МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЛИПОВА СВЯТОСЛАВА ВАСИЛІВНА

Допускається до захисту:
завідувач кафедри інформаційних систем управління
д-р екон. наук, професор
_____ О.М. Анісімова
«____»__._____ 20___ р.

ОСОБЛИВОСТІ РОБОТИ З ДОКУМЕНТАМИ, ЩО МІСТЯТЬ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ, В СИСТЕМІ ОБОРОНИ УКРАЇНИ

Спеціальність 029 Інформаційна, бібліотечна та архівна справа

Кваліфікаційна (бакалаврська) робота

Керівник:
Ковальська Л.А., професор кафедри
інформаційних систем управління
д-р істор. наук, доцент

Оцінка: ____ / ___ / _____
(бали / за шкалою ЄКТS / за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця – 2021

АНОТАЦІЯ

Липова С.В. Особливості роботи з документами, що містять конфіденційну інформацію, в системі оборони України. Спеціальність 029 «Інформаційна, бібліотечна та архівна справа» Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У роботі розкрито основні засади організації документообігу в системі оборони України, основу якого визначають нормативно-правові документи та загальні вимоги його організації. Висвітлено результати та наступні кроки впровадження електронного документообігу. Проаналізовано особливості створення документів та налагодження інформаційної комунікації в системі оборони України. Акцентовано увагу на роботу з документами, що містять конфіденційну інформацію в системі оборони України. Опрацьовано вимоги до впровадження інформаційних технологій в роботі з документами з особливим доступом та забезпечення системами захисту даних.

Ключові слова: інформаційна безпека, конфіденційна інформація, Збройні сили України, документообіг, система оборони України.

Табл. 8. Рис. 14. Бібліограф.:45 найменувань

Lypova S. Features of working with the documents containing confidential information in the defense system of Ukraine. Specialty 029 «Information, Library and Archival Affairs». Vasyl Stus Donetsk National University, Vinnytsia, 2021.

The paper reveals the basic principles of document management in the defense system of Ukraine, the basis of which is determined by regulatory documents and general requirements of its organization. The results and next steps in the implementation of electronic document management are highlighted. Peculiarities of creating documents and establishing information communication in the defense system of Ukraine are analyzed. Emphasis is placed on working with documents that contain confidential information in the defense system of Ukraine. Requirements for the introduction of information technology in working with documents with special access and providing data protection systems have been developed.

Key words: information security, confidential information, Armed Forces of Ukraine, document circulation, defense system of Ukraine.

Table. 8. Fig. 14. Bibliographer.: 45 items.

ЗМІСТ

ВСТУП

Актуальність дослідження. Стрімкий розвиток інформаційно-комунікаційних технологій актуалізує питання їх ефективного впровадження у роботу всіх галузей і сфер життя. Документообіг сьогодні в епоху розвитку інформаційних технологій замінюють електронними системами. Організації різних форм власності спілкуються шляхом обміну електронними документами, який економить час і полегшує роботу працівників. Свою специфіку в цей процес вносить робота з документами з обмеженим доступом до інформації та необхідність її захисту.

У Міністерстві оборони України та всіх підпорядкованих йому підрозділах уже тривалий час використовується система обміну даними, але це одна з декількох систем, які інтегруються в життя української армії. Використання таких систем обміну даними є вкрай необхідним для подальшого існування у цифровому світі. Адже швидкість прийняття правильного рішення є запорукою успіху виконання поставлених бойових завдань та збереження життя військовослужбовців. Структури системи оборони усвідомлюють необхідність впровадження подібних систем у повсякденну діяльність, зокрема щодо управління різними підрозділами, віддання наказів на всіх рівнях – від тактичного до стратегічного.

Використання новітніх технологій, спрямованих на збільшення ефективності роботи, водночас породжує нові ризики, які можуть призводити до розкриття службової або чутливої інформації. І якщо ця інформація є власністю держави та належить до певних силових структур, то наслідки можуть бути катастрофічними. Саме цей аспект роботи з документами, що містять конфіденційну інформацію і став предметом наукового кваліфікаційного дослідження.

Мета кваліфікаційної роботи – простежити специфіку роботи з документами, що містять конфіденційну інформацію, в системі оборони України та можливості використання інформаційно-комунікаційних технологій.

Для досягнення мети дослідження передбачено послідовне виконання таких **завдань**:

- проаналізувати засади документообігу в системі оборони України;

- вивчити загальну характеристику документообігу інформаційного середовища;

- з'ясувати специфіку роботи з документами що містять конференційну інформацію в системі оборони України;

- здійснити аналіз стану роботи з документами, що містять конфекційну інформацію в закладах оборони України;

- розглянути впровадження інформаційних технологій у роботі з документами в системі оборони України;

Об'єктом роботи є організація документообігу та вимоги роботи з документами, що містять конфіденційну інформацію, в системі оборони України.

Предметом роботи є особливості функціонування документів, що містять конфіденційну інформацію, та можливість впровадження інформаційно-комунікаційних технологій в системі оборони України.

Апробація результатів дослідження. Наукові положення, викладені у бакалаврській роботі відображені частково у науковій статті Віснику студентського наукового товариства Донецького національного університету імені Василя Стуса (м. Вінниця, 2019); апробовані на конференціях та опубліковані у збірниках матеріалів IV, V, та VI Всеукраїнської наукової студентської конференції «Інформаційні технології і системи в документознавчій сфері» (м. Вінниця, 2019, 2020, 2021).

Структура кваліфікаційної бакалаврської роботи: вступ, три розділи і шість підрозділів, висновки, список використаних посилань (45 найменувань), додатки. Робота викладена на 54 сторінках друкованого тексту, основна частина якої становить 45 сторінок. Розділ Додатки містить п'ять ілюстрацій. У роботі наведену інформацію проілюстровано у вигляді 8 таблиць та 14 рисунків.

РОЗДІЛ 1
ОРГАНІЗАЦІЯ ДОКУМЕНТООБІГУ В СИСТЕМІ ОБОРОНИ УКРАЇНИ

1.1. Загальна характеристика та вимоги до організації документообігу з особливим доступом

Сьогодні робота зі службовими документами забезпечують зберігання необхідної документної інформації, її швидкий пошук, оперативність переміщення й виконання, а також забезпечення умов для всіх видів робіт з документами з моменту складання чи отримання до знищення або ж передавання в архів – становить єдиний технологічний цикл і є важливим організаційним чинником управлінської діяльності.

Документообіг це рух документів в установі від моменту створення або від одержання зі сторони до моменту передачі на зберігання до архіву «інформаційна безпека» системі оборони України [26, с.157].

Інформаційна безпека підприємства полягає у формуванні принципів, методів та заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію [17, с.158].

Увесь спектр інтересів інформаційної безпеки можна поділити на такі основні категорії, як:

1) доступність – можливість за визначений час отримати певну інформаційну послугу;

2) цілісність – релевантність та несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання;

3) конфіденційність – захищеність від несанкціонованого доступу.

Сьогодні система заходів дає змогу виявляти вразливі місця інформаційно-комунікативної системи підприємства та небезпеки які загрожують їй, і методи нейтралізації виявлених загроз [41, с.55]. Загрозою визнається подія, яка може викликати порушення функціонування інформаційної системи, включаючи

спотворення, знищення або несанкціоноване використання бази даних. Можливість реалізації загроз залежить від наявності вразливих місць в інформаційній системі. Склад і специфіка вразливих місць визначається типом вирішуваних завдань, характером інформації, апаратно-програмними особливостями обробки інформації на підприємстві, наявністю засобів захисту та їхніми характеристиками [48, с.139]. Порядок ведення електронного документообігу на підприємстві передбачено внутрішніми положеннями, розробленими на основі Закону України «Про електронні документи та електронний документообіг» [24, с.126] (табл. 1.1).

Таблиця 1.1. – Характеристика параметрів документопотоку

№	Назва параметру документопотоку	Характеристика параметру документопотоку
1.	Зміст або функціональна приналежність	Характеризується складом документів та інформації, що входять в документопотік та описується ознаками, за якими документи класифікуються, індексуються та опрацьовуються.
2.	Структура	Характеризується різними потоками документів, відповідно до певного функціонального призначення документів, що входять у документопотік.
3.	Режим або циклічність	Характеризується змінами часу та змінами інформаційного змісту. що відбуваються за рахунок зовнішнього та внутрішнього впливу на діяльність організації (наприклад, сезонні зменшення політичної, управлінської, ділової активності, та зменшення внутрішніх ритмів в роботі організації та ін.)
4.	Спрямованість або напрям	Характеризується залежністю від технологічної ланки опрацювання документів: (документи, які підлягають реєстрації та документи, що не реєструються; документи з контролем виконання та без контролю та ін.). На напрям документопотоку впливає спосіб оцінки і засвідчення документів: погодження, затвердження, ознайомлення та ін.
5.	Обсяг або об’єм	Характеризується кількістю документів чи обсягом інформації, що міститься в документах (наприклад, кількість аркушів, кількість знаків, кількість доручень, кількість виконавців та ін.)

Тобто, важливим параметром документопотоку, що впливає на структуру організації діловодства на підприємстві і її штатний розклад є об'єм. Це кількість документів, що надходять в організацію і створюється у ній за певний проміжок часу [19, с.104]. Розглянемо структуру алгоритму впровадження електронного документообігу на підприємстві на рисунку 1.1.

Рисунок 1.1. – Структура алгоритм впровадження електронного документообігу на підприємстві [36].

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Для взаємодії з контролюючими органами є можливість скористатися електронним кабінетом платника (ЕКП), який відкриває нові можливості у цьому напрямку, а саме: через ЕКП платник зможе ставати на облік та зніматися з нього, вносити зміни в облікові відомості про себе, переходити на іншу систему оподаткування [30, с. 204].

Створення документообігу різнорідних потоків у єдиному просторі дає змогу відображати зв'язки між різними типами документів: технічними, адміністративними, нормативними, фінансовими та ін. Кожен документ відповідно до свого потоку рухається в межах свого маршруту, розробляється і контролюється різними користувачами відповідно певного напряму [18, с.319].

Сьогодні автоматизація системи управління про кар'єру військовослужбовця, повинно бути стандартом. Розглянемо характеристику електронного документу у таблиці 1.2 [27, с.134].

Таблиця 1.2. – Характеристикам електронного документу

№	Електронний документ
1.	Оформлення в електронному вигляді, за необхідності в паперовому вигляд
2.	Обробка даних за допомогою інформаційних систем і фіксація в електронних регістрах бухгалтерського облік
3.	Здійснюється через телекомунікаційні та інформаційні системи або через електронні носії інформації
4.	Зберігаються згідно зі строками, установленими законодавством, на спеціальних електронних носіях
5.	Згідно з інструкцією, знищення відбувається спеціально призначеною особою, яка також відповідальна за програмне забезпечення, що перевіряє факт знищення документів

Електронний документ являється документом, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [31, с.98].

Основним з етапів впровадження електронного документообігу є отримання електронного цифрового підпису. Цей етап не в повній мірі залежить від підприємства, так як є обов'язковим в обігу для користувачів електронного документа [1].

Також класифікація загроз інформаційній безпеці може бути здійснена поділом загроз на пов'язані із внутрішніми і зовнішніми факторами.

Окремо варто виділити загрози, пов'язані з навмисними помилками, що виникають за межами бізнесу. До таких загроз відносять [17, с. 153]:

– несанкціонований доступ до інформації, що зберігається в системі;

– розроблення і поширення комп'ютерних вірусів;

– недбалість у розробленні, підтримці та експлуатації програмного забезпечення, що приводить до краху комп'ютерної системи.

На жаль, доводиться констатувати, що уніфікований підхід до класифікації загроз інформаційній безпеці відсутній.

Зберігання документа, переведеного у електронну форму, має свої переваги та недоліки у таблиці 1.3.

