Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Модель вибору та аналізу комплексу засобів захисту державних інформаційних ресурсів критичної інфраструктури»

Виконавець: студент IV курсу, групи КБ-41

_____ **Олександр БУЧИК**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Сергій ТОЛЮПА
Нормоконтроль		Леся БАРАНОВСЬКА

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** **Бучику Олександру Сергійовичу**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи «Модель вибору та аналізу комплексу засобів захисту державних інформаційних ресурсів критичної інфраструктури»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації (протокол №6 від 28.11.2024 р.)

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Нормативно-правові акти України, методичні рекомендації та стандарти, аналітичні матеріали і звіти про сучасні кіберзагрози для державних інформаційних ресурсів об'єктів критичної інфраструктури, а також функціональні та архітектурні особливості систем електронного документообігу

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Проаналізувати нормативно-правову базу та стандарти у сфері захисту державних інформаційних ресурсів критичної інфраструктури, класифікувати засоби захисту інформації, розробити модель вибору та аналізу комплексу засобів захисту систем електронного документообігу критичної інфраструктури

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність моделі вибору та аналізу комплексу засобів захисту систем електронного документообігу державних інформаційних ресурсів критичної інфраструктури полягає в її потенційній користі для фахівців у галузі кібербезпеки та державних установ, що експлуатують такі системи.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 25 листопада 2024 року

Завдання видав _____ (підпис) Сергій ТОЛЮПА (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр БУЧИК (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Формулювання мети, завдань і уточнення постановки дослідження	25.11.2024 – 01.12.2024	виконано
2	Огляд, аналіз та систематизація літературних джерел	02.12.2024 – 22.12.202	виконано
3	Аналіз нормативно-правової бази та стандартів у сфері захисту ДІР КІ	23.12.2024 – 14.01.2025	виконано
4	Класифікація та аналіз існуючих засобів захисту інформації для СЕДО	15.01.2025 – 04.02.2025	виконано
5	Розробка та обґрунтування моделі вибору та аналізу комплексу засобів захисту СЕДО для КІ	05.02.2025 – 25.03.2025	виконано
6	Оцінювання результатів дослідження та формування узагальнених висновків	26.03.2025 – 10.04.2025	виконано
7	Оформлення пояснювальної записки відповідно до методичних рекомендацій.	11.04.2025 – 06.05.2025	виконано
8	Підготовка та подання пакету документації до захисту в ЕК	07.05.2025 – 13.05.2025	виконано

Завдання видав _____ (підпис) Сергій ТОЛЮПА (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр БУЧИК (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему «Модель вибору та аналізу комплексу засобів захисту державних інформаційних ресурсів критичної інфраструктури» містить 94 сторінок основного тексту, ілюстрована 11 рисунками та 2 таблицями, містить посилання на 30 джерел літератури.

Актуальність теми. Ключовими факторами, що зумовлюють актуальність даної теми, є:

1. критична важливість інформаційних ресурсів та інфраструктури;
2. залежність державних органів і підприємств критичної інфраструктури (КІ) від систем електронного документообігу (СЕДО);
3. зростання кіберзагроз та неспровокована агресія рф проти України; необхідність системного підходу до захисту;
4. практичне значення безпосередньо для нашої держави.

Метою роботи є розробка моделі для вибору та аналізу комплексу засобів захисту державних інформаційних ресурсів критичної інфраструктури, що обробляються в системах електронного документообігу.

Об’єктом дослідження є процес вибору та аналізу комплексу засобів захисту систем електронного документообігу державних інформаційних ресурсів критичної інфраструктури.

Предметом дослідження є моделі, методи та засоби захисту систем електронного документообігу як складової критичної інфраструктури.

Для досягнення поставленої мети потрібно вирішити наступні завдання:

1. Проаналізувати існуючі підходи, стандарти та нормативно-правову базу щодо захисту державних інформаційних ресурсів та критичної інфраструктури, з особливим акцентом на вимоги до безпеки систем електронного документообігу.
2. Розглянути основні категорії засобів захисту інформації релевантних для систем електронного документообігу.

3. Розробити модель вибору засобів захисту, що враховує специфіку роботи систем електронного документообігу з державними інформаційними ресурсами та їх інтеграцію в критичну інфраструктуру.

Практична цінність моделі вибору та аналізу комплексу засобів захисту систем електронного документообігу державних інформаційних ресурсів критичної інфраструктури полягає в її потенційній користі для фахівців у галузі кібербезпеки та державних установ, що експлуатують такі системи.

Ключові слова: державні інформаційні ресурси, критична інфраструктура, модель, об’єкти критичної інфраструктури, комплекс засобів захисту, система електронного документообігу, кваліфікований електронний підпис, кіберзагрози.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ДІР	–	державні інформаційні ресурси
КІ	–	критична інфраструктура
ОКІ	–	об’єкти критичної інфраструктури
КІІ	–	критична інформаційна інфраструктура
СЕДО	–	система електронного документообігу
ШПЗ	–	шкідливе програмне забезпечення
TDoS	–	Telephone Denial-of-Service
АРМ	–	автоматизоване робоче місце
КЕП	–	кваліфікований електронний підпис
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
SIEM	–	Security Information and Event Management
АЦСК	–	акредитований центр сертифікації ключів
API	–	Application Programming Interface
РМК	–	реєстраційно-моніторингова картка
СЕВ ОВВ	–	система електронної взаємодії органів виконавчої влади
УІБ	–	управління інформаційною безпекою
СУІБ	–	система управління інформаційної безпеки
КСЗІ	–	комплексна система захисту інформації
Держспецзв’язку	–	Державна служба спеціального зв’язку та захисту інформації України
СЗІ	–	системи захисту інформації
КЗІ	–	криптографічний захист інформації
СВЕД	–	системою взаємодії електронних документів
CERT-UA	–	Центр реагування на кіберзагрози
ПЗ	–	програмне забезпечення
СУБД	–	система управління базами даних
ТЗ	–	технічне завдання

ЗМІСТ

ВСТУП

В умовах зростання масштабів кібератак, гібридної агресії з боку рф та активної цифровізації державного управління, питання захисту державних інформаційних ресурсів (ДІР), що обробляються в системах критичної інфраструктури (КІ), набуває особливого стратегічного значення. Одним із ключових елементів даної інфраструктури виступають системи електронного документообігу (СЕДО), які забезпечують оперативний обмін та збереження інформації у державному секторі. Тематика кваліфікаційної роботи висвітлена на прикладі систем електронного документообігу, як одного з критично важливих компонентів цифрової державної інфраструктури. Актуальність теми зумовлена низкою ключових факторів, зокрема сучасними викликами у сфері кібербезпеки, воєнним станом в Україні та необхідністю адаптації до стандартів ЄС у межах євроінтеграційного курсу держави.

Розглянемо дані ключові фактори.

1. Критична важливість інформаційних ресурсів та інфраструктури.

Державні інформаційні ресурси [1] є основою функціонування будь-якої держави, а їхня безпека – запорукою національної безпеки та стабільності. Коли мова йде про критичну інфраструктуру (енергетика, транспорт, зв’язок, фінанси, водопостачання тощо), ці ресурси набувають стратегічного значення. В Україні діє Закон України «Про критичну інфраструктуру», в якому визначені правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки [2].

