контролюють конфіденційні документи та інформацію, управляють документопотоками, створюють бази даних для комп'ютерних систем і картотеки для паперових носіїв, знищують чернетки документів, зберігають важливі для організації документи та знищують їх відповідно до встановлених процедур.

Захист інформації в документопотоках забезпечують комплексом різноманітних заходів технологічного, аналітичного та контрольного характеру. Кожна стадія, процедура оброблення або виконання документа супроводжують відповідними обліковими операціями, закріпленням документа за конкретним співробітником та його персональною відповідальністю за збереження носія і конфіденційність інформації.

Загалом, технологічний процес обліку конфіденційних документів включає операції, які є обов'язковими для обліку, оброблення та зберігання цих документів. У процесі передавання документів виконавцям і повернення документів виконують комплекс технологічних та обмежувальних операцій, що дозволяють запобігти розголошенню та витоку документної інформації.

Провівши аналіз організації конфіденційного діловодства, було виявлено, що частина сучасних компаній реєструють конфіденційні документи в автоматизованій системі, інші – дотримуються паперової форми реєстрації документів, попри те, що в компаніях встановлено системи електронного документообігу. Це зазвичай пов’язано з браком знань та умінь використання нових технологічних та програмних засобів працівниками діловодства.

Отже, перспективою створення єдиної системи конфіденційного діловодства, що відповідає сучасним вимогам щодо автоматизації процедур оброблення інформації різних рівнів доступу, зводиться до доопрацювання наявної нормативно-методичної бази щодо роботи з інформацією обмеженого доступу та розроблення нових методичних документів, що регламентують порядок та технології роботи з конфіденційними документами в автоматизованих системах. Такий спосіб є релевантним для будь-яких типів автоматизованих інформаційних систем, наприклад, систем електронного документообігу.

Висновки до розділу 1

У першому розділі визначено основні нормативно-правові та організаційні аспекти роботи з конфіденційною інформацією. Встановлено, що конфіденційною є інформація, яка становить комерційну, виробничу, особисту таємницю, та не підлягає широкому розголошенню. До категорії конфіденційної інформації відносимо: персональні дані фізичних осіб, комерційну таємницю, професійну таємницю, інформацію, яка обмежена в доступу відповідно до законодавства.

Нормативно-методичне забезпечення системи захисту конфіденційної інформації призначене для регламентації процесів забезпечення безпеки інформації підприємства, зокрема під час роботи персоналу з конфіденційними відомостями, документами, базами даних.

Визначено перелік нормативно-правових актів, які забезпечують захист конфіденційної інформації. До цього переліку віднесено: Конституцію України, ЗУ «Про інформацію», ЗУ «Про захист персональних даних», ЗУ «Про доступ до публічної інформації», ЗУ «Про державну таємницю», постанови КМУ, накази міністерств та центральних органів виконавчої влади, інструкції та положення державних органів.

Досліджено особливості організації конфіденційного діловодства в умовах розвитку інформаційних технологій. Встановлено, що метою конфіденційного діловодства є забезпечення захисту конфіденційної інформації, що міститься в документах, від несанкціонованого доступу, витоку, втрати або пошкодження.

У процесі аналізу діяльності служби діловодства з’ясовано, що її працівники контролюють конфіденційні документи та інформацію, управляють документопотоками, створюють бази даних для комп’ютерних систем і картотеки для паперових носіїв, знищують чернетки документів, зберігають важливі для організації документи та знищують їх відповідно до встановлених процедур.

Отже, служба діловодства має забезпечувати захист конфіденційної інформації на всіх етапах її життєвого циклу, починаючи від створення документа і до його знищення або архівації.

РОЗДІЛ 2
ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ТА ЗАХИСТУ АВТОМАТИЗОВАНОЇ СИСТЕМИ ДІЛОВОДСТВА ВІЙСЬКОВОЇ ЧАСТИНИ

2.1. Аналіз ефективності організації обігу документів обмеженого доступу військової частини

Ведення документів у бригаді тактичної авіації є критично важливою частиною її функціонування. Це забезпечує належне управління, координацію, облік і звітність, необхідні для ефективного виконання завдань. Ведення документів обмеженого доступу вимагає ретельного підходу і дотримання встановлених норм та стандартів, що забезпечують чітку та ефективну роботу бригади тактичної авіації.

Зазначимо, що *військова частина* – це структурний підрозділ Збройних Сил, який має власне організаційне і командне управління, чітко визначене місце дислокації та завдання, що виконує конкретні функції щодо забезпечення обороноздатності держави.

Військова частина включає особовий склад, техніку та озброєння, необхідні для виконання бойових і службових завдань.

Військова частина є складником Збройних сил України, створеним відповідно до директиви або наказу вищого командування, який виконує завдання та функції, визначені специфікою діяльності різних видів Збройних Сил. Керування частиною покладено на командира, який відповідає за організацію та виконання бойових завдань, підтримання дисципліни та порядку, управління особовим складом, технікою та озброєнням, а також забезпечення належного рівня бойової готовності підрозділу.

Бригада тактичної авіації є ключовим елементом військово-повітряних сил і виконує широкий спектр завдань, включаючи повітряні удари, підтримку наземних військ, розвідку, а також захист повітряного простору.

Організаційно повітряні сили України складаються з таких підрозділів: Повітряне командування «Захід»; Повітряне командування «Центр»; Повітряне командування «Схід»; Повітряне командування «Південь». Розглянута військова частина входить в один із зазначених підрозділів.

Варто також зазначити, що організаційна структура бригади тактичної авіації складається з різних підрозділів, кожен з яких виконує свої специфічні завдання. Вона включає такі основні компоненти:

1) командування (командир, заступник командира) – здійснює загальне керівництво та несе відповідальність за бойову готовність, виконання завдань бригади;

2) штаб бригади (начальник штабу, оперативний відділ, відділ розвідки, відділ зв'язку, відділ документаційного забезпечення управління (діловодства), відділ логістики) – координує основні процеси роботи штабу і забезпечує виконання наказів командира;

3) авіаційні ескадрильї № 1, 2 – основні бойові підрозділи, які оснащені бойовими літаками;

4) підрозділи забезпечення: пожежний взвод, медичний пункт, технічна служба, транспортний підрозділ;

5) батальйони (зв'язку та радіотехнічного забезпечення; аеродромно-технічного забезпечення).

Розглянемо організаційну структуру військової частини на рисунку 2.1.