Таблиця 1.3. – Переваги та недоліки способів зберігання інформації

Спосіб	Переваги	Недоліки
Тільки текст	Потребує незначної кількості дискового простору Доступний повнотекстовий пошук документа Можливе повторне використання тексту при підготовці документів у відповідь	Рукописні документи не скануються Можливе не зовсім точне відтворення зовнішнього виду документа Необхідний час на верифікацію документа
Тільки образ	Можна сканувати рукописи і документи поганої якості Економія часу на верифікації	Повнотекстовий пошук неможливий Обсяг збережуваної інформації більший, ніж при зберіганні тексту
Текст + образ	Доступний повнотекстовий пошук Можливе повторне використання тексту Можна сканувати всі документи	Підвищені вимоги до апаратного забезпечення для зберігання великих обсягів інформації

Робочий процес поділяється на завдання – окремі неподільні етапи виконання роботи. Співробітники виконують завдання згідно своїх посадових

інструкцій, у певній послідовності. Виконання завдання супроводжується потоком інформації: фіксуються параметри виконання завдання (як мінімум, факт його виконання для сигналу до початку наступного завдання.

Розглянемо структуру документів та їх види на рисунку 1.2. [16, с.134].

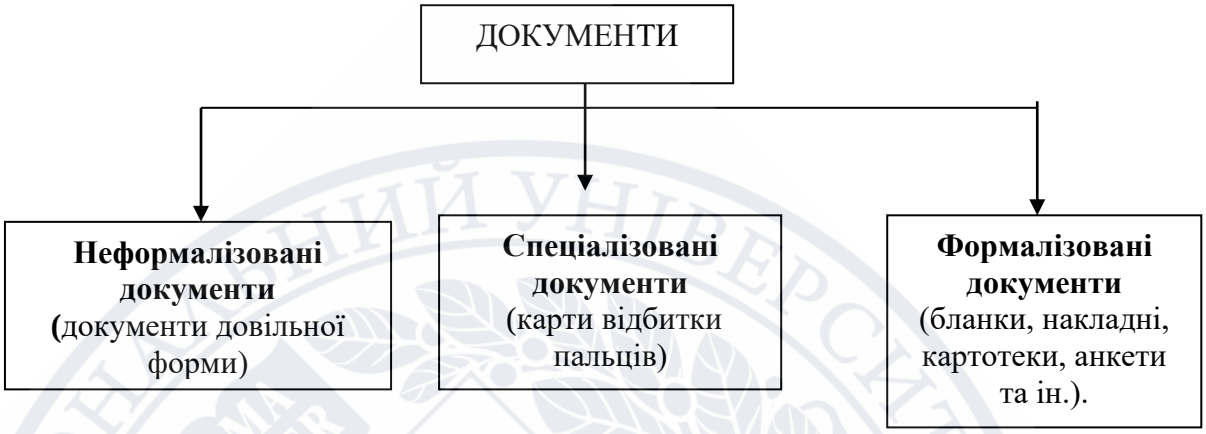


Рисунок 1.2. – Структура документів та їх види

Впровадження системи електронного документообігу сьогодні є ключовим фактором вдалого і успішного ведення діловодства [9, с.134]. Одним із найважливіших видів діяльності із забезпечення інформаційної безпеки підприємства є виявлення, оцінка та запобігання загрозам інформаційно-комунікативним системам і інформаційним ресурсам. Інформаційне забезпечення діяльності підприємства слід розглядати не лише в загальному вигляді, охоплюючи всі функції управління, а й окремими функціональними управлінськими процесами [20, с.142]:

Отже, створення інформаційного забезпечення на підприємстві полягає у підвищенні ефективності управління підприємством. Інформаційні ресурси розглядаються як упорядкована сукупність документованих даних і знань, відомостей, інформації, що призначені для задоволення інформаційних потреб користувачів та можуть бути використані для прийняття рішення.

1.2. Електронний документообіг у системі оборони України

Електронний документообіг – це життєвий цикл електронних документів в організації, починаючи від їх отримання, проходження в підрозділах зі зміною стану і закінчуючи списанням в архів.

Ефективність керування підприємством, установою певною мірою залежить від того, наскільки розумно в ньому організований документообіг. Адже, документообіг та управлінська діяльність тісно пов’язані одне з одним. Від того, наскільки оперативно здійснюється рух, опрацювання документів та їх передавання на виконання, залежить швидкість отримання інформації, необхідної для прийняття управлінського рішення.

Під документообігом розуміють рух документів від моменту складання їх на конкретному підприємстві або одержання від інших підприємств до здачі в архів після опрацювання та систематизації [41, с. 124].

Згідно ДСТУ 2732:2004 «Діловодство та архівна справа. Терміни та визначення понять» документообіг – це рух службових документів в установі від дати їхнього створення чи одержання до дати завершення виконання або надсилання [13, с. 128].

Цей термін обґрунтовує систематизацію руху документів в середині установи, а також узагальнює їх шлях як невід’ємну складову робочого процесу. Процеси документообігу розглядаються, перш за все, як документальне відображення і забезпечення управлінських дій, як система вторинних процесів, які забезпечують і відображають всі операції управління.

За умов комп’ютеризації управління і з переходом до зберігання інформації на електронних носіях документообіг (документальне забезпечення управління) розуміють як створення інформаційної бази документів на різноманітних носіях для використання управлінським апаратом у процесі реалізації його функцій [17, с. 29].

Електронний документообіг здійснюється відповідно до законодавства України або на підставі договорів. Відповідно до ст. 9 Закону України «Про

електронні документи та електронний документообіг», електронний документообіг − сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення ЕД, які виконуються із застосуванням перевірки цілісності та в разі необхідності з підтвердженням факту одержання таких документів [16, с.105]. Ознайомимося із структурою електронного документообігу на рисунку 1.3.

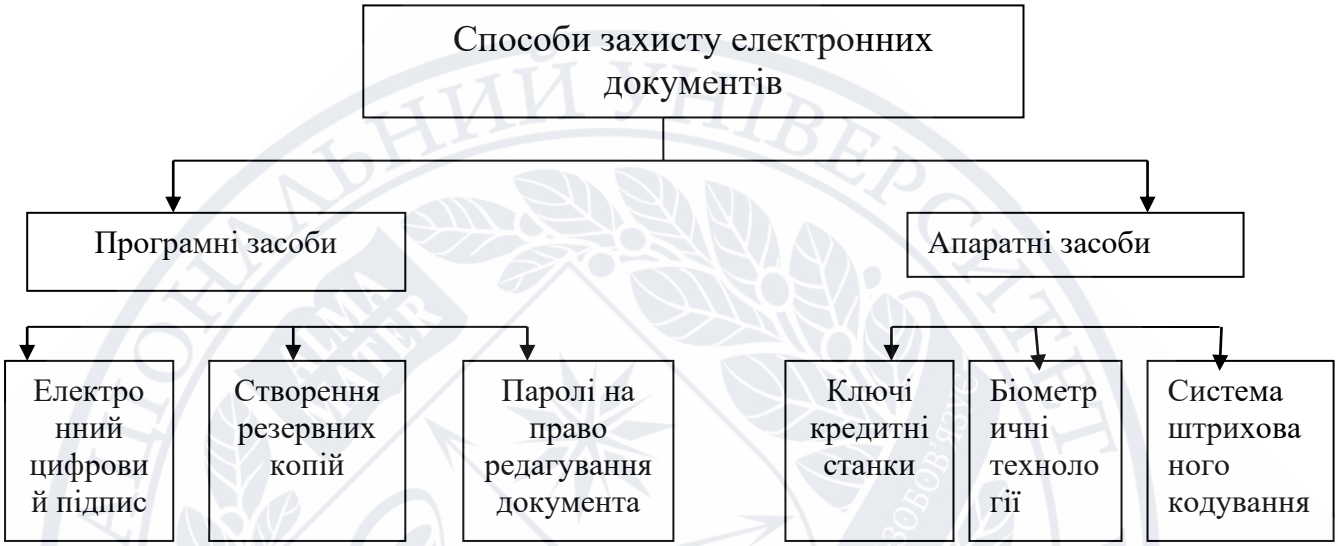


Рисунок 1.3. – Способи захисту електронного документообігу [16, с. 90].

Електронний документообіг дозволяє створити єдиний інформаційний простір, інтегруючи в інформаційний вузол усі документальні системи. Інтеграція здійснюється без втрати якості роботи з документами, зі збереженням традицій діловодства.

Основа подібної інтеграції – надійне сховище документів і взаємодіючі з ним системи документообігу [37, с. 162]. Всі документи зберігаються в єдиному сховищі, що дозволяє забезпечити оптимальний пошук і відбір інформації при підготовці матеріалів. Однак робота з архівними документами є важливим етапом при підготовці нових матеріалів. Інтеграція архіву ЕД у єдиний інформаційний простір організації дозволить зробити доступ до архівних матеріалів оперативним і ефективним. Доступ до світових інформаційних ресурсів, перехід на електронні технології документування, зберігання і передання документів, тобто перехід на принципово нові способи організації

інформації і доступу до неї, ставлять перед службою діловодства нові наукові і прикладні завдання [12, с. 90].

Електронний документообіг – це високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи фірми, установ і організацій» [11, с. 182].

Інше визначення електронного документообігу пропонує Матвієнко О. – «це процес створення, одержання, спільного використання, ревізії, розподілу та зберігання документів та інформації, яку вони містять у межах певної інформаційної системи» [23, с. 158].

Тлумачення електронного документообігу пропонує Крутова А. − «це процес створення, одержання, оброблення, зберігання, сумісного використання, відправлення, передавання й знищення ЕД та інформації, яка в них міститься в рамках певної інформаційної системи» [19, с. 115].

В свою чергу, Перехрест Г. визначає електронний документообіг як високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи фірми, установи і організації [36, с. 201].

Головне завдання електронного документообігу полягає в підвищенні ефективності та якості роботи підприємства за рахунок впровадження системи прозорості руху документів і контролю за їх виконанням. Електронний документообіг насамперед пов`язаний з будовою єдиного інформаційного середовища підприємства [15, с. 184].

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством. Одиницею електронного документообігу є електронний документ – «документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа» [21, с.127].

ЕД може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Згідно зі ст. 5 Закону України «Про

електронні документи й електронний документообіг», візуальною формою подання електронного документа є відображення даних [1].

Статус ЕД визначається його реквізитом, що набирає таких значень:

1) версія – примірник ЕД та стадії створення, який відрізняється від інших його примірників порціями вмісту;

2) оригінал – примірник ЕД, яким першим набуває чинності, що зазначається в процесі реєстрації відповідним значенням спеціального реквізиту;

3) дублікат – примірник ЕД, який має юридичну силу оригіналу;

4) копія – примірник ЕД, який точно відтворює вміст його оригіналу, а також усі його реквізити чи їх частину [13, с. 209].

ЕД – інформація, що зафіксована на електронних носіях, яка містить реквізити, що дозволяють її ідентифікувати.

Впровадження систем електронного документообігу представлено на рисунку 1.4.

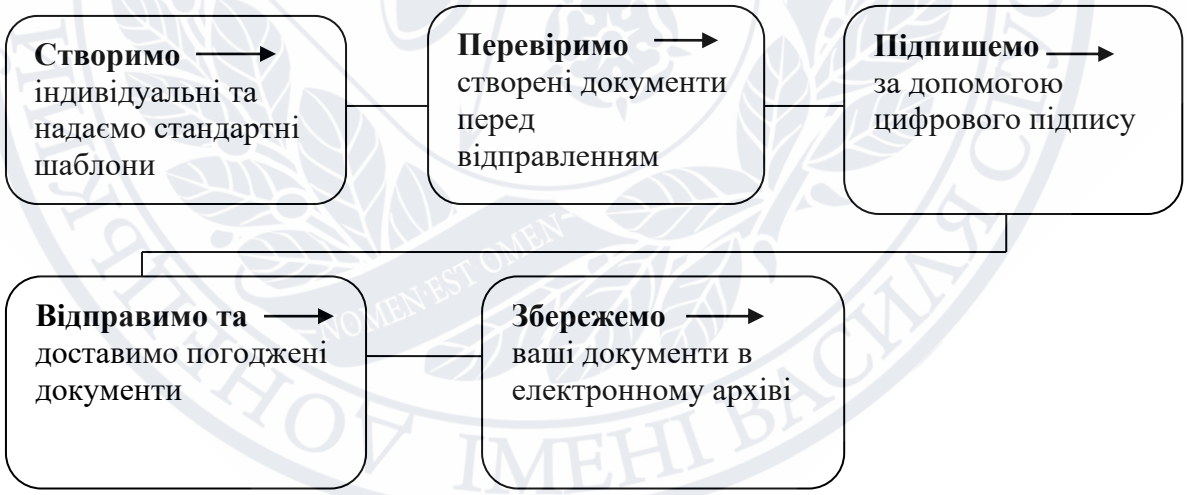


Рисунок.1.4. – Реалізація системи електронного документообігу [51]

В основі електронного документообігу лежить обмін даними автоматизованих систем із застосуванням електронного цифрового підпису яким буде засвідчуватися електронна накладна [13, с. 26].