Вихід з ладу або компрометація таких систем може призвести до:

- масштабних техногенних катастроф, прикладами яких є зупинка енергопостачання, порушення роботи транспорту, що загрожує життю та здоров’ю громадян та т.ін.;
- соціального хаосу, якій несе за собою втрату довіри до державних інститутів, паніки серед населення;

- значних економічних збитків;
- підриву обороноздатності держави, особливо в умовах, коли ворог активно використовує кібератаки як елемент гібридної війни.

2. Залежність від СЕДО.

Сучасні державні органи та підприємства критичної інфраструктури активно переходять на електронний документообіг. СЕДО стають невід'ємною частиною їхньої повсякденної діяльності, обробляючи та зберігаючи величезні обсяги критично важливої інформації.

До такої інформації відносяться:

- конфіденційні дані, а саме службова інформація, персональні дані співробітників та громадян, фінансові операції;
- управлінські рішення, до яких відносяться протоколи засідань, накази, розпорядження, стратегічні плани;
- технічна документація – схеми, креслення, проєктні рішення, що стосуються роботи об'єктів критичної інфраструктури (КІ).

Таким чином, СЕДО фактично є серцем інформаційного обміну в даних структурах. Їхня компрометація або збій можуть призвести до:

- витоку конфіденційної інформації, що може бути використана ворогом або зловмисниками;
- порушення цілісності та автентичності документів, що ставить під сумнів легітимність рішень та операцій;
- блокування роботи організації через відсутність доступу до життєво важливих документів, що паралізує ухвалення рішень та оперативне реагування.

3. Зростання кіберзагроз та агресія рф.

Особливої актуальності тема набуває в умовах повномасштабної війни, розв'язаної рф проти України. Кібератаки є невід'ємною частиною гібридної агресії, спрямованої на: дестабілізацію державних інститутів, руйнування критичної інфраструктури, збір розвідувальної інформації, створення паніки та підрив довіри.

Атаки на КІ [3], яка містить важливу інформацію та забезпечує життєво важливі процеси, є однією з пріоритетних цілей для ворога. Тому розробка ефективних моделей захисту є прямим внеском у кіберстійкість держави.

4. Необхідність системного підходу до захисту.

Існує велика кількість засобів та підходів до захисту інформації критичної інфраструктури. Однак їхній хаотичний вибір або впровадження без належного аналізу та моделювання може бути неефективним, дорогим і навіть створювати нові вразливості.

Модель вибору та аналізу комплексу засобів захисту дозволяє:

- систематизувати процес ідентифікації ризиків та вибору адекватних засобів захисту;
- об’єктивно оцінити ефективність вже існуючих або потенційних захисних механізмів;
- оптимізувати витрати на кібербезпеку, інвестуючи в найбільш ефективні рішення;
- забезпечити відповідність національним та міжнародним стандартам і вимогам законодавства у сфері захисту інформації в КІ.

5. Практичне значення для України.

В умовах євроінтеграції та цифровізації, Україна активно працює над адаптацією до європейських стандартів кібербезпеки та підвищенням стійкості своїх інформаційних систем. Результати даної бакалаврської роботи можуть стати практичною основою для:

- розробки методичних рекомендацій для державних органів та суб’єктів КІ щодо захисту їхніх СЕДО;
- підвищення кваліфікації фахівців з кібербезпеки;
- формування національних політик та стратегій у сфері захисту ДІР КІ;

Таким чином, обрана тема має конкретну суспільну та державну цінність, сприяючи зміцненню національної кібербезпеки та забезпеченню стабільного функціонування критичної інфраструктури України.

Мета кваліфікаційної роботи полягає у розробці моделі для вибору та аналізу комплексу засобів захисту державних інформаційних ресурсів критичної інфраструктури, що обробляються в системах електронного документообігу.

Об’єктом дослідження є процес вибору та аналізу комплексу засобів захисту систем електронного документообігу державних інформаційних ресурсів критичної інфраструктури.

Предметом дослідження є моделі, методи та засоби захисту систем електронного документообігу як складової критичної інфраструктури.

Для досягнення поставленої мети потрібно вирішити наступні завдання:

4. Проаналізувати існуючі підходи, стандарти та нормативно-правову базу щодо захисту державних інформаційних ресурсів та критичної інфраструктури, з особливим акцентом на вимоги до безпеки систем електронного документообігу.

5. Розглянути основні категорії засобів захисту інформації релевантних для систем електронного документообігу.

6. Розробити модель вибору засобів захисту, що враховує специфіку роботи систем електронного документообігу з державними інформаційними ресурсами та їх інтеграцію в критичну інфраструктуру.

Апробація результатів роботи та публікації. Результати, отримані в межах дослідження, були апробовані на міжнародних науково-практичних конференціях та опубліковані у відповідних наукових виданнях. До опублікованих матеріалів належать:

1. S. Toliupa, S. Buchyk, O. Kulinich, O. Buchyk. PROTECTION OF STATE MANAGEMENT OF CRITICAL INFRASTRUCTURE OBJECTS UNDER THE INFLUENCE OF CYBER ATTACKS. Інфокомунікаційні технології та електронна інженерія, Вип. 2, № 2, 2022. – С. 33–41. – Режим доступу: http://ictee.arleons.com/?journal=ictee&page=issue&op=view&path%5B%5D=ictee-2-2-22&path%5B%5D=ictee-2-2-22-st4-en (DOI: https://doi.org/10.23939/ictee2022.02.033);

2. Buchyk O., Toliupa S. Regulatory and legal support for the selection of a set of means to protect state information resources of critical infrastructure (Satellite): Conference Proceedings, November 21, 2024, Kyiv, Ukraine / Ministry of Education and Science of Ukraine, Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). – Kyiv: Publishing House «Caravela», 2024. pp. 110-111.

Окремо варто зазначити, що здобувач, автор даної роботи, має практичний досвід у сфері функціонування систем електронного документообігу. Протягом кількох років він виконував обов’язки адміністратора СЕДО «SCHRIFT», що підтверджується відповідним сертифікатом та додатком до нього, які наведені у додатку Г та Д кваліфікаційної роботи.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА РОЛІ СЕДО

1.1 Концепція критичної інфраструктури та її інформаційних ресурсів

У контексті стрімкого розвитку технологій та поглиблення глобалізаційних процесів, належне функціонування сучасних держав, їхнього економічного потенціалу та соціального добробуту визначається надійністю та безперебійністю роботи складних, взаємопов’язаних систем. Серед означених систем, КІ посідає особливе місце, оскільки являє собою сукупність об’єктів, систем, мереж, активів та процесів, виведення з ладу або руйнування котрих здатне спричинити катастрофічні наслідки для національної безпеки, економічної стабільності, суспільного порядку та життєдіяльності населення. Тому даний аспект, що, своєю чергою, безпосередньо впливає на стійкість функціонування держави, має бути ключовим у сучасних безпекових дослідженнях.

Зважаючи на критичну важливість цих систем, виникає потреба в чіткому визначенні та класифікації їхніх складових. Відповідно до національного законодавства України у сфері захисту критичної інфраструктури, а саме постанови № 1109 Кабінету Міністрів України «Деякі питання об’єктів критичної інфраструктури» від 9 жовтня 2020 р. [4], визначено вичерпний перелік секторів КІ, їхніх підсекторів, типів основних послуг, надання яких є життєво важливим, а також зазначено секторальні органи у сфері захисту КІ. Відповідно до даної класифікації щодо основних секторів критичної інфраструктури належать наступні, наведені у таблиці 1.1.