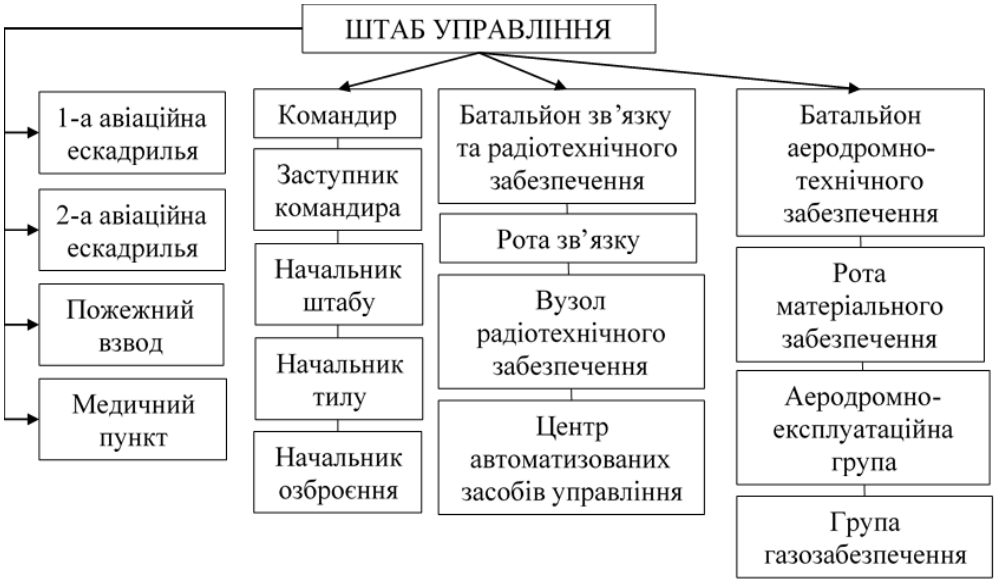

Рисунок 2.1. Організаційна структура військової частини

Розроблено автором

Організація конфіденційного діловодства у військовій організації покладається на службу документного забезпечення управління, яка відповідальна за розроблення, упровадження та контроль за дотриманням процесів, що забезпечують належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів.

Роль начальника служби діловодства військової частини полягає у керівництві процесами організації, зберігання та оброблення документів, що пов’язані з функціонуванням військової одиниці. Ця посада передбачає відповідальність за встановлення системи реєстрації та класифікації документів, забезпечення їх безпеки та доступності, а також ведення документального обліку відповідно до законодавства та внутрішніх вимог військової установи. До того ж начальник служби діловодства може брати активну участь у розробленні стратегій та політики управління документообігом для оптимізації робочих процесів та забезпечення ефективності управління інформацією [29, с. 83].

Організація діловодного обслуговування військових підрозділів проводиться у спеціально обладнаних приміщеннях, що відокремлені, оснащених тамбуром із вікном для видачі документів або бар’єром. Для забезпечення захисту вхідних документів двері приміщень мають бути оснащені надійними замками. Основні етапи роботи служби документаційного забезпечення управління здійснюють відповідно до розпорядку дня, встановленого начальником військової частини.

Основне завдання служби діловодства – це забезпечення у військовій частині уніфікованого порядку документування управлінської інформації та роботи з документами, а також використанням сучасних інформаційних технологій для автоматизації основних процесів роботи з електронними даними. Також відповідна служба відповідає за методичне керівництво та

контроль дотримання послідовності етап роботи з документами в усіх підрозділах військової частини [30, с. 68].

Визначено, що працівникам особового складу військових частин, які здійснюють оброблення службових документів, заборонено:

1) усно або письмово передавати інформацію про службові операції, заходи та дійсні місця розташування військових частин особам, що не мають відношення до цих операцій;

2) вносити особисті запити на бланках з назвою військової частини;

3) незаконно перевозити або передавати через кордон службові документи або видання, які не підлягають опублікуванню;

4) вести обговорення щодо змісту службових документів у присутності осіб, що не мають відношення до цих документів [28, с. 261].

Командир військової частини затверджує список працівників, які відповідають за облік документів обмеженого доступу, у формі: резолюції на документі; розпорядчого документа із зазначенням прізвищ виконавців; письмового дозволу. За порушенням вимог зберігання і виконання документів, які містять інформацію обмеженого доступу, працівники служби ДЗУ несуть відповідальність згідно з чинним законодавством.

Документи обмеженого доступу групують відповідно до призначення:

1) з питань мобілізації (на документах проставляють літеру «М»);

2) з питань криптографічного захисту інформації (проставляють гриф «К»);

3) з питань інформації спеціального призначення (проставляють літери «СІ»).

Для забезпечення конфіденційного діловодства існують такі напрями діяльності: документування, документообіг, оперативне зберігання документів, використання документів, захист інформації.

Документообіг як основний складник діловодства військової частини регламентується інструкцією з документування управлінської інформації та організації роботи з документами, яка затверджена наказом командира

військової частини. До основних операцій військового документообігу включають: реєстрацію та первинне опрацювання вхідної кореспонденції; ведення реєстрів та журналів обліку документів; передавання документів на виконання до структурного підрозділу чи посадової особи; забезпечення зберігання та доступу до документів; складання та оформлення вихідних документів; захист інформації від несанкціонованого доступу, зміни чи знищення. Обіг документів обмеженого доступу складається з вхідних, вихідних і внутрішніх військових документів.

Зазначимо, що *військове документування* – це систематичний процес створення, оброблення, зберігання, захисту та використання документів у військових організаціях, спрямований на забезпечення належного управління, виконання завдань, підтримку оперативної діяльності та забезпечення правової захищеності [30, с. 74].

Основними принципами військового документування є:

1) *законність* – всі документи повинні відповідати чинному законодавству та нормативно-правовим актам;

2) *конфіденційність* – захист документів від несанкціонованого доступу та розголошення інформації;

3) *уніфікація* – використання стандартів, типових форм та методів роботи з документами;

4) *захист* – забезпечення належного фізичного збереження документів та їх захист від пошкодження, зміни або втрати.

Ці принципи сприяють ефективному управлінню документами у військовій сфері, забезпечують належний рівень безпеки та правову захищеність діяльності військових організацій.

Військові документи – це офіційні документи, які створюють, отримують та зберігають військові організації та установи в процесі діяльності. Вони відображають управлінську, оперативну, адміністративну та діяльність у сфері національної безпеки та оборони. Саме документи є

основним засобом для прийняття управлінських рішень і керування військового частиною [30, с. 75].

Особливістю військових документів є їх відомча приналежність до Збройних Сил України, яка визначається тим, що документи розробляють та видають посадовими особами армії. Військові документи використовують переважно у військових частинах та установах у межах військового відомства. Їхня дія поширюється на посадових осіб військових частин, військовослужбовців, громадянський персонал ЗСУ і в окремих випадках на інших громадян країни.

Документний склад військової частини відображено на рис.2.2.