Головне завдання системи електронних документів є організування раціонального руху, опрацювання та збереження електронних документів, організування їх пошуку як по атрибутах, так і за змістом.

Для регулювання правовідносин у сфері інформаційних технологій Верховною Радою України ухвалено кілька Законів України, які набули чинності, а саме: Про електронні документи та електронний документообіг [5], Про обов'язковий примірник документів; Про Національну програму інформатизації [4], Про телекомунікації [3].

Сьогодні ЕЦП має вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувала. ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Особистий ключ – параметр криптографічного алгоритму формування ЕЦП, доступний тільки підписувачу. Відкритий ключ являється параметр криптографічного алгоритму перевірки ЕЦП, доступний суб'єктам відносин у сфері використання ЕЦП [52].

Постійне збільшення кількості інформації, необхідної для прийняття адекватних управлінських рішень, призводить до того, що традиційні методи роботи з документами стають все більше нерентабельними [11, с. 235].

Так, за статистичними даними *15 % паперових документів губляться, а для їх пошуку працівники витрачають близько 30 % свого часу*.

Традиційні методи, які відрізняються високим ступенем емпіризму, в сучасному документаційному забезпеченні управління себе вже не виправдовують. У зв'язку з цим стала нагальною потреба автоматизації існуючих систем документообміну та переходу на електронний документообмін - високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи з документами [18, с. 125].

Кількість документів з паперовими носіями в середньому за рік збільшується на 7 %, а з електронними - вдвічі. Види систем електронного документообігу показано на рисунку 1.5.

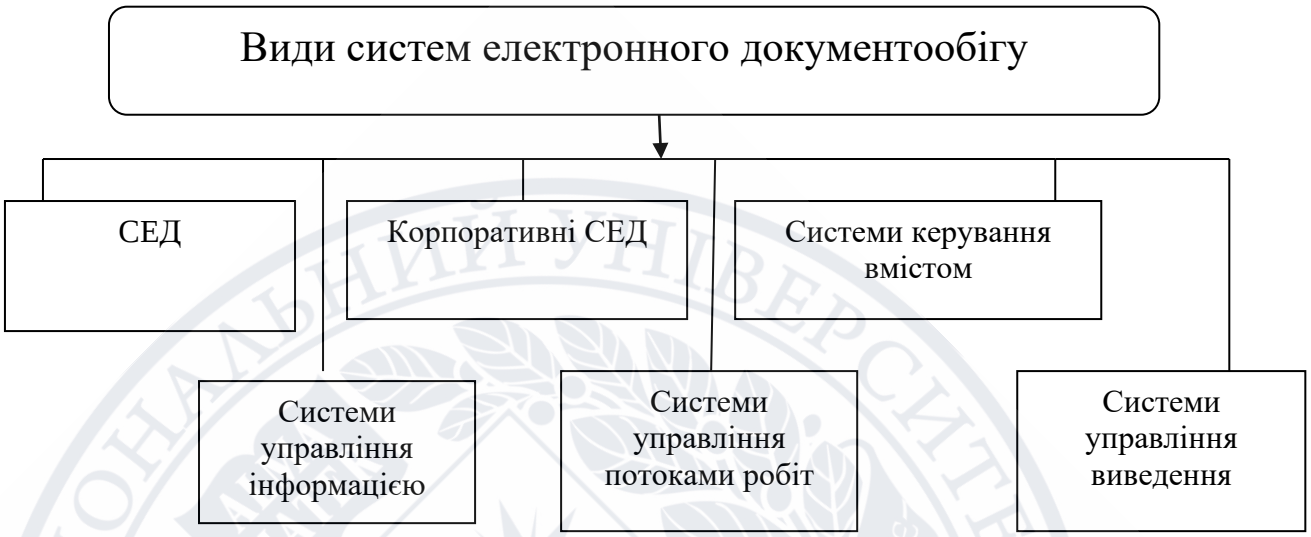


Рисунок.1.5. – Види систем електронного документообігу [37, с. 160].

Залежно від цілей і завдань, розрізняють внутрішній і зовнішній документообіг. Електронний документообіг всередині організації дозволяє обмінюватися документами тільки в межах структурних підрозділів компанії. Зовнішній документообіг – це обмін вхідною та вихідною документацією з контрагентами (клієнтами, контролюючими органами).

Функції системи електродного документообігу [40, с. 117]:

1. Централізоване управління документами - СЕД
2. Підтримка життєвого циклу документів - СЕД
3. Колективна робота над документами - СЕД.

Система електронного документообігу являється програмне забезпечення, головними завданнями якого є організація і підтримка життєвого циклу електронних документів. Розглянемо переваги та функції систем електронного документообігу у таблиці 1.3 [48, с. 100].

Таблиця 1.3. – Переваги та функції систем електронного документообігу.

Прозорість всіх етапів діяльності компанії	*Скорочення часу на операції з документами*	*Зручність роботи з електронними документами*	*Підвищення відповідальності працівників підприємства*	*Поліпшення якості обслуговування клієнтів*
Кожен документ, завдання або процес фіксуються в системі електронного документо-обігу, супроводжуються обліково-реєстраційною інформацією, яка спрощує контроль термінів виконання, моніторинг, аналітику, планування	Керівник і співробітники підприємства набагато швидше справляються з такими повсякденними діями над документами, як створення, пошук, узгодження, затвердження, відправка, перевірка та ін.	У СЕД передбачені - розмежування прав доступу, автоматичне завантаження з каталогу, повний цикл договірного обліку, сканування, розпізнавання для повнотекстового пошуку, використання шаблонів, редагування і контроль версій	Завдяки системі повідомлень у системі, співробітники просто не зможуть забути про будь-яке завдання, а облік робочого часу і трудовитрат дозволить керівному складу ефективніше планувати розподіл завдань між працівниками	Рух електронних документо-потоків відбувається значно швидше і чіткіше, ніж в оффлайн режимі, а значить звільняє час для більш уважного ставлення до кожного клієнта і прояви індивідуального підходу

Система електронного документообігу (СЕД) автоматизована багато користувальницька система (комп'ютерна програма), впроваджена на підприємстві, що дозволяє організувати спільну роботу співробітників з різними електронними документами [32, с. 108]. З урахуванням переваг технологій необхідно застосовувати все в електронному урядуванні [37, с.108].

Отже, для запровадження електронного документообігу (ЕД) перед органами влади, передусім, постало завдання зі створення нормативно-правової бази, що забезпечує його здійснення шляхом належної організації відповідних процесів та дотримання вимог до оформлення документів.

РОЗДІЛ 2
СТВОРЕННЯ ТА РУХ ДОКУМЕТІВ, ЩО МІСТЯТЬ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ

2.1 Основні вимоги до роботи з документами, що містять таємну конфіденційну інформацію

В сучасному суспільстві інформаційна влада поряд з політичною, економічною та військовою владою має значне, а й інколи визначальне значення в системі владних відносин. За таких умов, основна стурбованість у сфері забезпечення національної інформаційної безпеки пов'язана з можливістю застосування інформаційно-комунікативних технологій в цілях, несумісних із завданнями забезпечення стабільності і безпеки [36, с. 239].

В одному з попередніх номерів розглянуто види службової інформації, яка потенційно може містити комерційну таємницю, методи захисту комерційної таємниці, а також відмітні риси, сутність і завдання конфіденційного діловодства.

Дослідник Янчук Ю.Б. стверджував, що конфіденційна інформація – це відомості, в тому числі і комерційна таємниця, які знаходяться у володінні, користуванні, або розпорядженні підприємства, організації чи установчий зберігаються та поширюються у порядку встановленому положенням цього підприємства [22, с.137].

Комерційна таємниця належить до різновидів конфіденційної інформації, що не є власністю держави. У частині 1 статті 36 Господарського Кодексу України поняття «комерційна таємниця» визначається як відомості, що недержавною таємницею, пов'язані з виробництвом, технологією цього підприємства.

Облік документів, що містять комерційну таємницю, охоплює:

- присвоєння та про ставлення в облікових формах і на документах реєстраційних номерів;

- запис облікових і пошукових даних (дати, автора, заголовка, кількості сторінок, відомостей про місцезнаходження тощо) про документи [33, с.174].

Обліку підлягають усі без винятку виготовлені на підприємстві документи з грифом обмеженого доступу. Їх обліковують за кількістю сторінок, а друковані видання (книги, журнали, брошури) — за кількістю примірників. Документи, що містять комерційну таємницю, реєструють один раз. Облік ведеться у журналі обліку конфіденційних документів та видань, або на картках, зазвичай окремо від обліку документів загального діловодства.

Різновиди документів, що містять конфіденційну інформацію представлено на рисунку 2.1.

Рисунок 2.1. – Види документів, що містять конфіденційну інформацію [10, с. 174].

Розбудова системи інформаційної безпеки включає в себе політико-правове конструювання вказаної системи та інституційне забезпечення політики інформаційної безпеки.

Схоже визначення дає Закон «Про інформацію» у статті 21, а саме: «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних

повноважень. Розглянемо структуру інформаційного обмеження із доступом на рисунку 2.2 [20, с. 178].

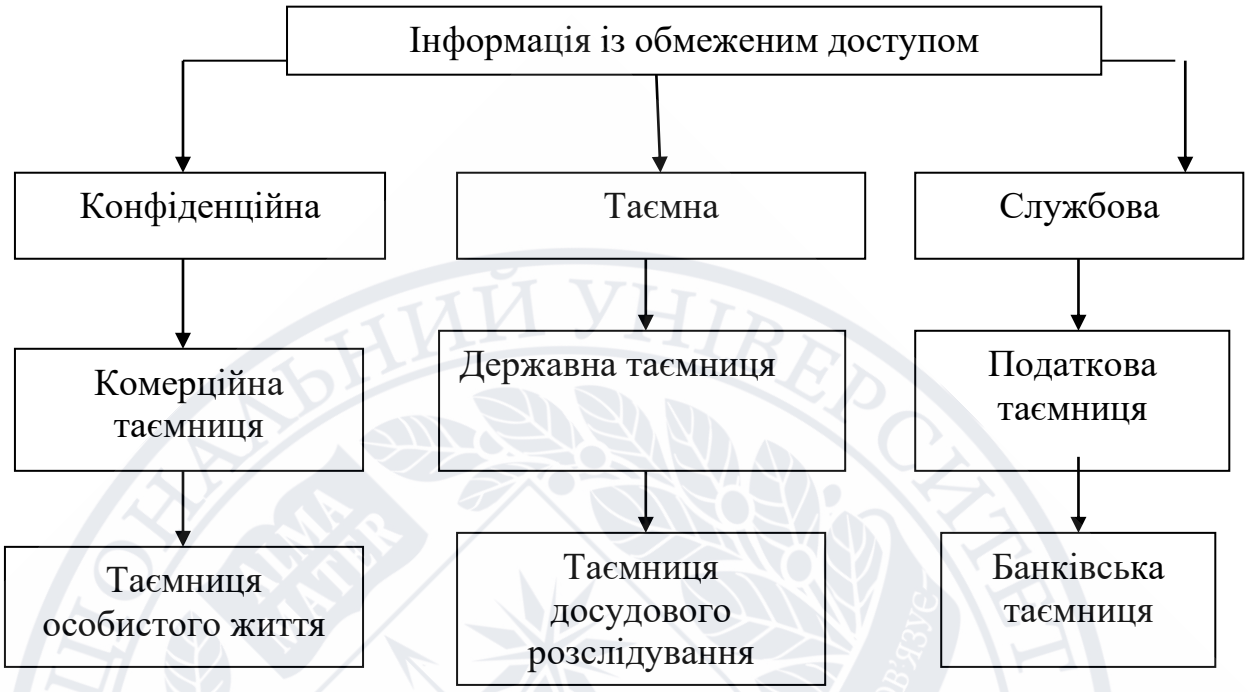


Рисунок 2.2. – Структуру інформаційного обмеження із доступом

За роки незалежності в Україні створено практично нову галузь законодавства – інформаційного. Його основою є право кожного, закріплене у статті 34 Конституції України, на свободу думки і слова, вільне вираження своїх поглядів і переконань [26, с.173].