Таблиця 1.1

Перелік секторів критичної інфраструктури

№	Сектор	№	Сектор
1.	Паливно-енергетичний сектор	13.	Цивільний захист населення і територій
2.	Цифрові технології	14.	Охорона навколишнього природного середовища
3.	Захист інформації	15.	Сектор оборони
4.	Харчова промисловість та агропромисловий комплекс	16.	Правосуддя
5.	Державний матеріальний резерв	17.	Виконання кримінальних покарань, тримання під вартою та утримання військовополонених
6.	Охорона здоров’я	18.	Державна реєстрація
7.	Ринки капіталу та організовані товарні ринки	19.	Наукові дослідження та розробки.
8.	Фінансовий сектор (секторальний орган - Мінфін)	20.	Фінансовий сектор (секторальний орган - Національний банк)
9.	Транспорт і пошта	21.	Вибори та референдуми
10.	Системи життєзабезпечення	22.	Соціальний захист
11.	Промисловість	23.	Інформаційний медіа сектор
12.	Сектор громадської безпеки	24.	Державна влада

Проте незалежно від конкретної галузевої приналежності та спектру послуг, функціонування кожного із зазначених секторів КІ, у свою чергу, базується на обробці та зберіганні значних обсягів інформаційних ресурсів. Саме ці дані, відомості та знання, що циркулюють у цифрових системах, формують основу для прийняття рішень, управління процесами та надання життєво важливих послуг. Таким чином, проаналізувавши загальну характеристику секторів КІ, особливу увагу необхідно приділити дефініції та класифікації ДІР, які є безпосереднім об’єктом захисту. Під ДІР, у контексті даної роботи, слід розуміти будь-яку інформацію (дані, відомості, знання), що створюється, обробляється, накопичується, зберігається або передається державними

органами, а також підприємствами, установами та організаціями, що належать до державної власності, або діють від імені держави. У контексті функціонування КІ, ДІР не є просто пасивними даними, вони виступають як ключові активи, які забезпечують оперативне, стратегічне та адміністративне управління життєво важливими системами.

До ключових інформаційних ресурсів КІ належить розгалужена сукупність даних, що є фундаментальними для їхнього безперебійного функціонування та стійкості. По-перше, це операційні та телеметричні дані систем SCADA/ICS, котрі включають критичні показники сенсорів, детальні журнали подій та параметри технологічних процесів. Дана інформація є основою для віддаленого контролю та управління об’єктами КІ, забезпечуючи їх стабільну роботу, що, своєю чергою, запобігає аварійним ситуаціям.

По-друге, до ДІР належить управлінська та адміністративна інформація, яка охоплює нормативні документи, законодавчі акти, плани реагування на надзвичайні ситуації, протоколи засідань, накази, а також розпорядження та стратегічні плани розвитку усіх секторів КІ. Цей масив даних є життєво важливим для координації діяльності та забезпечення ефективності державного управління.

Третім важливим типом є персональні дані, що стосуються як співробітників об’єктів КІ, так і користувачів послуг, які надаються цією інфраструктурою. Захист цих даних має підвищене значення, оскільки вони підлягають особливому захисту згідно з національним законодавством та міжнародними стандартами.

Четвертою значною категорією виступає технічна та проєктна документація. До її складу входять детальні схеми мереж, інженерні проєкти, технічні паспорти об’єктів КІ, а також відомості про використовуване обладнання та програмне забезпечення. Ця інформація є не просто архівом, а основою для експлуатації, модернізації та відновлення критичних систем.

П’ятим аспектом є фінансова та економічна інформація, що охоплює дані про бюджетні асигнування, фінансові транзакції, інвестиційні проєкти та

облікові відомості. Її цілісність та конфіденційність безпосередньо впливають на економічну стабільність функціонування секторів КІ та національної економіки в цілому.

Нарешті, ключовим ресурсом є інформація про кіберзагрози та інциденти безпеки, що є зведенням про виявлені кібератаки, відомі вразливості та зафіксовані інциденти безпеки, що дозволяє не лише реагувати на поточні загрози, але й постійно вдосконалювати системи захисту, адаптуючи її до нових викликів. Кожен з цих типів інформаційних ресурсів потребує специфічних підходів до захисту, що і обумовлює необхідність розробки ефективної моделі вибору та аналізу відповідних засобів.

Високий ступінь інтеграції та взаємозалежності, притаманний сучасній критичній інфраструктурі, формує специфічні ризики. Так, порушення функціонування інформаційних систем в одному секторі КІ, наприклад, внаслідок цілеспрямованої кібератаки на енергетичну систему, здатне спричинити каскадні ефекти та призвести до системних збоїв в інших секторах, таких як транспорт або зв’язок, що, своєю чергою, може мати значні наслідки. Дана взаємозалежність багаторазово підвищує загальну вразливість усієї системи до кібератак, оскільки компрометація інформаційних ресурсів в одному сегменті може мати деструктивний вплив на інші.

Такі системні вразливості, що мають здатність спричиняти реальні фізичні наслідки, були яскраво продемонстровані під час кібератаки на українські енергопостачальні компанії у грудні 2015 року [5], яка стала однією з перших у світі публічно визнаних успішних кібератак, що призвела до фізичного відключення об’єктів критичної інфраструктури та значних перебоїв в енергопостачанні. Атака була ретельно спланована і тривала кілька місяців. Вона здійснювалася за допомогою варіанту шкідливого програмного забезпечення (ШПЗ) «BlackEnergy 3». Основним вектором проникнення були цільові фішингові електронні листи (spear-phishing), які містили шкідливі вкладення, часто у вигляді документів Microsoft Office (Excel, PowerPoint, Word) з

вбудованими макросами. Відкриття таких документів співробітниками енергетичних компаній призводило до зараження їхніх робочих станцій.

Після початкового компрометування зловмисники, ідентифіковані як група «Sandworm» (яку пов'язують з російськими спецслужбами), використовували «BlackEnergy 3» для встановлення постійного доступу до корпоративних мереж, розвідки IT та операційних технологічних мереж, викрадення облікових даних користувачів з високими привілеями, а також для горизонтального переміщення всередині систем, що дозволило їм отримати контроль над системами промислового контролю та управління (SCADA/ICS), зокрема над інтерфейсами управління операторів.

Безпосереднє відключення електропостачання відбулося 23 грудня 2015 року. Хакери віддалено авторизувалися на робочих станціях операторів трьох українських обленерго (зокрема, «Прикарпаттяобленерго» та «Київобленерго») і, використовуючи легітимні інструменти управління, почали відключати електричні підстанції. Зокрема, у випадку «Прикарпаттяобленерго» було відключено близько 30 підстанцій та знеструмлено близько 225 – 230 тисяч споживачів, які залишалися без електроенергії від 1 до 6 годин.