Рисунок 2.2. Документний склад військової частини

Розроблено автором

Загальні характеристики документного складу військового управління включають: сувору цільову спрямованість; предметно-матеріальне закріплення інформації; наявність необхідних формальних елементів для ідентифікації та використання документів.

Основними групами військових документів є:

1. *Нормативно-правові акти* (накази, розпорядження, інструкції, постанови), які регулюють діяльність військових підрозділів та установ.

2. *Адміністративні документи* (плани, звіти, протоколи, службові записки), що відображають організаційно-управлінську діяльність.

3. *Оперативно-службові документи* (бойові накази та розпорядження, директиви, оперативні плани, донесення, звіти про виконання бойових завдань).

4. *Фінансово-економічні документи*, зокрема: бюджети, кошториси, фінансові звіти, документи обліку та звітності.

5. *Особові документи* (особові справи, трудові книжки, характеристики, атестації військовослужбовців тощо).

6. *Інформаційно-довідкові документи*, а саме: довідки, аналітичні огляди, доповіді.

Варто також зазначити, що військові документи забезпечують: інформаційну підтримку управлінських рішень, фіксують управлінські процеси і дії; планування, організацію та контроль оперативної діяльності військових підрозділів; правовий статус документної інформації; контроль за виконанням поставлених завдань; передавання інформації між різними рівнями управління та підрозділами у сфері оборони країни.

Документний склад військової частина відіграє ключову роль у реалізації заходів з бойової підготовки, оперативних і мобілізаційних питань, організації служби військ, матеріально-технічного забезпечення, а також експлуатації озброєння і бойової техніки. Загальними функціями військових документів є: інформаційно-комунікативна, кумулятивна, комунікативна, культурна. До спеціальних функцій належать: управлінська, пізнавальна, правова, облікова.

Втрата, зміна чи знищення інформації обмеженого доступу особливо небезпечна в електронних документах, адже виявити факт порушення конфіденційності досить складно. До факторів ризику щодо захисту конфіденційної інформації військової частини належать:

1. Поширення та доступність багатофункціональних засобів інформатизації та зв’язку відкривають можливості для «разового» використання абонентського обладнання з метою приховування протиправної діяльності, утруднення можливого контролю з боку правоохоронних органів та збирання ними доказової бази.

2. Розвиток послуг з надання доступу до мережі Інтернет як стаціонарного, так і мобільного забезпечує свободу передавання інформації:

– дозволяє зловмисникам встановлювати контакт із зацікавленою стороною (спецслужбами, злочинцями);

– ускладнює виявлення та припинення їх діяльності, а також визначення ідентифікаційних даних;

– відкриває для правопорушників можливості щодо вибору найбільш сприятливих місця та часу передавання викраденої інформації.

3. Мережеві технології, стандарти, протоколи, відповідне програмне та апаратне забезпечення загалом розробляють за кордоном, що не дозволяє повністю контролювати усі функціональні можливості таких інструментів.

4. Анонімне використання засобів та послуг зв’язку, а також доступ до мережі Інтернет додатково ускладнюють ідентифікацію осіб, їх пошук та фіксацію дій.

5. Різноманітність служб, сервісів та програмного забезпечення, призначених для передавання інформації в мережі Інтернет (електронна пошта, соціальні мережі, програми-месенджери, файлообмінні мережі тощо) створює передумови для організації прихованої багатоканальної взаємодії між членами злочинних груп та спільнот, а також сприяє розвитку незаконного обігу інформації обмеженого доступу.

6. Широке поширення та доступність програм, призначених для шифрування трафіку, забезпечення анонімності користувачів та приховування активності в мережі, сприяє формуванню у злочинців почуття безкарності, переконаності у неможливості їх викриття та затримання правоохоронними органами.

7. Недосконаліть правової системи, що регулює суспільні відносини в інформаційній сфері, додатково ускладнює діяльність правоохоронних органів щодо контролю за інформаційними ресурсами відкритих інформаційно-телекомунікаційних мереж.

8. Недостатня підготовленість та обізнаність військовослужбовців про актуальні інформаційні загрози дозволяють зловмисникам розглядати особовий склад як найуразливіший елемент у системі обігу закритої інформації.

На сучасному етапі існують такі типи захисту конфіденційної інформації: організаційний, законодавчий, фізичний, технічний, а також взаємодія з працівниками.

Способи захисту електронних документів військової частини включають: шифрування даних, зокрема використання криптографічних методів для перетворення інформації в код, доступний лише уповноваженим особам; використання електронних підписів для забезпечення автентичності та цілісності документів; впровадження систем управління доступом; використання багаторівневого механізму перевірки користувачів; встановлення антивірусного програмного забезпечення для виявлення та нейтралізації шкідливих програм; створення резервних копій даних для відновлення інформації у випадку втрати чи пошкодження; розроблення та впровадження внутрішньої політики щодо захисту інформації [39, с. 91].

Аналіз ефективності організації обігу документів обмеженого доступу військової частини уможливив формулювання таких висновків:

1. Виявлено, що лише 80% документів обмеженого доступу мають належний рівень захисту інформації, тоді як решта 20% може бути доступна неуповноваженим особам через недостатній контроль за розповсюдженням документів.

2. Середній час оброблення документів складає 2 робочих дні, що відповідає стандартам, проте існують певні затримки у випадках оброблення документів, які потребують додаткових дозволів або перевірок.

3. Встановлені процедури обігу документів дотримуються належним чином на 90%, проте залишаються окремі випадки, коли документи можуть бути використані без відповідного авторизованого доступу.

4. Система аудиту дозволяє виявляти порушення безпеки даних, однак деякі інциденти залишаються непоміченими через недостатню автоматизацію цього процесу.

5. Технічні засоби захисту документів обмеженого доступу військової частини виявилися надійними, проте необхідно оновити програмне забезпечення для підвищення ефективності. Наявність застарілих програмних та апаратних засобів знижує ефективність системи контролю та захисту інформації.

Відповідно до проведеного аналізу ефективності обігу документів обмеженого доступу військової частини рекомендовано впровадити нові програмні засоби для автоматизації процесу оброблення документів, організувати навчання персоналу з використання цих систем та зміцнити систему аудиту та контролю для забезпечення максимального рівня безпеки конфіденційної інформації.

2.2. Проблеми та перспективи забезпечення захисту інформації обмеженого доступу в СЕД військової частини

Після проведено аналізу системи обігу документів обмеженого доступу виявлено проблеми, які пов’язані з: відсутністю оснащення сучасними уніфікованими засобами автоматизації, телекомунікації та зв’язку; недосконалістю засобів і механізмів управління доступом до інформаційних ресурсів; порушенням принципу одноразового введення інформації під час діяльності посадових осіб служби діловодства військової частини.