Класифікатором галузей законодавства України, затвердженим наказом Міністерства юстиції України № 43/5 від 2 червня 2004 року, виділяється галузь законодавства, що регулює суспільні відносини, пов'язані із зв'язком, інформацією та інформатизацією. Так, суспільні відносини в інформаційній сфері регулюються рядом законів, які становлять відповідну систему, що складається з Конституції України, Законів України Про Основні засади розвитку інформаційного суспільства в Україні Про інформацію [3], Про науково-технічну інформацію [5], Про державну таємницю [4].

Сьогодні не можна недооцінювати роль держави як головного гаранта конституційного права на інформацію. Зазначене гарантування права на інформацію можливе лише в умовах демократичної правової держави, оскільки

право на інформацію історично виникає з розвитком демократії, яке відроджене нею і може реально існувати та розвиватися тільки в демократичному суспільстві [36, с.194].

Повертаючи документ, що містить комерційну таємницю, працівник служби діловодства (секретар) зобов'язаний:

1) звірити номер документа з відповідним номером у журналі реєстрації;

2) перевірити кількість аркушів цього документа;

3) розписатися у відповідній графі журналу за повернутий документ і проставити дату повернення у присутності працівника, який щойно повернув цей документ.

Про доступ до публічної інформації, Про інформацію, Про захист персональних даних у справі захисті інформації та обмеженого доступу до інформації. Розглянемо порівняння змісту статей Законів України у таблиці 2.1.

Таблиця 2.1. – Порівняння змісту статей Законів України

Стаття 7 Закону Про доступ до публічної інформації	Стаття 11 і 21 Закону Про інформацію	Стаття 2 закону Про захист персональних даних
Конфіденційна інформація - інформація доступу до якої обмежно фізичною або юридичною особою, крім суб'єктів вкладних повноважень, відповідно до передбачених ними умов.	*Інформація про фізичну особу* (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована. До конфіденційної інформації про фізичну особу належать зокрема дані про освіту, сімейний стан та інше.	*Персональні дані* - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована, або може бути конкретно ідентифікована

Найважливішими загрозами тут є вороже використання інформаційно-комунікативних технологій на рівні держав проти інформаційних інфраструктур в політичних та військових цілях, злочинна і терористична діяльність в кіберпросторі.

Зокрема, сьогодні інформаційно-психологічний вплив на масову відомість населення країн розглядається як один із ключових елементів національної могутності держави.

Політико-правове конструювання системи інформаційної безпеки та системи її забезпечення в передбачає використання:

1) теорії інформаційного суспільства, що розглядає засоби інформації як єдиний стимул і джерело соціального розвитку;

2) теорії соціального насильства, яка розглядає форми насильства: легітимну, парціально-легітимну, псевдолегітимну, нелігітимну, а також зброю соціального насильства;

3) теорії інформаційної війни, яка розглядає адаптивні механізми і архетипи інформаційної війни;

4) теорій міжнародної та національної безпеки – парадигм захищеності та самореалізації, синергетичного і діяльнісного підходів до розуміння безпеки;

5) теорії глобалістики, що відкриває реальну можливість створення нової, ненасильницької ідеології і нові можливості реагування на ймовірні виклики та загрози міжнародній та національній безпеці;

6) теорії державного управління, що розглядає місію, функції та завдання системи забезпечення національної безпеки;

7) інституціоналізму, у якому акцентується увага на питаннях взаємодії держави та громадянського суспільства в процесі розроблення політики національної безпеки та інформаційної політики [23, с.104].

Суть останнього полягає в розгляді інформаційних процесів як результату дії соціальних інститутів, коли правові інститути займають найважливіше місце в регулюванні інформаційних відносин в сучасному суспільстві [17, с. 58].

Система забезпечення національної безпеки (найпростішого) механістичного типу може бути ефективної лише за умов чіткого визначення об’єкта, суб’єкта, їх завдань, функцій, місії, методів і механізмів управління [15, с. 170].

Зазначимо, що в сучасних умовах інформаційно-психологічного протиборства вказані обов'язкові вимоги ефективного функціонування системи забезпечення інформаційної безпеки механістичного типу виконати досить проблематично [26, с.185].

Система забезпечення інформаційної безпеки адаптивного типу має негативний зворотній зв'язок, змінює насамперед свої внутрішні параметри / структуру й здатна пристосовуватися до змін, що відбуваються в зовнішньому середовищі, але діє, як правило. [13, с. 107].

Системне забезпечення та інформаційну безпеку креативного типу пропонуємо визначити як захист інформаційного суверенітету, як форми вираження суверенітету особистості, суспільства і держави, що легалізується законодавством та виражається в захисті конституційних прав і свобод людини і громадянина в інформаційній сфері [38, с.194].

Доступ до документів, що містять комерційну таємницю, здійснюється лише на підставі письмового дозволу керівника підприємства. Дозвіл на доступ може оформлятися як [15, с.28]:

♦ резолюція керівника підприємства на документі;

♦ оформлене у змісті розпорядчого документа (наказу, розпорядження або рішення) доручення щодо виконання документа із зазначенням посади і прізвища працівника – виконавця документа.

♦ окремо оформлений письмовий дозвіл на видавання документів.

Доступ виконавців до документів, що містять комерційну таємницю, здійснюється відповідно до затвердженого списку посадових осіб, які мають право працювати з такими документами. Зміни до цих списків, пов'язані з розширенням або, навпаки, з обмеженням зазначеного кола осіб, вносяться з письмового дозволу керівника підприємства на підставі відповідних доповідних записок керівників структурних підрозділів.

Отже, виконавець документа та особи, які візували й підписували документ, допускаються до нього без спеціального дозволу. У разі відсутності виконавця у зв'язку з відрядженням, відпусткою чи хворобою його

документами мають право користуватися керівник структурного підрозділу – інші працівники того самого підрозділу, які мають стосунок до зазначених документів.

2.2. Обмеження доступу та використання інформації документів, що містять конфіденційну інформацію в структурах оборони України

Конфіденційна інформація являється важливою інформація про юридичну або фізичну особу, важливі проекти доступ до якої обмежений і засекречений у закладі оборони України. Засекречений доступ до важливої інформації є її відкриття чи поширення або копіювання можливо лише за згодою її власників та на тих умовах, які вони здійснюються [23, с.237].

Відповідно до Закону «Про доступ до публічної інформації» *конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов* [2].

Схоже визначення нам дає Закон «Про інформацію» у статті 21, а саме: *«конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень* [11, с.108].

Конфіденційна інформація може поширюватися за бажанням згодою відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом».

Інформація з обмеженим доступом – це така інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб.

Обмежується доступ до інформації, а не до документу. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, то відкрита інформація може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу.

За змістом статті 6 Закону України «Про доступ до публічної інформації» вбачається, що інформація з обмеженим доступом, може бути наступною [38, с.194]:

1) конфіденційна інформація в закладах;

2) таємна інформація – (важлива інформація), доступ до якої обмежується і розголошення якої може завдати шкоди особі, суспільству і державі.

3) службова інформація – документи ОУ які міститься все про суб'єктів владних повноважень [17, с.135]:

Закон гарантує громадянину доступ до публічної інформації, а державні органи та установи — розпорядників цієї інформації – зобов’язує цей доступ забезпечувати. Втім це не значить, що можна, написавши запит, отримати абсолютно будь-яку інформацію. Розглянемо персональні дані та конфіденційна інформація на рисунку 2.3.

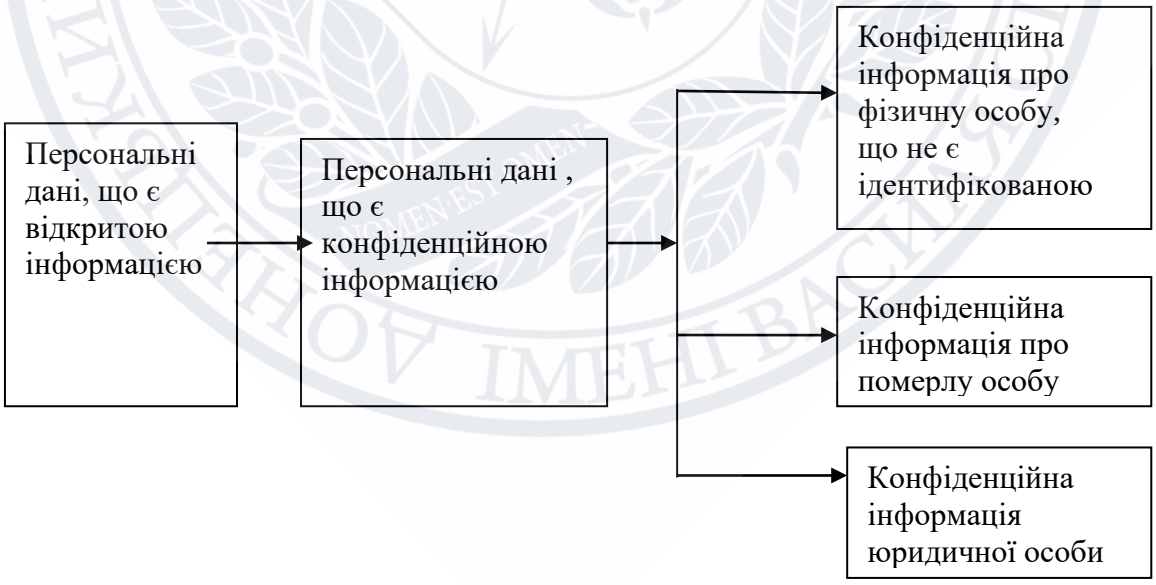


Рисунок 2.3. – Персональні дані та конфіденційна інформація

Проте повернемось до співвідношення понять конфіденційної інформації та персональних даних. Перше, що важливо запам’ятати персональні дані – це

завжди інформація про фізичну особу, при чому лише живу особу. Відповідно до статей 24 і 25 Цивільного кодексу України людина як учасник цивільних відносин вважається фізичною особою. Її цивільна правоздатність виникає в момент народження і припиняється в момент смерті. Тому, враховуючи положення Закону «Про захист персональних даних» і Цивільного кодексу, інформація про померлу особу не є її персональними даними.

Рішення про віднесення інформації до державної таємниці, продовження строку дії раніше прийнятого рішення про віднесення інформації до державної таємниці, зміну ступеня секретності інформації, скасування раніше прийнятого рішення про віднесення інформації до державної таємниці приймаються державним експертом з питань таємниць протягом одного місяця з часу надходження звернення державного, органи місцевого самоврядування.

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, особливої важливості, «цілком таємно» або «таємно» на схемі 2.4.