Окрім безпосереднього відключення електроенергії, кібератака включала низку додаткових етапів, спрямованих на ускладнення процесу відновлення роботи енергетичної інфраструктури. Зокрема, зловмисники виводили з ладу елементи IT-інфраструктури за допомогою деструктивного ШПЗ «KillDisk», яке знищувало дані на серверах та робочих станціях, а також виводило з ладу критичні компоненти, такі як джерела безперебійного живлення, модеми та комутатори шляхом перезапису їхнього вбудованого програмного забезпечення. Дані дії суттєво ускладнювали перезавантаження систем і повернення їх до штатного режиму функціонування. Додатково здійснювалися атаки на кол-центри у формі Telephone Denial of Service (TDoS), що блокувало телефонні лінії енергетичних компаній і позбавляло споживачів можливості повідомляти про відключення або отримувати актуальну інформацію. У деяких випадках також повідомлялося про фізичні втручання, зокрема вимкнення аварійного живлення

в операційних центрах, що унеможливлювало ручне управління системами та ще більше ускладнювало процес реагування.

Відтак, даний інцидент слугує переконливим прикладом реалізації каскадних ефектів та підкреслює критичну взаємозалежність інформаційних систем у масштабах КІ.

Впровадження ефективної системи захисту є ключовим аспектом саме для мінімізації подібних ризиків та забезпечення стійкості функціонування КІ. Таким чином, захист інформаційних ресурсів КІ, базується на фундаментальних властивостях інформаційної безпеки (тріада CIA, або КЦД):

- конфіденційність, що забезпечує доступність інформації виключно авторизованим суб'єктам (несанкціоноване розголошення може призвести до непоправних стратегічних втрат);
- цілісність, що забезпечує повноту, точність та достовірність інформації, а також її методів обробки (несанкціонована модифікація або руйнування даних може спричинити критичні помилки у прийнятті рішень або збоїв у технологічних процесах);
- доступність, що забезпечує своєчасний та надійний доступ авторизованих користувачів до інформації та необхідних ресурсів. Відмова в обслуговуванні може призвести до паралічу життєво важливих функцій.

Будь-яке порушення одного з цих принципів може призвести до низки серйозних наслідків, починаючи від значних фінансових втрат та репутаційних ризиків, і закінчуючи загрозою життю та здоров'ю населення, а також підривом національної безпеки. З огляду на зазначене, розробка та впровадження комплексного й системного підходу до захисту ДІР КІ є не просто бажаною практикою, а життєво необхідним імперативом для забезпечення стабільного функціонування держави в умовах сучасних кіберзагроз.

1.2 Системи електронного документообігу як об'єкт захисту в критичній інфраструктурі

У сучасному державному управлінні та функціонуванні секторів критичної інфраструктури, що характеризуються високим рівнем цифровізації, СЕДО набули статусу невід'ємного та стратегічно важливого компонента. Дана трансформація зумовлена не лише прагненням до оптимізації адміністративних процесів та підвищення ефективності взаємодії, але й нагальною необхідністю забезпечення відповідності сучасним вимогам щодо оперативності, прозорості та контрольованості інформаційних потоків у динамічному середовищі. СЕДО являють собою комплекс програмно-апаратних засобів, організаційних регламентів та методичних рішень, призначених для всебічного управління електронними документами протягом усього їхнього життєвого циклу, що включає процеси створення, реєстрації, обробки, узгодження, візування, підписання (зокрема, з використанням кваліфікованого електронного підпису), виконання, моніторингу, зберігання, пошуку та архівування документів. Їхнє впровадження дозволяє не тільки раціоналізувати адміністративні процеси та значно підвищити швидкість обміну інформацією, але й забезпечити її централізоване зберігання, а також можливість детального аудиту на всіх етапах життєвого циклу документа, що є критично важливим для забезпечення прозорості та підзвітності.

В умовах функціонування КІ, що постійно знаходиться під загрозою зовнішніх та внутрішніх деструктивних впливів, роль СЕДО набуває особливого, першочергового значення. Вони еволюціонували з простих інструментів для оцифрування паперових архівів у критично важливі інформаційні системи, через які здійснюється управління життєво необхідними процесами. Кожен документ, що циркулює у СЕДО об'єкта КІ – від договорів та оперативних звітів до стратегічних рішень щодо кіберзахисту – містить потенційні ризики у випадку його компрометації, що зумовлює їхню високу привабливість для зловмисників.

У рамках даного дослідження, що зосереджене на моделі вибору та аналізу засобів захисту ДІР КІ, особливу увагу необхідно приділити принципам функціонування та архітектурним особливостям СЕДО, які безпосередньо впливають на її захищеність та стійкість до загроз. Типові СЕДО, розробляються

з урахуванням нагальних потреб сучасного документообігу та вимог до інформаційної безпеки. Вони є складними інтегрованими інформаційними комплексами, покликаними забезпечити повний перехід від традиційного, паперового діловодства до повністю електронного формату, що відповідає концепції «безпаперового офісу» та «цифрової держави». Їхній функціонал охоплює усі без винятку стадії життєвого циклу документа, починаючи від його ініціації (створення) або надходження до організації, подальшої офіційної реєстрації, автоматизованої маршрутизації за визначеними бізнес-процесами, візування та узгодження з усіма зацікавленими сторонами, юридично значущого підписання (найчастіше із застосуванням кваліфікованого електронного підпису, або ж внутрішнього підпису системи), ефективного контролю за виконанням і, на завершення, його довгострокового зберігання та архівування з дотриманням нормативних вимог.

Впровадження СЕДО для ДІР КІ в Україні має свої унікальні особливості, зумовлені геополітичною ситуацією, постійними кіберзагрозами, динамічним законодавством та потребою в технологічній незалежності, що вимагає комплексного та продуманого підходу до імплементації таких критично важливих систем. Ключові аспекти, які необхідно брати до уваги, наведено у таблиці 1.2.

Таблиця 1.2

Ключові аспекти впровадження СЕДО в ДІР КІ

№	Аспект	Характеристика
1.	Посилена кіберстійкість та безпека в умовах воєнного стану	В умовах повномасштабної агресії з боку рф та постійних кібератак, СЕДО для ДІР КІ має бути максимально захищеною, що означає не просто базове шифрування, а багаторівневий захист, що включає системи виявлення вторгнень (IDS/IPS), системи управління подіями безпеки (SIEM) для моніторингу в реальному часі, та активне використання кіберрозвідки для передбачення загроз. Необхідно враховувати ризики фізичних атак на інфраструктуру, тому розгортання системи у географічно розподілених дата-центрах, зокрема за межами України (з дотриманням

Продовження таблиці 1.2

		законодавчих вимог щодо обробки даних), є критично важливим для забезпечення безперервності роботи. Розробка сценаріїв для офлайн-можливостей та швидкого відновлення після збоїв, а також підтримка «гарячої» заміни є обов’язковими для забезпечення безперебійності функціонування.
2.	Динамічне законодавче та нормативно-правове поле	Українське законодавство у сферах кібербезпеки та захисту інформації електронних довірчих послуг постійно змінюється та доповнюється. СЕДО для ДІР КІ повинна бути максимально гнучкою та адаптивною до цих змін, щоб забезпечувати безперервну відповідність, що включає не лише відповідність Законам України "Про захист інформації в інформаційно-телекомунікаційних системах" та "Про електронні довірчі послуги", а й усім відповідним постановам Кабінету Міністрів України, національним стандартам та рекомендаціям, висвітленим у даній роботі. Використання кваліфікованого електронного підпису (КЕП) є невід’ємною частиною легітимізації електронних документів, і СЕДО повинна забезпечувати безшовну інтеграцію з усіма основними акредитованими центрами сертифікації ключів (АЦСК) в Україні.
3.	Технологічна незалежність та імпортозаміщення	В умовах геополітичної нестабільності, пріоритетним є використання українських програмних продуктів та рішень для СЕДО, дозволяючих зменшити залежність від іноземних постачальників, що є критично важливим для ДІР КІ, а також забезпечує відповідність національним вимогам до захисту інформації. Системи, що пройшли державну експертизу в галузі захисту інформації, мають перевагу. Впровадження рішень на базі відкритих стандартів також сприяє технологічній незалежності, оскільки уникнення «прив’язки» до одного вендора забезпечує гнучкість та можливість подальшого розвитку системи.
4.	Кадрові та організаційні виклики	В Україні існує дефіцит кваліфікованих фахівців у сфері інформаційної безпеки та розробки СЕДО. Це вимагає інвестицій у навчання та перекваліфікацію персоналу, а також створення сприятливих умов для залучення та утримання талантів. Підтримка та вмотивованість на рівні вищого керівництва є абсолютно критичною для успіху проєкту, оскільки