Автоматизація всього циклу роботи з документами військової частини дозволить значно підвищити рівень керування підрозділами для забезпечення необхідно розмежування доступу до інформації обмеженого доступу. Структура і зміст інформаційних потоків системи повинні відповідати

факторам, які впливають на вирішення поставлених військовій частині бойових завдань.

Електронний документообіг має стати основою для організації оперативного вирішення різних завдань діяльності військової частина, зокрема для забезпечення автоматизованого обміну даними під час технічного обслуговування авіаційної техніки, оцінки стану об’єктів частини тощо. Електронний документообіг значно оптимізує процеси роботи з документами, зменшуючи витрати часу, ресурсів та паперу, а також підвищуючи рівень безпеки та ефективності.

Електронний документообіг – це «процес обміну документами та інформацією електронному форматі; створення, оброблення, підписання, розсилання та зберігання документів за допомогою цифрових технологій та спеціалізованих програмних засобів» [20, с. 16].

Перевагами електронного документообігу є: швидкість передавання документів у режимі реального часу; ефективність автоматизованого створення, підписання та надсилання документів; забезпечення захисту інформації обмеженого доступу за допомогою шифрування даних та ідентифікації користувачів; використання засобів аудиту та контролю для відстеження основних процесів роботи з документами.

Система електронного документообігу (СЕД) – це комплекс програм для автоматизації та оптимізації процесів обміну документами в електронному форматі.

Основні компоненти систем електронного документообігу включають:

1. Серверне програмне забезпечення, яке забезпечує функції зберігання документів, керування правами доступу, автентифікацію користувачів та інші адміністративні функції.

2. Клієнтське програмне забезпечення, яке встановлюють на комп’ютери користувачів для взаємодії з системою електронного документообігу через графічний інтерфейс.

3. Модуль для інтеграції з іншими системами, зокрема системами управління відносинами з клієнтами, системами управління фінансами або електронними поштовими сервісами.

3. Модуль безпеки, який забезпечує захист від несанкціонованого доступу до документів, шифрування даних та інші методи безпеки.

4. Модуль аналітики для аналізу даних та статистики щодо обігу документів, що дозволяє здійснювати контроль та оптимізацію робочих процесів.

Вибір відповідної системи електронного документообігу необхідно здійснювати відповідно до потреб та вимог військової частини. При цьому необхідно враховувати не лише функціональні характеристики системи, але й зручність, безпеку, інформаційну підтримку, вартість та аспекти, пов’язані зі специфікою захисту документів обмеженого доступу.

Класифікація програмних рішень для систем електронного документообігу може бути здійснена за різними критеріями, включаючи функціональність, призначення, архітектуру, технологію діловодства, відкритість і масштабованість системи, способи захисту інформації, вартість. Комплексний підхід обрання СЕД дозволить здійснити впровадження системи, яка повністю відповідатиме вимогам автоматизації управлінської діяльності військової бригади.

Загальна класифікація СЕД здійснюємо за типовими характеристиками, зокрема:

1. За функціональністю:

– системи управління документами, які призначені для створення, зберігання, організації, керування правами доступу до документів (Microsoft SharePoint, OpenText, Alfresco);

– системи електронного підпису та цифрових сертифікатів, які забезпечують юридичної чинності за допомогою електронного цифрового підпису (DocuSign, Adobe Sign, GlobalSign);

– системи управління робочими процесами автоматизують бізнес-процеси, пов’язані з обробленням документів (IBM Business Process Manager, Appian, Bonita BPM).

2. За призначенням:

– універсальні системи, призначені для використання в різних галузях та організаціях (Microsoft SharePoint, OpenText, Alfresco);

– галузеві рішення – спеціалізовані для певних галузей, зокрема для військових організацій (DefenseReady).

3. За архітектурою:

– клієнт-серверні системи, в яких документи та програмні модулі зберігаються на сервері, а доступ до них здійснюється через клієнтські додатки (Microsoft SharePoint, Alfresco);

– хмарні рішення, які забезпечують доступ до документів через вебінтерфейси (Google Workspace, Dropbox Business, Box).

4. За рівнем інтеграції:

– незалежні програми, які використовують без інтеграції з іншими системами (Evernote, Notion);

– інтегровані системи (SAP Document Management, Microsoft Dynamics 365).

Для військових організацій важливо обирати систему, що забезпечить високий рівень безпеки, інтеграцію з існуючими системами та підтримку специфічних вимог військової частини. На основі аналізу визначено, що найкращими варіантами можуть бути комплексні програми Microsoft SharePoint та OpenText, або гнучкі хмарні програми Google Workspace та DocuWare.

Проведемо комплексну оцінку систем електронного документообігу, які доречно впровадити у діяльність військової частини:

1. Microsoft SharePoint – це потужна платформа, розроблена для управління контентом, співпраці та створення інтранет-сайтів у межах організацій (рис. 2.3).

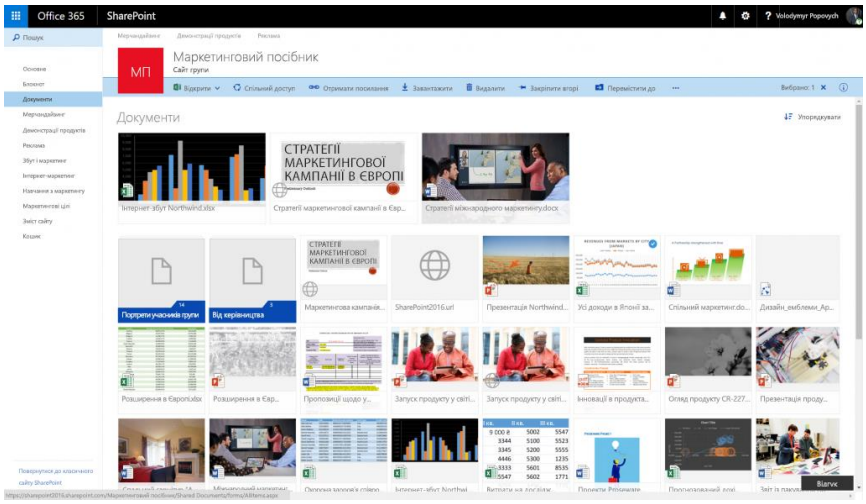

Рисунок 2.3. Інтерфейс програми Microsoft SharePoint

Функціональні можливості системи Microsoft SharePoint:

– інтегрується з іншими продуктами Microsoft, такими як Office 365, Teams, Outlook, що сприяє зручності експлуатації;

– підтримує багаторівневу систему безпеки, зокрема багатофакторну аутентифікацію та шифрування даних;

– містить всі необхідні модулі для робочих процесів та управління документами [46].