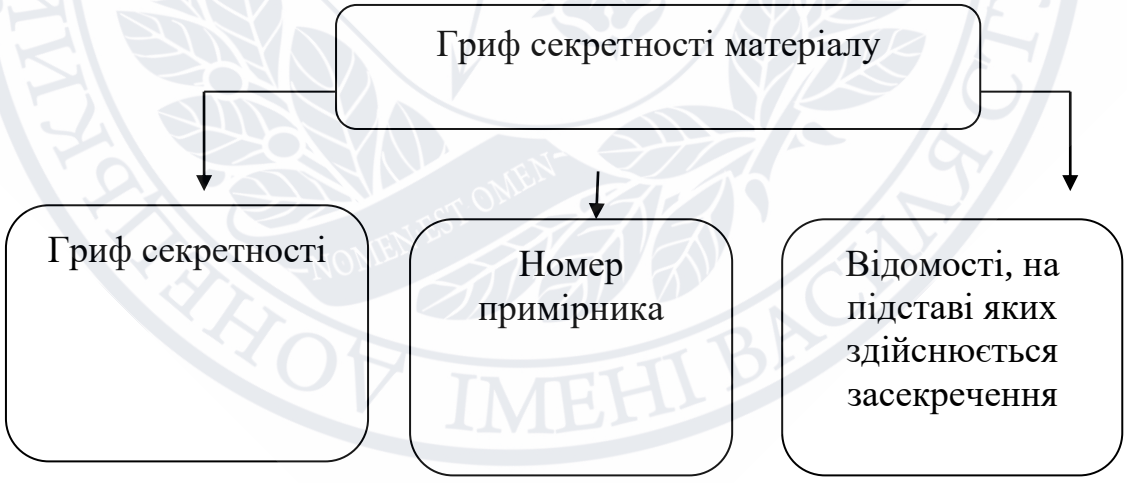


Рисунок 2.4. – Гриф секретності матеріалу

Такі рішення підлягають реєстрації Службою безпеки України та є підставою для формування Зводу відомостей, що становлять державну таємницю, і внесення змін до зазначеного Зводу, до галузевих або відомчих розгорнутих переліків відомостей, що становлять державну таємницю. Порядок реєстрації рішень державних експертів з питань таємниць

визначається Кабінетом Міністрів України [12, с.140].

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із відомостей, що становлять державну таємницю –«особливої важливості», «цілком таємно» або «таємно».

Комерційна таємниця має бути відповідна до комерційного виробничого та його характеру. За винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці і щодо яких ця юридична особа вжила заходи щодо збереження секретності. До конфіденційної юридичною особою може бути віднесена також і інша інформація.

Інформаційно-комунікаційні технології в документообіг системи оборони України є сукупність технологій, що забезпечують фіксацію інформації, її обробку і обмін інформацією передачу, поширення, розкриття [19, с. 127].

Розглянемо впровадження інформаційно-комунікаційних технологій в документообіг системи оборони України на рисунку 2.5.

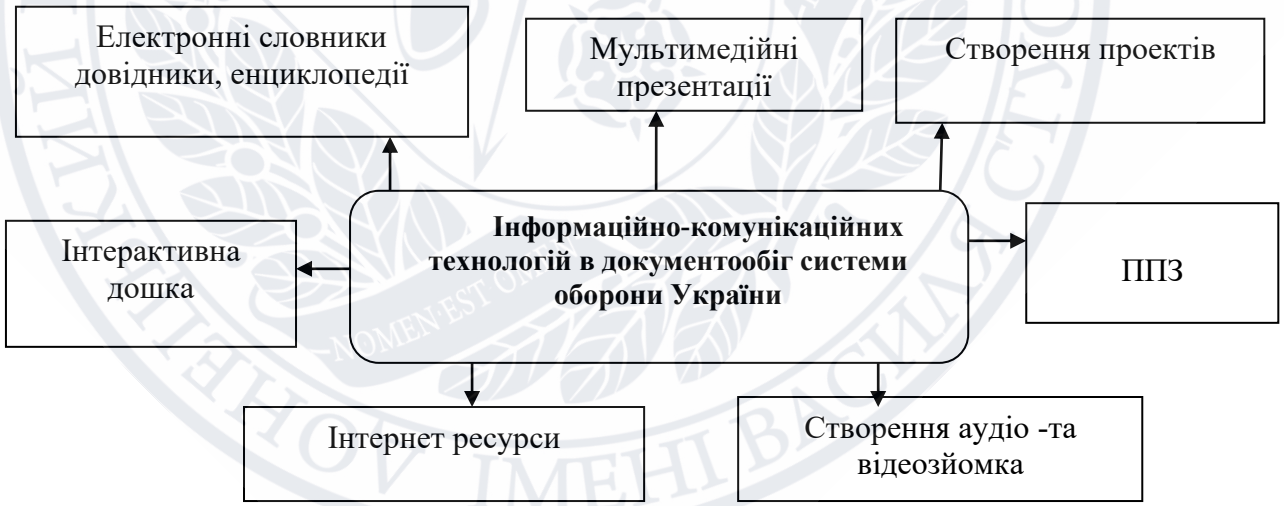


Рисунок.2.5. – Інформаційно-комунікаційні технології в документообігу системи оборони України

Проте необхідно враховувати, що це потребує значних затрат на організацію навчання порівняно з традиційними технологіями, що пов'язане з необхідністю використання значної кількості технічних (комп'ютери, модеми тощо), програмних (підтримка технологій навчання) засобів, а також з

підготовкою додаткової організаційно-методичної допомоги (спеціальні інструкції для тих, хто навчається, та для викладачів), нових підручників і навчальних посібників.

Міноборони планує переводити документи, які є базовими для військовослужбовців, в електронну форму. Мова йде про автоматизацію системи управління, про кар'єру військовослужбовця, адже це повинно бути стандартом. Всі папери повинні бути електронними, як рапорти, проходження ВЛК, заявки з електронними підписами тощо. Це все повинно перейти у безпаперову форму, при чому на рівні усіх Збройних Сил [41, с.28].

Науково-технічну інформацію, яка потенційно може містити комерційну таємницю, становлять:

- ідеї, винаходи, відкриття; окремі формули;
- нові технологічні проекти;
- програмне забезпечення;
- результати наукових досліджень;
- конструкторська документація, зокрема креслення, схеми, записи;
- плани розвитку підприємства та його інвестицій [11, с. 30].

Отже, повніший і точніший склад і обсяг відомостей, що містять комерційну таємницю конкретного підприємства, порядок захисту й доступу до цих відомостей, а також правила користування відповідними документами визначає керівництво цього підприємства. До проведення такої роботи керівництво може залучати відповідних фахівців - аналітиків.

Всі документи які становлять державну таємницю і містять конфіденційну інформацію, а також вони належать до обмеженої категорії тому вони призначені тільки в обмеженому колі [37].

РОЗДІЛ 3
РЕАЛІЗАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ В РОБОТІ ІЗ ДОКУМЕНТАМИ, ЩО МІСТЯТЬ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ

3.1. Інформаційні технології в роботі з документами з особливим доступом та новітні системи захисту даних

Військова частина – це основна організаційно-самостійна одиниця Збройних Сил України, яка має своє дійсне та умовне найменування, фінансується з коштів Державного бюджету, веде самостійне господарство, має кошторис надходжень та видатків, рахунки в установах банків, печатки із зображенням Державного Герба України і своїм найменуванням, тобто наділяє військову частину всіма ознаками, які приманні юридичній особі [7, с. 108].

Військова частина А1445 являється однією із військовою одиницею постійної організації в збройних силах, що організаційно може входити до складу більшої військової частини або з'єднання. Під поняттям «частина» найчастіше маються на увазі полк або бригада.

Характеристика в/ч А1445 — підрозділ військової розвідки України, який за організаційно-штатною структурою входить до складу Сухопутних військ України. Військова частина яка знаходиться за адресою: 22434, Україна, Вінницька область, с. Гущинці.

Під військовою частиною пропонує розуміти органи військового управління, з'єднання, частини, кораблі, військові навчальні заклади, установи та організації Збройних Сил України, які утримуються за рахунок коштів Державного бюджету України, ведуть відокремлене господарство, мають кошторис надходжень та видатків, рахунки в установах банків, печатку із зображенням Державного Герба України і своїм найменуванням. Дане визначення не є конкретним та в більшій мірі заплутує тлумачення даного поняття, змішуючи його головні ознаки.

Наказом Міністерства фінансів України «Про затвердження Порядку обліку платників податків і зборів» визначено, що військова частина – військові частини, заклади, установи, організації Збройних Сил України та інших утворених відповідно до законів України військових формувань. Здійснивши аналіз положень Наказу Міністерства оборони України «Про затвердження Положення про військове (корабельне) господарство Збройних Сил України», можна, узагальнивши, зазначити, що військовій частині (з'єднанню) притаманні такі характерні риси, а саме:

а) мають право постійного чи тимчасового користування різними об'єктами матеріально-технічної бази, матеріальними засобами, призначеними для забезпечення бойової підготовки і виховної роботи, військового побуту, правильної експлуатації, ремонту, зберігання озброєння, військової техніки і майна;

б) у своїй власності мають культурно-освітнє майно – технічні засоби виховання (у тому числі, поліграфічне устаткування), газетний папір, світлотехнічну апаратуру, устаткування сцен клубів та центрів культури, просвіти і дозвілля, музичні інструменти, телевізори, магнітофони, відеомагнітофони, програвачі, платівки, відео – та аудіокасети, настільні ігри, художні картини і скульптури, матеріали наочної агітації, друковані видання, витратні й експлуатаційні матеріали та інше майно, яке використовується в інтересах виховної роботи у Збройних Силах України;

в) командир військової частини, яка має права юридичної особи, у межах своїх повноважень та виділених коштів має право укладати господарські угоди або договори та нести повну відповідальність за обґрунтоване і правомірне витрачання (використання) коштів на пов'язану з цими угодами діяльність.

Водночас, на нашу думку, військовим частинам притаманні наступні ознаки:

1) є складовим елементом ЗСУ;

2) зовнішнім атрибутом військової частини є зображення Бойового Прапора військової частини ЗСУ, який розміщується на бланку Грамоти

Президента України, яка видається військовій частині під час вручення Бойового Прапора;

3) є колективним утворенням;

4) здійснення керівництва військовою частиною покладено на командира військової частини, який повинен забезпечувати постійний розвиток військового господарства частини, впровадження наукової організації праці при його веденні, постійне поліпшення матеріально-побутових умов та задоволення культурних потреб військовослужбовців, ощадливі та економні витрати матеріальних засобів і коштів, уміле й ефективне використання техніки при виконанні господарських заходів тощо.

Структурно військові частини складаються із:

–підрозділів (найменше військове формування, яке має командира); взводу (сукупність, як правило, 2-4 підрозділів);

–рота (сукупність декількох взводів); батальйонів (складається із декількох рот (зазвичай 2-4) і декількох взводів, що не входять в жодну із рот);

–полку (тактичне військове формування); бригад (військове формування, яке займає проміжне положення між полком і дивізією); дивізій (основне оперативно-тактичне формування);

–корпусу (є проміжним формуванням між дивізією і армією); армії (включає у себе дивізії, полки, батальйони усіх родів військ).

Разом з тим варто зазначити, що на сьогоднішній день гострою постала проблема визначення правового статусу такого структурного елементу військової частини як добровольчий батальйон, який перебуває у складі певної військової частини. У даному випадку мова йде саме про легалізацію цих добровольчих батальйонів та визначення відповідного правового.

Статус їх учасників, адже під час проведення антитерористичної операції горючими та невирішеними залишаються такі питання: видача зброї та її регулювання надалі, тобто наявність її обліку, забезпечення належним чином зберігання, передачу, проте нині у даному питанні спостерігається повний хаос; визначення статусу учасника бойових дій.

Водночас нагальною та невирішеною постає проблема законодавчого забезпечення права добровольців – учасників батальйонів бути визнаними членами АТО, тобто приймати активну участь не на підставі призову, а за власним бажанням, адже, сьогодні, такі особи можуть зіткнутися навіть з тим, що їх звинуватять в ухиленні від військової служби, оскільки вони де-юре продовжують обліковуватися як призовники, так як жодних підтверджуючих їхнє місцезнаходження документів їм не видають.

Так, на сьогоднішній день законодавцем здійснено розмежування та розподіл добровольчих батальйонів та визначено, що добровольчі батальйони будуть визнаватися законними, а їх учасники – членами АТО при умові їх приналежності до складу батальйонів Збройних Сил України, МВС чи Національної гвардії України.

Наявність подібних ситуацій, на нашу думку, спричиняє хаос та беззаконня в субординаційних відносинах, які виникають між добровольцем та його безпосереднім керівником.

Отже, водночас військова частина являється структурним елемент ЗСУ, сформований на основі директиви (наказу) вищого штабу (командира, командуючого), який виконує завдання та функції визначені специфікою діяльності видів ЗСУ та утримуються за рахунок коштів Державного бюджету.