Продовження таблиці 1.2

		впровадження СЕДО часто вимагає перегляду та оптимізації існуючих бізнес-процесів, що може зіткнутися з опором. Ефективна комунікація та навчання персоналу є ключовими для подолання «психологічного бар'єру» та підвищення довіри до нових цифрових інструментів.
5.	Оптимізація ресурсів та фінансування	Державні установи часто працюють в умовах обмежених бюджетів, що вимагає ретельного планування та обґрунтування інвестицій у СЕДО. Важливо шукати ефективні рішення, які забезпечують максимальний результат при оптимальних витратах. Водночас, можливість залучення грантів та допомоги від міжнародних партнерів для фінансування проєктів з кібербезпеки та цифровізації є важливою складовою стратегії. Такі кошти можуть суттєво прискорити та покращити процес впровадження.

1.2.1 Основні функціональні можливості СЕДО

Відповідно до зазначених вище тверджень сучасна СЕДО функціонує не лише як сховище для електронних документів, а є комплексним інтегрованим інструментом, що забезпечує автоматизацію всіх фаз їхнього життєвого циклу. Для ДІР КІ, де пріоритетними є оперативність, прецизійність та кіберстійкість, імплементація СЕДО вимагає реалізації низки ключових функціональних можливостей, які можна розділити на чотири логічні складові (рис.1.1).

1. Введення та ініціація документів

Функціонування СЕДО починається з етапу введення та ініціації документів, який слугує точкою входу для всієї подальшої інформації. Даний блок охоплює процеси, пов'язані як з надходженням зовнішньої кореспонденції, так і зі створенням внутрішніх документів.

Основною тут є підсистема обробки та обліку вхідних документів. Вона забезпечує гнучкість у методах реєстрації, підтримуючи як ручну, так і автоматичну реєстрацію вхідної кореспонденції. Це дозволяє оптимізувати процес залежно від обсягів та джерела надходження документів. До кожної

реєстраційно-моніторингової картки (РМК) система дозволяє прикріплювати довільну кількість електронних документів та/або їх електронних образів (файлів), що створює єдиний інформаційний простір для кожного елементу кореспонденції. Для підвищення ефективності, СЕДО інтегрує технологію drag-and-drop, яка дозволяє швидко заповнювати атрибути картки документа, попередньо відсканованого та розпізнаного, без повторного вводу даних та з мінімальним використанням клавіатури. Це значно прискорює процес реєстрації.

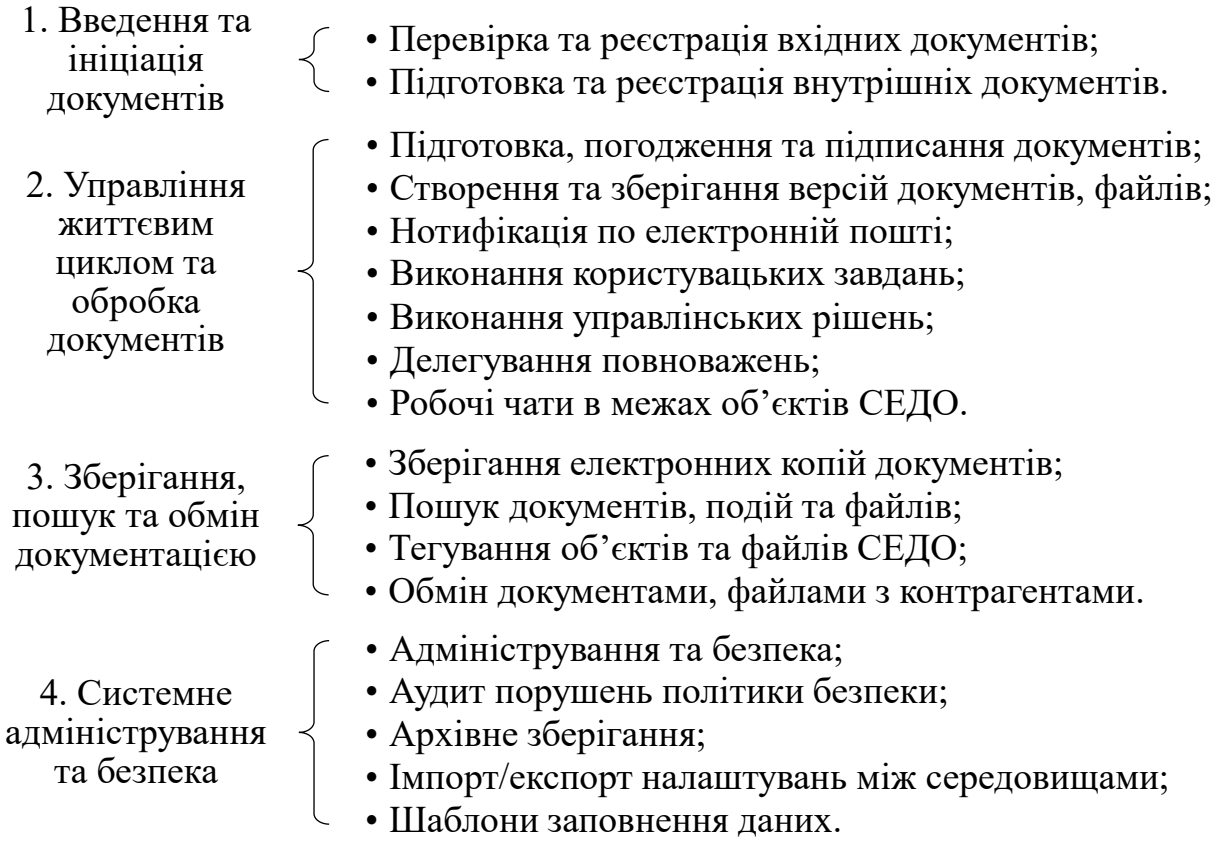


Рисунок 1.1 – Логічні складові функціональних можливостей СЕДО

Система також надає можливість доповнення довідника кореспондентів безпосередньо із функції реєстрації, що забезпечує актуальність бази даних. Після реєстрації СЕДО автоматично здійснює доставку вхідної кореспонденції безпосередньо адресату, а також за необхідності дозволяє постановку на контроль документа. Підсистема підтримує делегування повноважень у рамках обробки вхідних документів, дозволяє встановлення відмітки про виконання

доручень та відмітки про виконання документа в цілому. Для ефективної роботи передбачена розсилка (переадресація) отриманої кореспонденції, формування та ведення реєстру вхідної документації, а також здійснення пошуку документів за будь-якою кількістю атрибутів, включаючи повнотекстовий пошук, з можливістю друку знайденої інформації. Важливою є історія роботи з документами та можливість формування та друку необхідних звітів та реєстрів.