2. OpenText – це глобальна компанія, яка спеціалізується на програмному забезпеченні для управління інформацією та корпоративного управління контентом (ECM). Продукти OpenText забезпечують рішення для управління документами, електронними архівами, автоматизації бізнес-процесів та інших аспектів управління інформацією в організаціях (рис. 2.4).

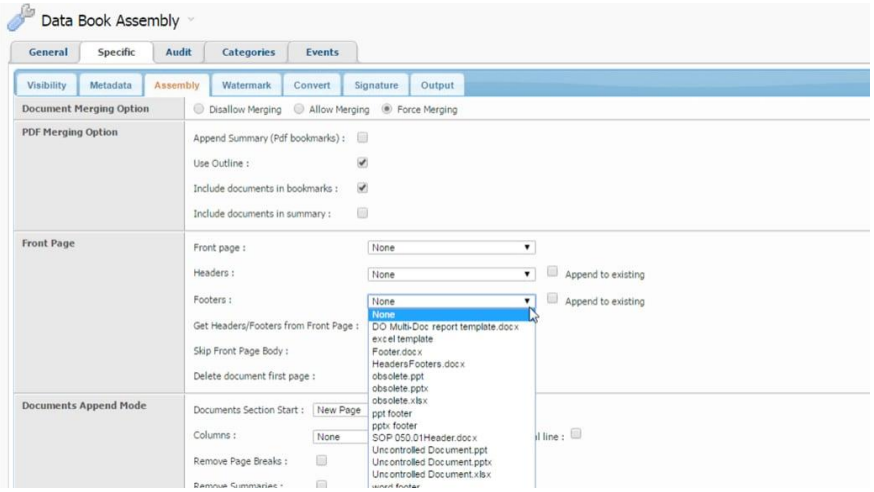

Рисунок 2.4. Інтерфейс програми OpenText

Функціональні можливості системи OpenText:

– пропонує повний спектр функцій для управління документами, а саме: архівацію, зберігання та редагування;

– підтримує всі сучасні стандарти безпеки та захисту даних;

– легко інтегрується з іншими корпоративними системами [45].

3. DocuWare – це сучасна платформа для управління документами та автоматизації робочих процесів, яка допомагає організаціям ефективно зберігати, керувати та опрацьовувати електронні документи (рис. 2.5).

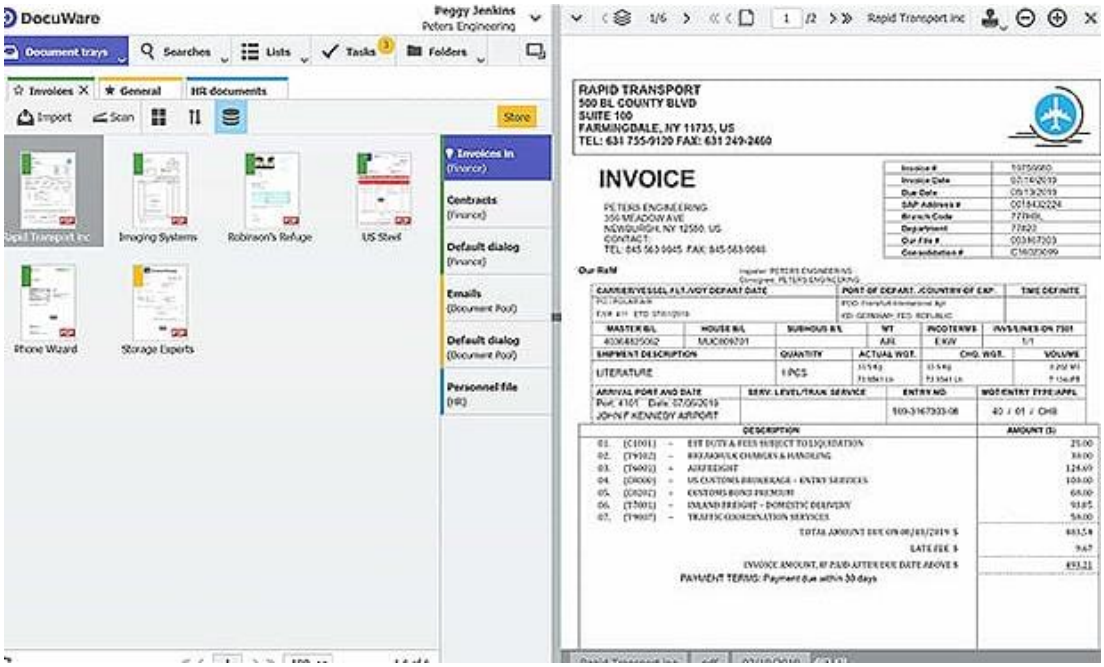

Рисунок 2.5. Інтерфейс програми DocuWare

Функціональні можливості системи DocuWare:

– забезпечує доступ до інформаційних ресурсів з будь-якого пристрою;

– має сертифікати відповідності найвищим стандартам безпеки;

– підтримує розширення функції автоматизації основних процесів роботи з документами [43].

4. Google Workspace – це набір інструментів для продуктивності та співпраці, розроблений компанією Google. Він призначений для покращення роботи в командах та забезпечення ефективної комунікації й управління контентом (рис. 2.6).

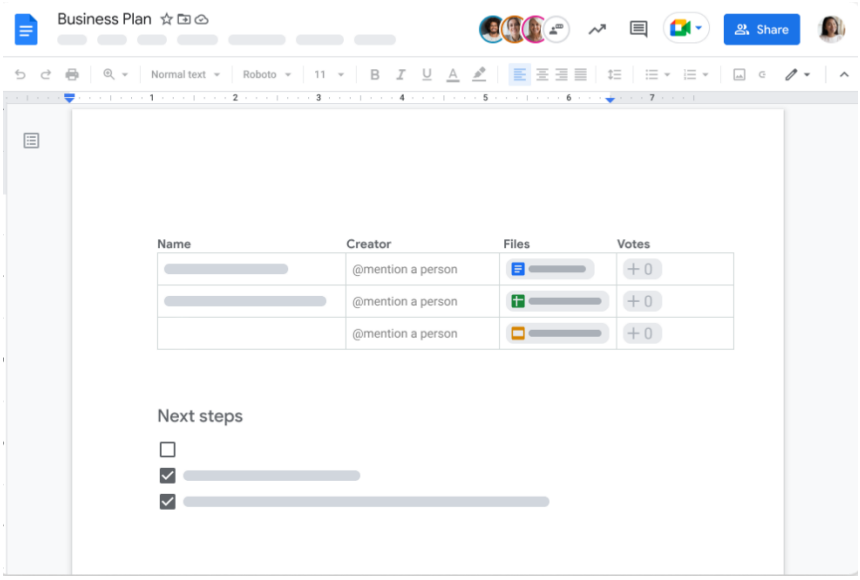

Рисунок 2.6. Інтерфейс програми Google Workspace (для роботи з електронними документами)

Функціональні можливості системи Google Workspace:

– організація кореспонденції та обмін документами електронною поштою;

– зберігання, організація, керування та спільна робота над документами у режимі реального часу;

– відстеження та аудит змін у документах для забезпечення прозорості та відповідності інформації;

– налаштування прав доступу до документів та контроль за їхнім використанням [44].