Розглянемо структуру військової частини А 1445 на рисунку 3.1.

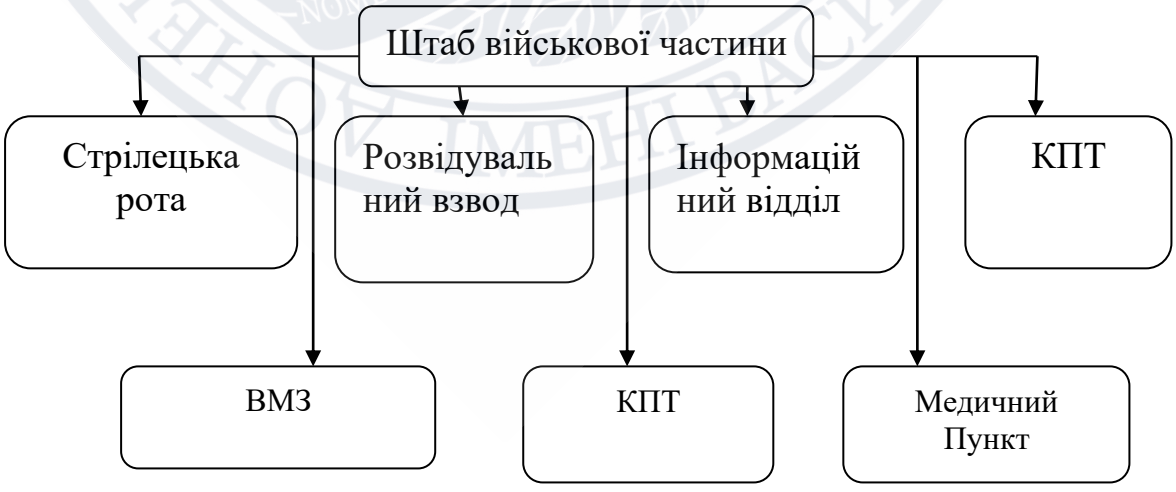


Рисунок – 3.1.Структура військової частини А 1445

В організаційно-штатній структурі вказуються: структурні підрозділи, що входять до складу військового формування, установи, організації, закладу; найменування і кількість посад військовослужбовців, робітників і службовців у кожному з них; посадові оклади, а також джерела грошових коштів для їх виплати.

Табель до штату є невід'ємним обов'язковим додатком до організаційно-штатної структури частини (підрозділу) у цьому документі в табличному вигляді розписано, які підрозділи мусять мати яку техніку.

Структура та чисельність особового складу військових навчальних підрозділів, що здійснюють підготовку військових фахівців, визначаються штатами, а військових навчальних підрозділів, що призначені для підготовки офіцерів запасу з числа студентів, - штатними розписами.

До складу військового інституту можуть входити факультети, кафедри, наукові, науково-дослідні центри та лабораторії, підрозділи курсантів (слухачів, студентів), навчальні центри, курси перепідготовки (підвищення кваліфікації) тощо. Військовий коледж створюється у складі ВНЗ або вищого військового навчального закладу третього (четвертого) рівнів акредитації та є його навчальним структурним підрозділом.

Робота радіотелеграфної передачі інформації військової частини А1445 на рисунку 3.2.

Рисунок – 3.2. Радіотелеграфування; інформаційний відділ військової частини А1445

Основними завданнями відділу є:

1) інформаційно-аналітичне забезпечення діяльності органів державної влади;

2) сприяння реалізації конституційного права громадян на свободу слова;

3) забезпечення проведення державної політики в інформаційній та видавничій сферах міста;

4) співпраця із засобами масової інформації різних форм власності;

5) створення умов для розвитку інформаційної та видавничої сфер на території міста;

6) забезпечення комунікативної політики влади та громадськості;

7) забезпечує реалізацію державної політики в інформаційній та видавничій сферах.

Отже, надає засобам масової інформації, суб'єктам видавничої справи всіх форм власності методичну, організаційно-практичну та консультаційну допомогу. Вживає у межах своїх повноважень заходів до провадження зовнішньоекономічної діяльності, захисту інтересів вітчизняних виробників інформаційної продукції на внутрішньому та зовнішньому ринках.

3.2. Впровадження інформаційно-комунікаційних технологій в документообіг системи оборони України

Впровадження інформаційно-комунікаційних технологій в документообіг системи оборони України ставить за мету проаналізувати існуючі в Україні СЕД, їх загальну організацію, окреслити проблеми щодо впровадження таких систем, визначити основні переваги електронного документообігу, як складової електронного урядування та визначити завдання для подальшого їх розвитку.

Одним із головних пріоритетів України є побудова інформаційного суспільства, орієнтованого на інтереси людей, відкритого для всіх і спрямованого на розвиток, в якому кожен міг би створювати і накопичувати

інформацію та знання, повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові для підвищення якості життя.

Застосування комплектів станцій супутникового зв'язку. Основою польової складової системи зв'язку ЗС України сьогодні залишається супутниковий зв'язок. Розглянемо аналіз балансу за новітні технологічні прилади на рисунку 3.1.

Таблиця 3.1. – Аналіз балансу нових технологічних приладів

№	Найменування	Рік виготовлення	Первісна вартість, грн	Знос, грн.	Залишкова вартість грн.
1.	Прилад TSA - 9	2019	198000,00	-	198000,00
2.	Тепловізор Pulsar Quantum HD 50S	2015	99000,00	43290,50	56609,50

З причини відсутності в Україні власних супутників зв'язку, цю послугу орендують у оператора зв'язку із застосуванням засобів транкінгового зв'язку. Розглянемо впровадження інформаційно-комунікаційних технологій в документообіг системи військової частини А1445 на рисунку 3.3.

Рисунок 3.3. – Інформаційно-комунікаційні технології в документообігу системи військової частини А1445

У державному агентстві резерву України використання ЕПЦ передбачено, але на час опитування воно не використовується (інформацію про кількість ключів не надано). Кабінет міністрів України щорічно звітує про стан інформатизації та розвиток інформаційного суспільства в Україні.

Таблиця 3.2. – Інформаційно-комунікаційних технологій в документообіг системи оборони України

№	Рівень технологізації діловодних процесів	Характеристика процесу	Характеристика засобів
1.	Автоматизація основних процесів документування	Текстовий процес сприяє оформленню текстів	Відсутня комплексна автоматизація всіх процесів
2.	Автоматизація роботи з документами	Використання комп'ютерної техніки для реєстрації документів	Документування та документообіг, сучасними процесами
3.	Об’єднання автоматизованих робочих місць	Обґрунтування групових автоматизованих робочих місць	Відсутність єдиної системи та єдиного програмного забезпечення ділових процесів

Досвід показав що, станом на кінець 2020 року в Сухопутних військах за рахунок державних закупівель, волонтерської допомоги активно використовувались засоби зв’язку іноземного, але, як правило, цивільного, виробництва: транкінгове обладнання Motorola, супутникові термінали Tooway, станції широкосмугового доступу фірм Ubiquiti, Microtik, комутатори і маршрутизатори фірм Cisco, Microtik, обладнання мережі тощо [31, с.214].

У подальшому, протягом 2015-2017 років у ЗСУ проводилось нарощування та удосконалення системи зв’язку й автоматизованого управління військами. З початком широкого застосування противником засобів і комплексів

радіоелектронної боротьби виникла необхідність в оснащенні радіостанціями військового призначення фірм Harris, Aselsan, Elbit [21, с.156].

Оператор, не втручаючись у налаштування, може використовувати станцію для зв'язку в будь-який момент [7, с.60].

Однією з переваг SDR є можливість отримання багатьох функцій і сервісів в одному компактному корпусі. Одна система може виконати роботу, для якої раніше вимагалося декілька радіостанцій.

Розглянемо Інформаційно-комунікаційних технологій в документообіг системи оборони України у таблиці 3.3.

Таблиця 3.3. - Інформаційно-комунікаційних технологій в документообіг системи оборони України

Назва СЕД (розробник)	*2018 рік*	*2019 рік*	*2020 рік*
Megapolis. документообіг (софтлайн)	32 %	21,18 %	40 %
OPTIMA-WorkFlow (Optima)	15 %	22,35 %	15 %
Док проф (ситроникс)	11 %	10,59 %	10 %
Дело (електронні офісні системи)	9 %	4,71 %	–
MasterDOC (Банкомсвязь)	2 %	3,53 %	5 %
Атлас доК (атлас)	2 %	5,88 %	5 %
летограф (летограф)	–	2,35 %	–
інше	29 %	29,41 %	25 %

Данні про військовослужбовців, які мають SDR-радіостанцію і вбудовані системи глобального позиціонування , можуть транслюватись у мережі так, що всі кореспонденти мережі, або тільки командир, може знати, і навіть бачити на реальній карті місцевості, де вони знаходяться. Строк служби військової радіостанції, як правило, дорівнює 15-20 рокам, а тому ще одна велика перевага SDR полягає у можливості оперативної її модернізації [25].

Щодо системи управління базами даних (далі – СУБД), то державні органи найчастіше віддають перевагу системам Oracle та MSSQL12.

За даними національного центру підтримки електронного урядування, в державних органах впроваджено та експлуатується СЕД, більшість з яких на даний час є несумісними між собою як за форматами електронного документу, так і за форматами ЕЦП. Така ситуація стала можливою у результаті хаотичного, несистемного розвитку національної системи ЕЦП та відсутності сертифікації СЕД і уніфікованих форматів, що не тільки унеможливлює електронну взаємодію державних органів між собою при наданні ними державних послуг та є загрозою національній безпеці держави.

Розглянули етапи розробки концепції захисту інформації на рисунку 3.4 [16, с.184].

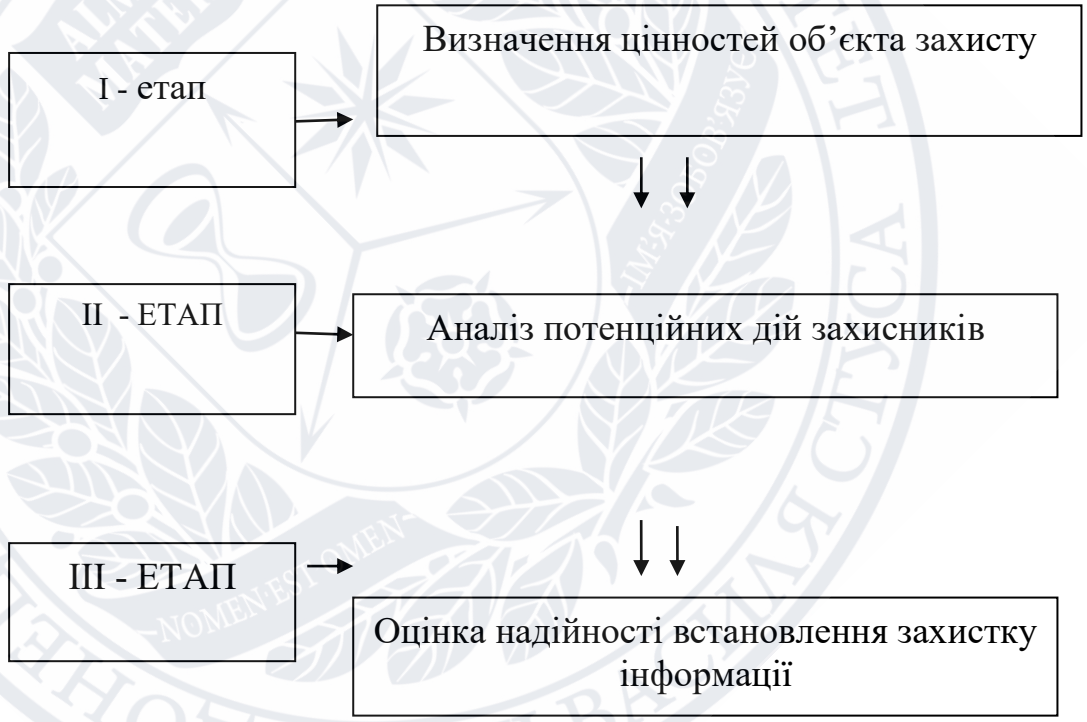


Рисунок 3.4. – Концепція захисту інформації

На рисунку ми побачили, що у військові частині розроблено основну концепції захисту у три етапи. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів.