Паралельно функціонує підсистема обробки та обліку вихідних документів. Вона також підтримує ручну та автоматичну реєстрацію вихідних документів, що забезпечує гнучкість у процесі їх відправлення. Ключові етапи, такі як узгодження та підписання вихідних документів, інтегровані в систему для забезпечення їх юридичної значимості. СЕДО дозволяє відправлення вихідних документів, у тому числі за попередньо налаштованими схемами розсилання. Як і для вхідної кореспонденції, система забезпечує формування та ведення реєстру вихідної документації, здійснення пошуку документів за будь-якою кількістю атрибутів, включаючи повнотекстовий пошук, з можливістю друку результатів. Також підтримується ведення історії роботи з документами та формування й друк необхідних звітів та реєстрів.

Особливе місце посідає підсистема обробки та обліку внутрішніх документів, що включає організаційно-розпорядчі документи. Вона надає функціонал для введення та реєстрації наказів, доручень, розпоряджень та протоколів. Однією з унікальних можливостей є створення розпорядчих документів з розділенням розпорядчої частини на пункти та/або підпункти з можливістю встановлення та подальшого контролю виконання по кожному пункту окремо. Ці документи проходять всі етапи підготовки, погодження, підписання і розсилки виконавцям. СЕДО забезпечує невід’ємність образу документа та атрибутів електронної картки для автоматичного формування візуального образу документа на підставі його картки, що забезпечує відповідність електронної форми паперовій.

2. Управління життєвим циклом та обробка документів

Виконання завдань, управлінських рішень та документів є центральною функцією даного блоку. СЕДО надає гнучкі можливості для створення завдань за пунктами структурованого документа, що дозволяє чітко розподіляти обов'язки. Система дозволяє надавати доступ до файлів необмеженій кількості співробітників/контрагентів, а також створювати завдання для певних посад (співробітників) та конкретних контрагентів. Завдання можуть бути створені як етапи обробки документів згідно з їх діловим процесом, що забезпечує автоматизацію «workflow». Система передбачає можливість створення завдань з терміном виконання, а також автоматичне створення періодично повторюваних завдань. Для управління процесом виконання, СЕДО дозволяє перенесення термінів виконання завдань із зазначенням причини та фіксацією факту перенесення у системному журналі. Система підтримує відправку документа до відома та фіксацію факту виконання завдання з можливістю введення звіту та описом результатів. Особливістю є ведення версій документа, що дозволяє відстежувати проходження процесу обробки та дії на кожному етапі, а також автоматичне закриття одного документа іншим (накладання крайньої версії на попередню). Для зручності користувачів, СЕДО дозволяє налагодження відображення переліку завдань з використанням фільтрів та угрупувань за різними критеріями. Функціонал делегування завдань іншим виконавцям забезпечує безперервність роботи, а пошук завдань за набором атрибутів картки спрощує навігацію. Також система забезпечує формування звітів з інформацією про стан виконання документів та переліку завдань з групуванням за терміном, виконавцем та контролером. Важливо, що при змінах в організаційній структурі, адміністратор може переносити або копіювати доступи/права по документам та переносити завдання по документам з однієї посади на іншу.

Контроль виконання завдань, управлінських рішень є окремою, але інтегрованою підсистемою. Вона дозволяє взяття документів (завдань) на контроль та формування картотеки цих документів. Система надає можливість встановлення у документа ознаки особливого контролю, при цьому автоматично створюється задача контролю документа в цілому. Можливе також ручне

створення задачі контролю з обов’язковим зазначенням конкретного завдання. СЕДО забезпечує нотифікацію виконавців про надання доступу до файлів через електронну пошту, а також перевірку своєчасного доведення документів до виконавців. Передбачена попередня перевірка та регулювання ходу виконання, а також інформування керівника та інших зацікавлених осіб про хід і підсумки виконання. Система дозволяє зняття документів з контролю та автоматичну фіксацію подій з документом у журналі аудиту. Контроль може бути як ручний (підтвердження виконання автором задачі), так і автоматичний (нотифікації про наближення/прострочення дедлайну, повідомлення керівника про прострочені завдання). Система також інформує автора завдань про те, що виконавець не відкривав завдання для перегляду. Для зручності, підсистема дозволяє налагодження відображення переліку документів з фільтрами та угрупуваннями за різними критеріями, пошук контрольних документів за атрибутами та формування звітів із статистично-аналітичною інформацією про стан виконання.

Підготовка, погодження та підписання документів також детально розкривається в даному блоці. СЕДО дозволяє перегляд картки одночасно з образом документа та відображення змін атрибутів на образі документа при його редагуванні. Документи можуть бути візуалізовані та збережені у форматі PDF. Важливою є функція зберігання документів, що перебувають на етапі підготовки, у базі даних до їх відправки в роботу. Система підтримує створення нових проєктів документів на основі шаблонів, що налаштовуються для кожного типу документа та користувача/групи. Обов’язковою є підтримка контролю версій та можливість спільної роботи з документом. СЕДО дозволяє визначення маршруту виконання операцій (візування і/або підписання) над документом та автоматичну фіксацію подій у журналі аудиту. Функція погодження документів надає такі можливості: побудову та збереження маршрутів візування/підписання як шаблонів, накладення електронно-цифрового підпису в ході візування/підписання, внесення коментарів та зауважень, паралельне або послідовне візування, повернення документа на доопрацювання ініціатору, повідомлення на електронну пошту про надходження документів на

візування/підписання, а також погодження документа через інтерфейс поштового повідомлення (без входу до СЕДО, якщо не потрібен КЕП). Усі ці дії також автоматично фіксуються у журналі аудиту.

Створення та зберігання версій документів, файлів є наскрізною функцією. СЕДО підтримує спільну роботу (через механізм створення нових версій) над окремим або кількома документами. Вона забезпечує впорядковане зберігання та автоматичне формування переліку версій документів з можливістю перегляду попередніх версій. Для уникнення конфліктів підтримується блокування документа для внесення змін іншим користувачам, а також паралельне редагування, погодження та доопрацювання документів через механізм створення нових версій.

3. Зберігання, пошук та обмін інформацією

Зберігання електронних копій документів є фундаментальною можливістю. СЕДО забезпечує збереження електронних копій у базі даних у форматі PDF, що гарантує їх універсальність та незмінність візуального представлення. Система дозволяє перегляд електронних копій документів, а також налагодження відображення переліку документів з використанням фільтрів та угрупувань за різними критеріями та пошук документів за набором атрибутів.