Для ефективної роботи служби діловодства військової частини запропоновано створення системи електронного документообігу, заснованої на локальній мережі з використанням хмарної технології Google Workspace та інтегрованого програмного забезпечення, що дозволяє ефективно застосовувати наявне телекомунікаційне обладнання. Встановлено, що це підвищує ефективність функціонування всіх ланок управління, значно спрощує діяльність командування військової частини, зменшує кількість особового складу, задіяного для ведення документообігу, та суттєво знижує фінансові витрати.

Основні інструменти хмарної технології Google Workspace відображено на рисунку 2.7.

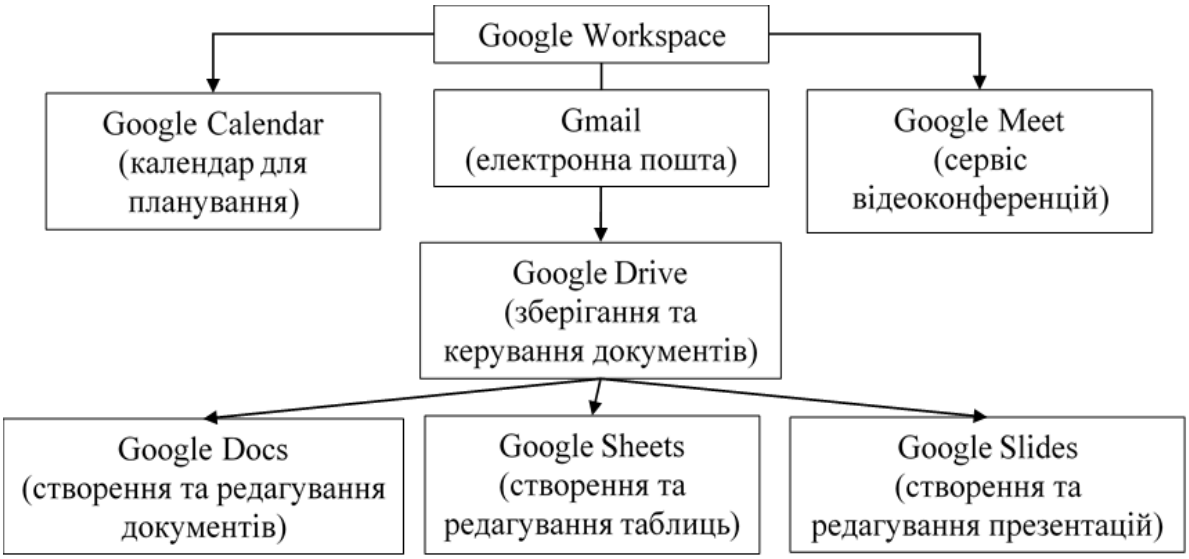

Рисунок 2.7. Інструменти хмарної технології Google Workspace

Розроблено автором за матеріалами [44]

Отже, інформаційна технологія Google Workspace значно покращує ефективність створення та використання інформаційно-комунікаційних послуг для військової частини. Правильно спроєктована та впроваджена хмарна технологія сприяє підвищенню ефективності роботи командування, кожної посадової особи та можливостей колективної роботи.

У військовій частині необхідно також ввести в експлуатації комплексну систему захисту інформації системи електронного документообігу. Доречно створити спеціальну службу захисту інформації, які буде адмініструвати усі процеси роботи з електронними документами в автоматизованій системі. Така служба координуватиме та консультуватиме роботи з впровадження чи модернізації системи захисту СЕД.

Для запобігання порушення захисту електронних документів у системі електронного документообігу рекомендовано також використати технологію розподілених реєстрів (блокчейн).

Блокчейн – це децентралізована технологія зберігання даних, яку використовують для створення послідовних ланцюжків блоків інформації про певні транзакції [15]. Для розподілення реєстрів використовують три основні

технології: мережеву архітектуру, кодування та бази даних. Технологія розподілених реєстрів забезпечує захисту, цілісність і незмінність даних.

Алгоритм роботи блокчейн-мережі складається з п’яти послідовних етапів: визначення транзакції; аутентифікація транзакції; створення блоку інформації; перевірка блоку; створення захищеного ланцюжка блоків даних.

СЕД на основі технології блокчейн є незалежною від централізованого сервера, що значно знижує ймовірність шахрайства. Відстеження постійних змін інфраструктури електронних документів та їх відповідність електронному підпису у системі відбувається за допомогою смарт-контрактів (автономних комп’ютерних програм оброблення запитів) [15].

За допомогою технології блокчейн процес передавання нових документів до військової частини і внесення змін до чинних нормативно-правових актів, порівняно з паперовим документообігом, значно прискориться. Відсутність необхідності відправлення паперового документа та внесення змін до нього призведе до зниження впливу «людського фактору».

Технологія розподілення даних повністю автоматизує основні процеси роботи з електронними документами на базі військової частини: приймання, первинне опрацювання, облік, відправлення та збереження службових документів; передавання командуванню вхідних документів і передавання їх на виконання відповідно до рішень керівництва; формування і оформлення справ, забезпечення їхнього обліку і зберігання; надання доступу до інформаційних ресурсів; дотримання правил роботи з документами обмеженого доступу; забезпечення оригінальності і актуальності електронних документів.

Система електронного документообігу на основі технології блокчейн дозволить автоматизувати процеси аудиту та моніторингу даних в системі електронного документообігу військової частини, а саме:

1) автоматизувати процеси контролю доступу до електронних документів;

2) реєструвати процеси опрацювання електронних документів в системі на основі ідентифікаційних даних;

3) автоматизувати процес формування та перевірки справжності електронного підпису;

4) здійснювати автоматичну перевірку актуальності сертифіката перевірки ключа електронного підпису, у такий спосіб значно скорочуючи часові витрати на оброблення запитів у СЕД;

5) підвищити захищеність даних в СЕД;

6) резервувати критично важливі функції СЕД завдяки застосуванню технології розподілених реєстрів (блокчейн);

7) підвищити ефективність роботи СЕД в умовах навмисних і ненавмисних зовнішніх впливів.