Ще одним кроком на шляху до оптимізації роботи з електронними документами в Україні стало розпорядження Кабінету міністрів України

питання впровадження системи електронної взаємодії органів виконавчої влади.

На виконання цього розпорядження було створено системи електронної взаємодії органів виконавчої влади (далі – система взаємодії), що дозволяє здійснювати обмін електронними документами. “положення про систему електронної взаємодії органів виконавчої влади затверджено постановою Кабінету міністрів України, а згодом міністерство юстиції України затвердило Порядок роботи з електронними документами через систему електронної взаємодії з використанням ЕЦП [28, с.134-135].

Слід зазначити, що найвагомішим документом, що дозволить унормувати роботу різних СЕД, а також системи взаємодії, є проект Порядку роботи з електронними документами та їх підготовки до передавання на архівне зберігання, розроблений державною архівною службою України.

Таблиця 3.4. – Програмне забезпечення

Назва системи (розробник)	Відсоток
Megapolis документообіг (софтлайн)	39,5 %
OPTIMA-WorkFlow (Optima)	13,2 %
АСКОД (інфоплюс)	10,5 %
Док проф (ситроникс)	5,3 %
MasterDOC (Банкомсвязь)	5,3 %

Згідно з даними різних джерел із мережі інтернет в Україні акредитованими центрами сертифікації ключів на сьогодні видано понад 800 тисяч посилених сертифікатів ключів, електронну звітність збирають 11 державних органів; так, міністерство доходів і зборів отримує електронну звітність від понад 480 тисяч суб’єктів господарювання.

Впровадження електронного документообігу з використанням ЕЦП, як пріоритетний напрям державної політики щодо електронного урядування, визначено актами президента України, верховної Ради України та Кабінету міністрів України [22, с.203].

Упродовж 2012 р. Центральним державним електронним архівом України проведено вивчення стану впровадження СЕД у державних органах. до 47 державних органів направлено запити щодо видів впроваджених СЕД та їх основних характеристик 23, відповіді надійшли від 42 державних органів.

Зазначені документи встановлюють загальні правила створення, відправлення, передавання, одержання, опрацювання, використання та зберігання електронних документів та електронних копій паперових документів, на які накладено ЕЦП, таких, що не містять інформацію з обмеженим доступом. Однак, незважаючи на те, що нині завершено дослідну експлуатацію системи взаємодії та здійснюється її підготовка до переведення у режим експлуатації, досі немає інструкції з організації роботи системи взаємодії, яка визначала б порядок дій органів влади для підключення до неї та безпосереднього опрацювання в ній документів і інформації, що забезпечує їх чітку взаємодію з іншими органами виконавчої влади та секретаріатом Кабінету міністрів України.

Причини витоку інформації також пов’язані, як правило, з недосконалістю керівних документів щодо збереження інформації, а також їх порушенням, у тому числі відступом від правил поводження з грифованими документами, технічними засобами, зразками продукції та носіями, що містять інформацію службового характеру. До таких факторів та порушень можна віднести:

- недостатнє знання користувачами основ захисту інформації й нерозуміння необхідності їх ретельного дотримання;
- використання неатестованих або несертифікованих технічних засобів обробки грифованої інформації, тому що це обладнання, у кращому випадку, просто може бути недоопрацьованим, а в гіршому — воно може містити закладки на фізичному або програмному рівнях;
- слабкий контроль за дотриманням правил захисту інформації з боку штатних або позаштатних служб захисту інформації та кібернетичної безпеки й інженерно-технічних підрозділів, які неналежним чином стежать за справністю обладнання або ліній;

- плинність кадрів, оскільки вони володіють інформацією з обмеженим доступом або даними службового характеру [42].

Захист інформації тією чи іншою мірою має забезпечуватися будь-якою системою обміну даними. При цьому впорядкування та консолідація інформації, впорядкування документообігу дає можливість створити більш якісну систему захисту.

Отже, проаналізувавши отримані відповіді, можна зробити висновок, що нині в державних органах впроваджено системи автоматизації діловодства і системи електронного документообігу. СЕД орієнтовані на автоматизацію документацій них процесів стосовно паперових документів. до основних функцій сад належать: реєстрація вхідних, вихідних та внутрішніх документів, контроль за їх виконанням.

Відповідні підрозділи кібернетичної безпеки інформаційно-телекомунікаційних систем здійснюють цілодобовий захист усіх систем обміну даними, які були прийняті на озброєння та використовуються в Збройних Силах України, адже головна мета — запобігти спробам викрадення, видалення чи модифікації інформації. Також коректне й повноцінне функціонування цих систем створює умови для ефективнішої роботи, швидкого прийняття рішення, від якого залежить подальша доля того чи іншого підрозділу.

ВИСНОВКИ

Кваліфікаційну роботу присвячено специфіці руху та характерним відмінностям в роботі з документами, що містять конфіденційну інформацію, в системі оборони України. Військові підрозділи в усьому світі вже активно використовують захищені системи обміну даними і майже зовсім відмовилися від паперового діловодства.

Останніми роками попит на системи обміну інформацією в Україні інтенсивно збільшувався, поступово усвідомлення цінності його впровадження і постійного використання назріло в стратегічних галузях. Виявлено, що важливим аспектом використання захищених систем обміну даними для прийняття ефективного рішення та збереження цілісності інформації в системі оборони виступають нормативно-правові засади та відповідні рішення в самій структурі.

Збройні Сили України — інтенсивний користувач системами обміну даними, оскільки налічує тисячі локальних мережевих адресатів, які існують у сотнях систем обміну даними та якими користується велика кількість людей щодня. Усі ці елементи системи є необхідними артеріями для правильного функціонування, ефективного управління та прийняття рішень, які, у свою чергу, приносять бажані результати.

Тому, упроваджуючи системи обміну даними, необхідно запровадити відповідні механізми безпеки, оскільки доступ до таємних документів надзвичайно великий. Також розглянуто можливі засоби захисту комп’ютерних мереж, мережевих пристроїв та операційних систем з їх файловими системами, систем обміну даними.

Простежено документообіг в структурах системи оборони України від моменту створення або від одержання зі сторони до моменту передачі на зберігання до архіву. В Збройних Силах України триває робота над зменшенням документообігу та впровадженням електронного військового

квитка. З поступовим наближенням Збройних Сил України до нових стандартів та структур, відбувається і процес унормування документообігу.

Окрім цього, у Збройних Силах України належну ефективність протягом останніх років показала захищена система електронного документообігу «СЕДО». Триває робота й над унормуванням нормативних документів для уніфікації особистих документів військовослужбовців. Паралельно проводяться дослідження щодо введення в дію автоматизованої електронної системи, яка передбачає використання електронного військового квитка (ЕВК).

Окремо в роботі представлено видові особливості документів, які містять державну таємницю та конфіденційну інформацію. Порівнюючи документи, що становлять державну таємницю та ті, які містять конфіденційну інформацію, можна зробити висновок – спільним є їх належність до категорії таємної інформації, тому і призначені вони для користування тільки в обмеженому колі.

Збитки, які може понести держава у разі розголошення державної таємниці, можуть бути набагато масштабнішими за розголошення комерційної таємниці на підприємстві. Відомості, що засекречуються під грифами «державна таємниця» та «комерційна таємниця» можуть бути найрізноманітнішого змісту: економічного, військового, фінансового, науково-технічного і інші. Однак існують межі, які не дозволено перетинати при віднесенні інформації до таємної. Види інформації, що має залишатись відкритою та критерії при відборі інформації до засекречування розглянуто в роботі.

Окрему увагу зосереджено на аспектах впровадження інформаційно-комунікаційних технологій в документообіг системи оборони України. Встановлено що захист інформації має забезпечуватися будь-якою системою обміну даними.

Впорядкування та консолідація інформації, налагодження документообігу дає можливість створити більш якісну систему захисту. Величезне значення для забезпечення конфіденційності інформації мають криптографічні системи

захисту даних, які забезпечують конфіденційність документа навіть у разі його потрапляння до рук сторонньої особи.

Загалом робота з військовими документами, які містять конфіденційну таємницю має свої особливості, однак існують межі, які не дозволено перетинати при віднесенні інформації до таємної. А система обміну даними повинна забезпечити не тільки передачу інформації, але її збереження від викрадення чи модифікації, а також мати можливість її швидкого відновлення.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Конституція України. Інститут законодавства Верховної Ради України. К., 1996. 116 с.

2. Закон України «Про державну таємницю» № 3856-12 від 21.01.94: http://zakon2.rada.gov.ua/laws/show/3855-12

3. Закон України «Про інформацію». Відомості Верховної Ради України. 1992. № 48. С. 658.

4 Закон України «Про захист від недобросовісної конкуренції» від 7 червня 1996 р., № 236. К., 1996. Т. 10. С. 303-311.

5. Апенюк С.А. Документообіг документів в установі на зберігання до архіву «інформаційна безпека» системі оборони України. К. Економічна наука. 2018. № 3. С. 66-69.

6. Баланенко О.Г., Павлова К.В. Інформаційні системи Пенсійного фонду України. Економіка та управління підприємствами. 2017. № 4-1. С. 113-116.

7. Бабенко Л.В. Історія становлення і теоретичні засади розвитку на сучасному етапі національного державотворення: дис. канд. наук з держ. управління. Одеський регіональний інститут державного управління. Одеса, 2017. 252 с.

8. Благодатний А.М. Деякі проблеми адміністративної відповідальності за порушення законодавства про державну таємницю. Збірник наукових праць. К., 2002. № 16. С. 200.

9. Діденок О.С. Правові проблеми захисту інформації з обмеженим доступом на шляху до НАТО. *Підприємство, господарство і право*. К., 2018. 319 с.

10. Глухівський Л. Державна таємниця та охорона прав на винаходи. *Інтелектуальна власність*. 2005. № 9. С. 289.

11. Глущик С.В. Сучасні ділові папери. К.: А.С.К., 2018. 173 с.

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

13. Глухівський Л. Державна таємниця та охорона прав на винаходи. *Інтелектуальна власність*. 2005. № 9. С. 289.

14. Глущик С.В. Сучасні ділові папери. К.: А.С.К., 1998. 173 с.

15. Загорецька О. Особливості роботи з документами, що містять комерційну таємницю підприємства. *Довідник кадровика*. 2011. № 9 (111). С. 40-46.

16. Ілюшенко Я.С. Інформаційне законодавство України. К. 2014. 437 с.

17. Інформаційне законодавство України. К., 2019. 232 с.

18. Кавторева Я. Документооборот: организация и ведение. Х.: Издательский дом «Фактор», 2004. 220 с.

19. Калюжний Р. Проблеми та перспективи правового забезпечення безпеки інформації з обмеженим доступом, що не становить державної таємниці. Збірник НТУУ «КПІ», МОН України, ДСТЗІ СБ України. К., 2000. С. 27–31.

20. Калакури І.А, Кушнаренко Н.Н. Документоведение. К.: Т-во «Знання», КОО, 2000. 460 с.

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

22. Ковалів С.А. Автоматизація діловодства. Перший етап. *Діловодство*. 2018. № 7. С. 41-46.

23. Кушнаренко Н.Н. Документоведение. К.: Т-во «Знання», КОО, 2000. 460 с.

24. Малиновського А.Г., Максимович Г.Ю. Нові можливості автоматизації діловодства. *Секретарська справа*. 2019. № 4. С. 19-2; 31-33; 36.

25. Мельника П.В. Основи інформаційного права України. К.: «Знання», 2019. 371 с.

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

27. Основи інформаційного права України. К. : «Знання», 2004. 274 с.

28. Рудик П.А. Коментар до конституційних змін. К.: ЦУЛ, 2008.297 с.

29. Ткаченко Н.Н. Документоведение. К.: Т-во «Знання», КОО, 2019. 460 с.

30. Терлецька Н.М., Білоконь К.В. Сучасні інформаційні технології як чинник ефективності інтегрованої інформаційно-аналітичної *Науковий вісник* Чернівецького університету. 2019. № 861. С. 103-104.