Функція шаблонів заповнення даних значно прискорює та уніфікує процес створення документів. СЕДО надає можливості автоматичного заповнення атрибутів документа в залежності від обраного виду документа. Крім того дозволяється створення та збереження маршрутів візування/підписання документів, шаблонів передач документів, переліку співробітників для ознайомлення, шаблонів заповнення форми резолюції, текстів резолюцій, а також переліку виконавців завдань із зазначенням їх ролі, що забезпечує високий рівень автоматизації та стандартизації. Нотифікація по електронній пошті забезпечує своєчасне інформування користувачів. СЕДО автоматично оповіщає про призначення завдань (з прямим посиланням на завдання), попередження про закінчення терміну виконання, повідомлення про невиконане завдання після

дедлайну, а також про будь-які зміни в документах, в роботі над якими залучений поточний користувач (додавання, зміна, видалення). Передбачено налагодження оповіщень для окремих користувачів або груп та налагодження часу оповіщення (негайно, щодня, щотижня).

Пошук документів, подій та файлів є потужним інструментом для швидкого доступу до інформації. СЕДО дозволяє пошук документів за встановленим діапазоном значень реквізитів, відбір множини документів за певними критеріями, а також пошук за значеннями реквізитів РМК. Обмін документами, файлами з контрагентами є ключовим для зовнішньої взаємодії. СЕДО забезпечує обмін електронними документами з Системою електронної взаємодії органів виконавчої влади (СЕВ ОВВ) на основі XML-формату, визначеного відповідним Наказом Міністерства освіти і науки, молоді та спорту України від 20.10.2011 № 1207 «Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення» [6]. Підсистема обміну з СЕВ ОВВ має можливість відправки документів у автоматичному та ручному режимах, автоматичну відправку сповіщень про результат обробки, та зазначення одного із семи затверджених сценаріїв організації проходження документів (видання доручень, надсилання на погодження/відповідь, заміна, узагальнення, інформаційні документи). Обов’язковим є накладання КЕП на документ, що відправляється через СЕВ. Система також забезпечує отримання документів та сповіщень з СЕВ, перевірку їх структури та відображення даних, реєстрацію отриманого документа з автозаповненням атрибутів та формування повідомлення-сповіщення «Підтвердження про реєстрацію». Підтримується ведення переліку учасників обміну через СЕВ, що є звуженням довідника «Зовнішні організації», відправка на виконання окремих завдань зовнішнім організаціям та налаштування відправки та отримання пакетів документів з використанням електронної пошти.

4. Системне адміністрування та безпека

Адміністрування та безпека надає адміністраторам повний контроль над СЕДО, що включає ведення облікових записів користувачів, розмежування

доступу на рівні екземплярів документів та розмежування доступу до операцій над документами. Також реалізовано розмежування доступу до окремих об’єктів СЕДО (реєстрів, довідників тощо). Система дозволяє управління доступністю/недоступністю полів картки для кінцевих користувачів та налаштування видимості атрибутів на картці документа в залежності від його виду. Безпека доступу забезпечується ідентифікацією користувача за логіном, автентифікацією за паролем та підтримкою двофакторної автентифікації.

Аудит порушень політики безпеки є ключовим для контролю. СЕДО дозволяє формування та перегляд системного журналу подій та журналу операцій над документом. Система надає можливість налагодження рівнів протоколювання подій аж до фіксації всіх подій всіх користувачів, що є критично важливим для виявлення та розслідування інцидентів. Архівне зберігання документів здійснюється згідно з вимогами законодавства України. СЕДО підтримує ведення номенклатури справ, формування зведеної номенклатури та формування справ. Система забезпечує автоматизовану підготовку описів справ та зведених описів для передачі на архівне зберігання. Електронні образи документів зберігаються у єдиному форматі PDF, а також забезпечується оперативний пошук архівних документів за будь-якими реквізитами та повнотекстовий пошук.

Делегування повноважень є гнучкою функцією для забезпечення безперервності роботи. При призначенні на посаду СЕДО дозволяє вибір типу призначення: «Штатне призначення», «Виконання обов’язків», «Реферування», а також рівня доступу: «Базовий», «Конфіденційний», «Секретний». Співробітник може делегувати права безпосередньо з обов’язковим зазначенням дати початку та закінчення. Можливе розподілення делегування за видами документів (всі, загальні, з обмеженим доступом) та за рівнем доступу. Делегування може включати право погодження/підпису документів, право накладання резолюцій, отримання/передачі документів та делегування всіх прав користувача. Система забезпечує нотифікації обом сторонам про делегування та закінчення терміну повноважень. Адміністратор також може делегувати

повноваження від одного користувача іншому. При делегуванні від реєстратора до реєстратора передаються права на реєстрацію документів по журналах.

Робочі чати в межах об’єктів СЕДО сприяють ефективній комунікації. СЕДО дозволяє здійснювати обговорення в реальному часі по документу, його завданню та на етапі погодження проєкту. Можливе додавання нового користувача в обговорення з наданням йому відповідного доступу до документу. Користувачі можуть редагувати та видаляти свої повідомлення, а система забезпечує збереження історії обговорень на формі документу.

Застосування КЕП є невід’ємною частиною системи. Модуль надає механізм підпису документів та проєктів (на етапах погодження та затвердження) для уповноважених користувачів. Він здійснює перевірку цілісності юридично значущих документів, перевірку чинності сертифікатів КЕП (інтерактивна перевірка в АЦСК, завантаження списків відкликаних сертифікатів) та перегляд системного протоколу застосування КЕП. Модуль підтримує адресне шифрування документів, дозволяючи дешифрувати їх лише зазначеним користувачам, та використовує криптографічні алгоритми, сумісні з усіма АЦСК України. Власник підприємства може автоматично отримувати доступ до проєкту документа, повертати його з зауваженнями або підписувати/затверджувати. Механізм підпису забезпечує однозначну ідентифікацію посадової особи та захист від підробки/використання іншою особою. Підписання може здійснюватися з одночасною автоматичною реєстрацією, після чого документ коригуванню не підлягає та автоматично направляється адресатам. Забезпечується візуалізація (друкування) вихідного номера та дати реєстрації підписаного КЕП документа.

Виконання користувацьких завдань реалізовано з гнучкими налаштуваннями для різних типів завдань, рівнів доступу та користувацьких сценаріїв для конкретних користувачів, підрозділів та груп. Тегування об’єктів та файлів СЕДО дозволяє групування документів до багаторівневих каталогів (ієрархій) за значенням їх атрибутів, де на кожному рівні можливе групування лише по одному атрибуту (наприклад, рік, контрагент). СЕДО надає можливості