Отже, доходимо висновку, що запропонована концепція СЕД на основі технології розподілених реєстрів дозволить суттєво підвищити ефективність роботи СЕД у майбутньому завдяки автоматизації процесів реєстрації операцій з електронними документами і контролю доступу до них, а також формування та перевірки ЕП, що також дозволить скоротити часові витрати на опрацювання запитів і підвищити захищеність даних у системі.

Застосування технології розподілених реєстрів (блокчейн) уможливить побудову ефективної системи захисту інформації на етапі проєктування системи електронного документообігу військової частини завдяки аудиту та моніторингу даних у системі, де спільне використання технологій електронного підпису та смарт-контрактів забезпечить регламентацію умов доступу до всіх інформаційних об’єктів у системі, а облік усіх інформаційних взаємодій забезпечить замкнутість інформаційного середовища СЕД військового формування.

Висновки до розділу 2

У другому розділі проаналізовано діяльність військової частини та визначено особливості організації обігу документів обмежено доступу. Військова частина як структурний підрозділ Збройних Сил, який має власне організаційне і командне управління, чітко визначене місце дислокації та

завдання, що виконує конкретні функції щодо забезпечення обороноздатності держави. Вона включає особовий склад, техніку та озброєння, необхідні для виконання бойових і службових завдань.

З'ясовано, що організаційна структура бригади тактичної авіації включає такі основні компоненти: командування, штаб бригади, авіаційні ескадрильї, підрозділи забезпечення та батальйони.

Зазначено, що організація конфіденційного діловодства у військовій організації покладається на службу документного забезпечення управління, яка відповідальна за розроблення, упровадження та контроль за дотриманням процесів, що забезпечують належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів. Служба відповідає за методичне керівництво та контроль дотримання послідовності етап роботи з документами в усіх підрозділах військової частини.

Після проведено аналізу системи обігу документів обмеженого доступу виявлено проблеми, які пов'язані з: відсутністю оснащення сучасними уніфікованими засобами автоматизації, телекомунікації та зв'язку; недосконалістю засобів і механізмів управління доступом до інформаційних ресурсів; порушенням принципу одноразового введення інформації під час діяльності посадових осіб служби діловодства військової частини.

Для ефективної роботи служби діловодства військової частини запропоновано створення системи електронного документообігу, заснованої на локальній мережі з використанням хмарної технології Google Workspace та інтегрованого програмного забезпечення, що дозволяє ефективно застосовувати наявне телекомунікаційне обладнання. Для запобігання порушення захисту електронних документів у системі електронного документообігу рекомендовано також використати технологію розподілених реєстрів (блокчейн). Запропоновані методи удосконалення системи конфіденційного діловодства покращать ефективність створення та використання інформаційно-комунікаційних послуг для військової частини, а також підвищать ефективність роботи командування.

ВИСНОВКИ

Під час дослідження здійснено теоретичне узагальнення і запропоновано вирішення проблеми встановлення системи електронного документообігу для автоматизації основних процесів роботи з документами військової частини. У роботі також розроблено алгоритм захисту конфіденційної інформації військових формувань від несанкціонованого доступу, пошкодження чи знищення.

1. У роботі розкрито теоретичні основи конфіденційного діловодства та визначено особливості його автоматизації. З'ясовано, що конфіденційне діловодство забезпечує загальні процеси роботи з документами обмеженого доступу. Метою конфіденційного діловодства є забезпечення захисту інформації на всіх етапах її життєвого циклу від несанкціонованого доступу, пошкодження або знищення.

Визначено, що сучасні інформаційні технології відіграють важливу роль у забезпеченні захисту документних ресурсів як окремої установи, так і безпеки держави вцілому. Автоматизація діловодства включає різні фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту, що використовують для цифрового збирання, зберігання, передавання, оброблення та використання ділової інформації. Воно базується на використанні різних електронних пристроїв і спеціального програмного забезпечення, а також створює комплексний механізм захисту автоматизованих інформаційних систем.

2. З огляду на мету та завдання нашого дослідження, було визначено організаційну структуру і напрями діяльності військової частини. Встановлено, що військова частина є ключовим елементом військово-повітряних сил і виконує широкий спектр завдань, зокрема повітряні удари, підтримку наземних військ, розвідку, а також захист повітряного простору. До складу військової бригади входить: командування, штаб бригади, авіаційні ескадрильї, підрозділи забезпечення, батальйони.

З’ясовано, що робота з конфіденційними документами у авіаційній бригаді покладається на службу діловодства, яка відповідальна за розроблення, упровадження та контроль за дотриманням процесів, що забезпечують належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів. Основним завдання служби є забезпечення у військовій частині уніфікованого порядку документування управлінської інформації та роботи з документами, а також використанням сучасних інформаційних технологій для автоматизації основних процесів роботи з електронними даними.

У роботі проведено детальний аналіз документів, які є основним засобом для прийняття управлінських рішень і керування військового частиною. Визначено, що основними групами військових документів є: нормативно-правові акти, адміністративні, оперативно-службові, фінансово-економічні, кадрові та інформаційно-довідкові документи.

3. Надано практичні рекомендації для впровадження та захисту автоматизованої системи електронного документообігу військової частини.

Відповідно до проведеного аналізу ефективності обігу документів обмеженого доступу військової частини рекомендовано впровадити нові програмні засоби для автоматизації процесу оброблення документів, організувати навчання персоналу з використання цих систем та зміцнити систему аудиту та контролю для забезпечення максимального рівня безпеки конфіденційної інформації.

Для ефективної роботи служби діловодства військової частини запропоновано створення системи електронного документообігу, заснованої на локальній мережі з використанням хмарної технології Google Workspace та інтегрованого програмного забезпечення, що дозволяє ефективно застосовувати наявне телекомунікаційне обладнання.

У військовій частині рекомендовано також ввести в експлуатації комплексну систему захисту інформації системи електронного документообігу. Доречно створити спеціальну службу захисту інформації,

які буде адмініструвати усі процеси роботи з електронними документами в автоматизованій системі.

Для запобігання порушення захисту електронних документів у системі електронного документообігу рекомендовано використати технологію розподілених реєстрів (блокчейн), яка повністю автоматизує основні процеси роботи з електронними документами на базі військової частини.

Доведено, що застосування зазначених технологій підвищить ефективність функціонування всіх ланок управління, значно покращить діяльність командування військової частини, а також суттєво знизить фінансові витрати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.05.2024).

2. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.05.2024).

3. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 08.10.2023. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 01.05.2024).

4. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 01.05.2024).

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.2018 №246-IX. Дата оновлення: 04.04.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 10.05.2024).

6. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.05.2024).

7. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 25.04.2024).

8. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. Дата оновлення 31.03.2023. URL: https://zakon.rada.gov.ua /laws/show/2469-19#Text (дата звернення: 25.04.2024).

9. Про оборону України: Закон України від 06.06.1991 р. № 1932-XII. Дата оновлення 04.04.2024. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 25.04.2024).

10. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1994 р. № 8073-X. Дата оновлення 19.05.2024. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 25.05.2024).

11. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. Дата оновлення 19.05.2024. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 25.05.2024).

12. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби безпеки України від 23.12.2020 р. № 383. Дата оновлення: 16.04.2024. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text (дата звернення: 25.05.2024).

13. Про затвердження Порядку ведення обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, що містять службову інформацію: Постанова КМУ від 19.11.2016 р. № 736-2016-п. Дата оновлення: 25.08.2023. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text (дата звернення: 01.04.2024).

14. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 30.05.2024).

15. Блокчейн. *Вікіпедія. Вільна енциклопедія*: вебсайт. URL: https://uk.wikipedia.org/wiki/Блокчейн (дата звернення: 01.05.2024).

16. Бурячок В. Л., Невойт Я. В. Метод визначення найбільш значимих загроз із «генеральної сукупності» загроз інформаційним ресурсам на підставі їх якісних та кількісних показників. *Сучасний захист інформації*. 2014. № 3. С. 18–21.

17. Василюк В. Система захисту інформації приватного підприємства. Організація служби захисту приватного підприємства. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2007. Вип. 1 (14), С. 45–51.

18. Виноградський М. Д., Виноградська А. М., Шкапова О. М. Робота персоналу з державною таємницею. Організація праці менеджера: навч. посіб. Київ, 2010. С. 385– 409.

19. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. *Економіка та суспільство : електрон. наук. фах. вид.* 2017. Вип. 11. С. 497–502.

20. Войнаренко М. П., Кузьміна О. М., Янчук Т. В. Інформаційні системи і технології в управлінні організацією: навч. посіб. Вінниця : ПП «Едельвейс і К», 2015. 496 с.

21. Гордієнко С. Г. Конфіденційна інформація та «таємниці»: їх співвідношення. *Часопис Київського університету права*. 2013. № 4. С. 233–238.

22. Державна служба спеціального зв'язку та захисту інформації України. *Вікіпедія. Вільна енциклопедія*: вебсайт. URL: https://uk.wikipedia.org/wiki/Державна_служба_спеціального_зв%27язку_та_захисту_інформації_України (дата звернення: 01.05.2024).

23. Довжук І. В. Діловодство (загальне, спеціальне): навч.-метод. посіб. Переяслав (Київ. обл.): Домбровська Я. М., 2020. 353 с.

24. Загорецька О. Особливості роботи з документами, що містять комерційну таємницю підприємства. *Довідник кадровика*. 2019. № 9 (111). С. 40–46.

25. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання. *Центр демократії та верховенства права*: вебсайт. URL: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/ (дата звернення: 01.04.2024).

26. Котенко А. М. Запобігання витоку інформації з обмеженим доступом матеріально-речовим каналом за рахунок використання систем відеоспостереження. *Сучасний захист інформації*. 2017. № 1. С. 48–52.

27. Кудряєва Т. В., Кузнецової В. Я. Державна таємниця як складова забезпечення національної безпеки. *Право України*. 2017. № 21. С. 121–122.

28. Кузьмич І. І. Поняття та особливості військових документів. *Форум права.* 2013. № 2. С. 259–265.

29. Литвинська С. В., Сібрук А. В. Організація роботи з документною інформацією у військкоматах в умовах особливого періоду. *Інформація та соціум*. 2023. С. 82–84.

30. Мельник С., Фівкін П., Пащенко Є., Зіняк Л. Військове документування та діловодство: навч. посіб. Харків, 2023. 118 с.

31. Мірошник Ю. Державна таємниця як складова забезпечення національної безпеки. *Право України*. 2004. № 9. С. 32–34.

32. Новікова Д. О. Організація електронного документообігу при роботі з конфіденційною інформацією у військових частинах України. *Тези 76-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів університету* (Полтава, 14 травня – 23 травня 2024 р.). Полтава : Нац. ун-т ім. Юрія Кондратюка, 2024. Т. 2. С. 301–302.

33. Організація захисту інформації з обмеженим доступом: підруч. / А. М. Гуз, О. Д. Довгань, А. І. Марущак та ін.; за ред. Є. Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України , 2011. 376 с.

34. Полішко Г. П. Інформаційні технології удосконалення документаційного забезпечення для силового відомства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 2. С. 81–87.

35. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. Київ: Вид. Національної академії внутріш. справ, 2012. 104 с.

36. Сельченкова С. Службова та конфіденційна інформація у практиці підприємств. *Довідник секретаря та офіс-менеджера*. 2017. № 2. С. 6–8.

37. Скулиш Є., Гуз А. Організація захисту інформації з обмеженим доступом – перспективний напрям підготовки фахівців в Україні. *Вища школа.* 2012. № 9. С. 21–29.

38. Список нормативних документів щодо інформаційної безпеки в Україні. *Вікіпедія. Вільна енциклопедія*: вебсайт. URL: https://uk.wikipedia.org/wiki/Список_нормативних_документів_щодо_інформаційної_безпеки_в_Україні (дата звернення: 01.05.2024).

39. Фастовець В., Сирцов В. Проблеми організаційно-правового забезпечення електронного обігу обмеженої інформації та інформатизації процесів документообігу. *Наукові праці Інституту законодавства Верховної Ради України.* 2020. № 4. С. 88–95.

40. Цілина М. М. Сучасні технології захисту й опрацювання конфіденційної документної інформації в організаціях і установах різних форм власності. *Бібліотекознавство. Документознавство. Інформологія*. 2021. № 4. С. 15–23.

41. Юрчак В. Ю. Перспективи правового забезпечення безпеки інформації державної таємниці. Київ, 2019. 473 с.

42. Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації. *Південноукраїнський правничий часопис*. 2021. № 1. С. 94–98.

43. *Document management software and workflow automation*: вебсайт. URL: https://start.docuware.com/ (дата звернення: 01.05.2024).

44. *Google Workspace*: вебсайт. URL: https://workspace.google.com/intl/uk/ (дата звернення: 01.05.2024).

45. *OpenText*: вебсайт. URL: https://www.opentext.com/ (дата звернення: 01.05.2024).

46. SharePoint. *Microsoft*: вебсайт. URL: https://www.microsoft.com/uk-ua/microsoft-365/sharepoint/collaboration (дата звернення: 01.05.2024).