31. Янківська Ю.О. Сучасні ділові папери. К.: А.С.К., 2018. 173 с.

32. Янчук О.М. Типологія документа. К.: Кн. палата України, 1998. 193 с.

33. Швец М.Я. Основи інформаційного права України. К.: «Знання», 2004. 274 с.

34. Швецова-Водка Г.М. Державна таємниця та охорона прав на винаходи. *Інтелектуальна власність*. 2005. № 9. С. 289.

35. Юрчак В.Ю. Перспективи правового забезпечення безпеки інформації державної таємниці. К., 2019. 473 с.

36. Академічний тлумачний словник. URL: http://sum.in.ua/s/chastyna.

37. Діловодство й архівна справа. Терміни та визначення понять / ДСТУ 2732:2004.

38. *Ковальська Л.А., Липова С.В., Мазуркевич Т.Л.* Перспективи розвитку послуг е-урядування у Вінниці. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. Випуск 11. Т. 1. 2019. С. 160-165. URL: http://jvestnik-sss.donnu.edu.ua/article/view/6700/6732

39. Липова С.В. Поняття та основні властивості віртуального офісу. Збірник матеріалів IV Всеукраїнської наукової конференції «Інформаційні технології і системи в документознавчій сфері» за підсумками науково-дослідницької роботи студентів спеціальності «Інформаційна, бібліотечна та архівна справа». Вінниця: ДонНУ імені Василя Стуса, 2019. С. 64-65.

40. Липова С.В. Невербальні засоби спілкування в умовах Internet-комунікації. V Всеукраїнська наукова конференція «Інформаційні технології і системи в документознавчій сфері» за підсумками науково-дослідницької роботи студентів спеціальності «Інформаційна, бібліотечна та архівна справа». Вінниця: ДонНУ імені Василя Стуса, 2020. С. 25-27.

41. Липова С.В. Особливості електронного документообігу у роботі з документами, що містять таємну інформацію. VI Всеукраїнська наукова конференція «Інформаційні технології і системи в документознавчій сфері» за підсумками науково-дослідницької роботи студентів спеціальності «Інформаційна, бібліотечна та архівна справа». Вінниця: ДонНУ імені Василя Стуса, 2021. С. 19-21.

42. Захист інформації в системах обміну даними. Офіційний сайт Міністерства оборони України. URL: https://www.mil.gov.ua/ukbs/zahist-informaczii-v-sistemah-obminu-danimi.html

43. Державні інформаційні системи та захист інформації: питання та відповіді. URL: https://softline.org.ua/news/derzhavni-informatsiini-systemy-ta-zakhyst-informatsii-pytannia-ta-vidpovidi.html

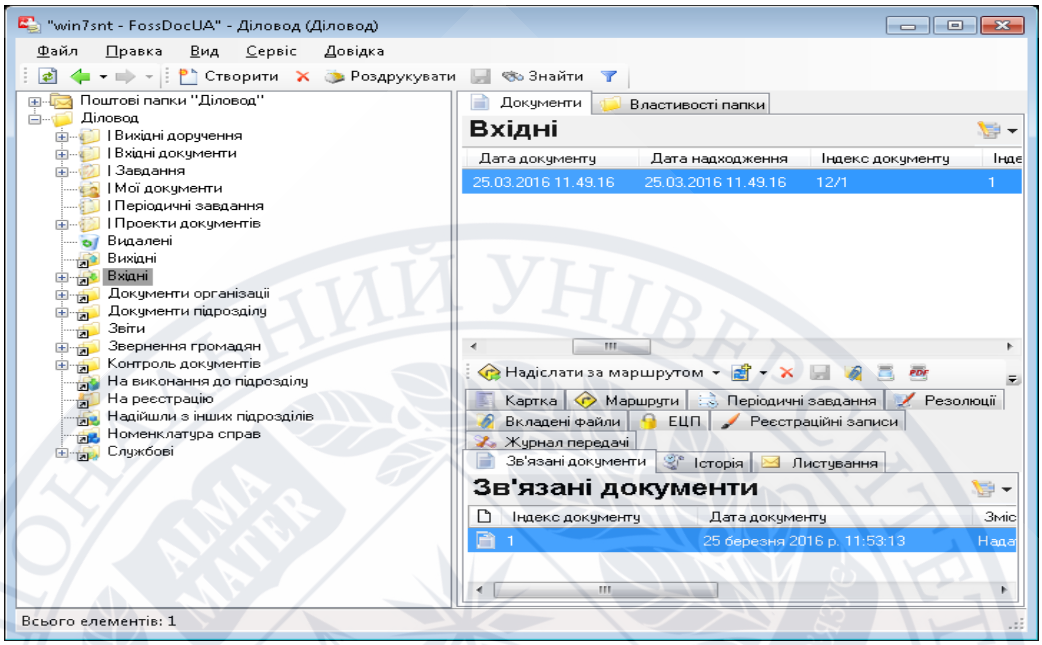
44. Перелік відомостей Міністерства оборони України, які містять службову інформацію (ПСІ – 2016). URL: https://www.mil.gov.ua/content/other/MOU_720_27122016.pdf

45. Про затвердження Інструкції із забезпечення доступу до публічної інформації в Міністерстві оборони України та Збройних Силах України. НАКАЗ Міністерства Оборони України № 319 від 13.06.2017. URL: https://zakon.rada.gov.ua/laws/show/z0827-17#Text

ДОДАТКИ

Додаток А

Підтримка різних видів документів



Додаток Б

Класифікація систем електронного документообігу

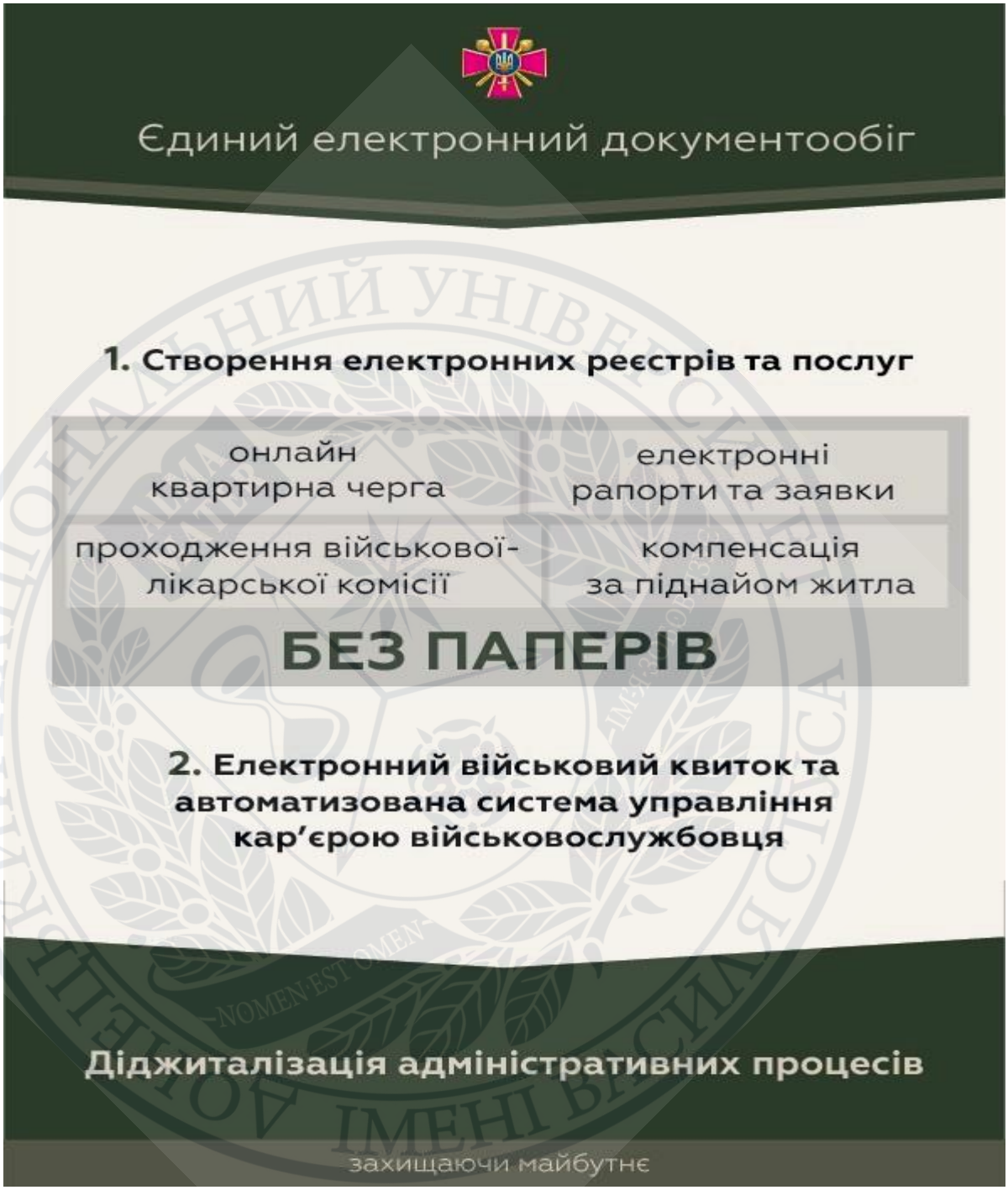
Клас системи	Функції(особливості)	Зберігання Документів
“Електронне діловодство”	забезпечення робот з електронними версіями документів і *реквізитами реєстраційно – контрольних форм* відповідно до прийнятих в Україні правил і стандартів діловодства	Робоча станція Виконавця
“Документообіг”	забезпечення чітко регламентованого і формально контрольованого руху документів усередині і поза організацією на основі інформаційно-телекомунікаційних технологій, часткова підтримка процесів роботи над документами	Робоча станція виконавця, файл-сервер
“Системи електронного управління документами”	забезпечення повного циклу: створення, перетворення, забезпечення безпеки, управління доступом і поширення великих обсягів документів у корпоративних комп’ютерних мережах, забезпечення контролю над потоками документів в установі, знищення тощо	Спеціальні сховища (центральні або розподілені файл-сервери) або в ієрархії файлової системи
“Корпоративні системи електронного управління документами”	забезпечення спільної роботи над документами і їх публікації, доступної практично всім користувачам, інтеграція з офісними пакетами, наявність інформаційних порталів та зв’язку через мережі Internet, Intranet та Extranet	спеціальні сховища (центральні або розподілені файл-сервери) або в ієрархії файлової системи

Додаток В

Документообіг системи оборони України

Додаток Г

Документообіг системи оборони України



Додаток Д

Спеціальний дозвіл системи оборони України

Інв. № 1146 від 13.11.2020 ДП "Житомирський бронетанковий завод"

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Управління Служби безпеки України в Житомирській області

вул. Фещенка-Чопівського, 7, м. Житомир, 10008, тел. (0412) 37-21-52
www.ssu.gov.ua, e-mail: usbu_zhr@ssu.gov.ua, Код ЄДРПОУ 20001510

СПЕЦІАЛЬНИЙ ДОЗВІЛ

на провадження діяльності, пов'язаної з державною таємницею

від "13" листопада 2020 року **№ ЖИЗ–2020-071**

Наданий

Державному підприємству "Житомирський бронетанковий завод"

на підставі заявки № 73/238дск від 22 жовтня 2020 року та акту спеціальної експертизи щодо наявності умов, необхідних для провадження діяльності, пов'язаної з державною таємницею, від «13» листопада 2020 року № 28/1166дск у Державному підприємстві "Житомирський бронетанковий завод", що підпорядковується Державному концерну "Укроборонпром".

Місцезнаходження: 12441, Житомирська область, смт. Новогуйвинське, вул. Дружби Народів, 1.

Місцезнаходження РСО: 12441, Житомирська область, смт. Новогуйвинське, вул. Дружби Народів, 1, на другому поверсі адмінбудівлі підприємства, каб. № 15.

Організаційно-правова форма: державна установа.

Категорія режиму секретності: третя.

Діє до 15 листопада 2022 року.

Начальник Управління **Сергій ЛИСАК**

Служба безпеки України в Житомирській області * Ідентифікаційний код 20001510 *