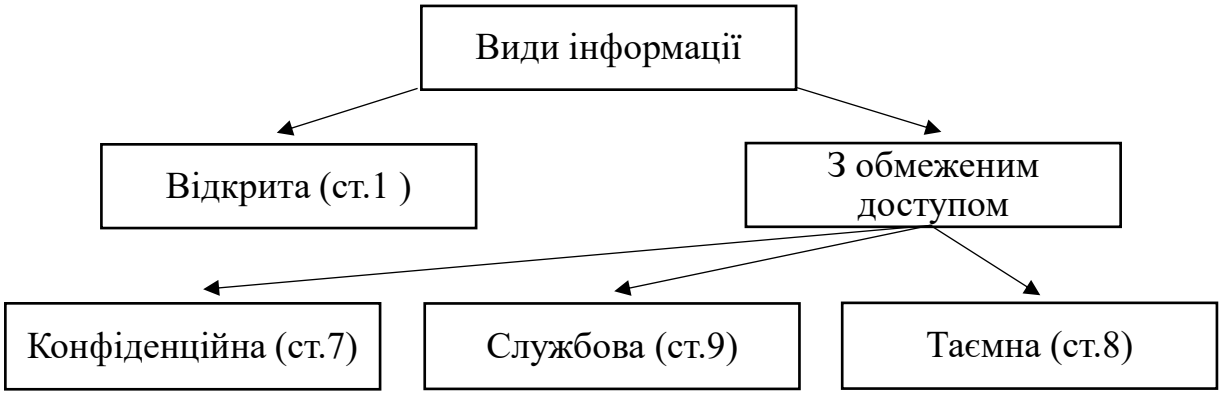
налаштування однієї або декількох ієрархій, де для кожного рівня обирається атрибут для формування каталогів. Каталоги формуються для всіх унікальних значень атрибутів. Документи автоматично групуються до наявних ієрархій при їх створенні або редагуванні за умови наявності всіх необхідних атрибутів. Система дозволяє сформувати нову або змінити існуючу ієрархію та згрупувати до неї вже наявні документи. Під час групування ієрархія не може бути змінена, а користувачам виводиться відповідне повідомлення. Для відображення, ієрархія має бути прив’язана до ярликів робочого столу, а права доступу встановлюються на рівні ярлика. У каталогах відображаються лише ті документи, до яких користувачі мають доступ, і не відображаються каталоги без доступних документів.

Імпорт/експорт налаштувань між середовищами є технічною, але критично важливою функцією для адміністрування. СЕДО дозволяє створювати необмежену кількість пакетів для експорту налаштувань, додаючи до них різні типи об’єктів системи: бібліотека атрибутів, процеси, групи атрибутів, дії, зовнішні системи та API, пошукові шаблони, правила контролю дублікатів, форми, типи документів, шаблони звітів/нотифікацій, шаблони розпізнавання, ярлики. При виборі об’єкта для експорту можна обирати екземпляр або екземпляри, а СЕДО автоматично додає всі пов’язані об’єкти. Система генерує файл пакету експорту з можливістю перегляду вмісту за типами об’єктів та екземплярами, а також перегляд графу зв’язків. Файли пакетів можна зберігати локально та імпортувати на іншому середовищі. Перед застосуванням імпортованого пакету система надає можливість перегляду його вмісту та графу зв’язків.

Дані чотири взаємопов’язані блоки функцій, від введення та обробки до зберігання, обміну та адміністрування, створюють цілісну, потужну, безпечну та ефективну СЕДО. Така система повністю відповідає високим вимогам ДІР КІ, забезпечуючи їх надійність, безперебійне функціонування та ефективне управління документацією в сучасних умовах.

1.2.2 Види інформації, що обробляється в СЕДО КІ

Задля ефективної побудови системи захисту ДІР КІ, що функціонують у СЕДО, першочерговим завданням є чітка класифікація видів інформації, яка обробляється в даних системах. Відповідно до наданої схеми (рис. 1.2) та положень Закону України «Про доступ до публічної інформації» [7], інформація поділяється на відкриту та з обмеженим доступом. Інформація з обмеженим доступом, у свою чергу, поділяється на конфіденційну, службову та таємну. Зважаючи на підвищені вимоги до захисту, у контексті використання СЕДО під час роботи з ДІР КІ особлива увага приділяється саме обробленню інформації з обмеженим доступом



Трискладовий тест є обов'язковим!
На схемі також присутні посилання на статті № 1,7,8,9 закону **№2939-VI**

Рисунок 1.2 – Схематичне зображення видів інформації

Як видно з представленої схеми:

Відкрита інформація включає публічну інформацію, доступ до якої є вільним, за винятком випадків, прямо встановлених законодавством. До неї належать загальнодоступні відомості, які не містять обмежень щодо поширення.

Інформація з обмеженим доступом, на відміну від відкритої, потребує спеціального правового режиму захисту, оскільки її розголошення, зміна або

втрата можуть завдати шкоди інтересам держави, юридичним чи фізичним особам. Вона, зі свого боку, поділяється на наступні підкатегорії:

- конфіденційна інформація, до якої відносяться відомості про фізичних та юридичних осіб, які не є суб'єктами владних повноважень. Доступ до такої інформації обмежений відповідно до чинного законодавства, і її розкриття може призвести до порушення прав та інтересів цих осіб;
- службова інформація, до якої належить внутрішньовідомча службова кореспонденція, а також інформація, зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни. Доступ до службової інформації обмежується для забезпечення ефективного виконання функціональних обов'язків відповідними державними органами та структурами;
- таємна інформація - категорія охоплює державну, професійну, банківську таємницю, таємницю досудового розслідування, а також інші види таємниць, передбачених законом. Доступ до таємної інформації є найбільш суворо регламентованим, а її компрометація може мати значні наслідки для національної безпеки, державного управління або функціонування фінансової системи.

Важливо зауважити, що на схемі також зазначено застосування «Трискладового тесту» [7], який є обов'язковим для оцінки можливості обмеження доступу до інформації або її розкриття у випадках, коли йдеться про відкриту інформацію. Застосування даного тесту дозволяє збалансувати право на доступ до інформації з необхідністю її захисту.

1.3 Нормативно-правова база та стандарти захисту інформації в критичній інфраструктурі та вимоги до СЕДО

Даний підрозділ розглянемо у розрізі трьох складових, які представлені на рисунку 1.3.

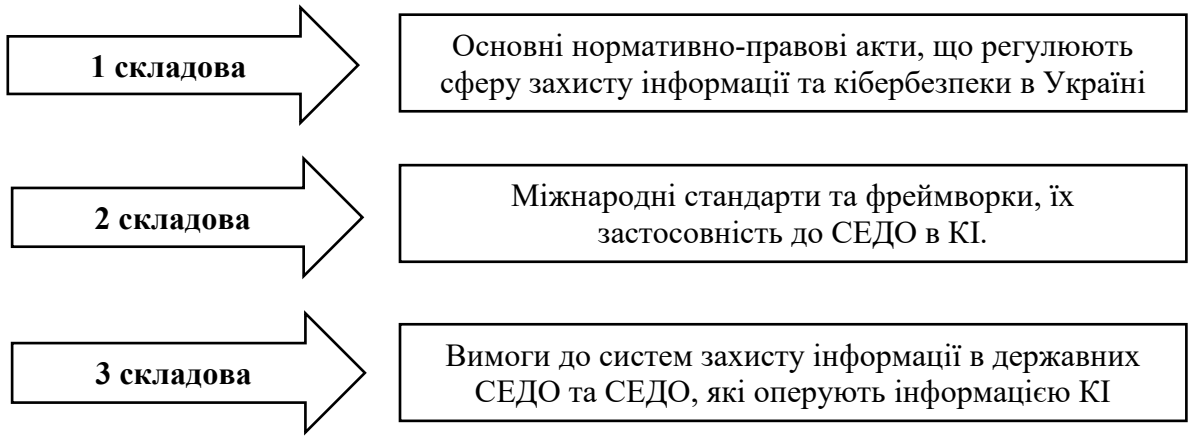


Рисунок 1.3 – Представлення трьох складових нормативно-правової бази та стандартів захисту інформації в критичній інфраструктурі, вимог до СЕДО

Законодавство України у сфері захисту інформації та кібербезпеки є динамічним та постійно адаптується до нових викликів. До основних нормативно-правововых актів, що регулюють ці питання, відноситься (складова 1, рис.1.2).

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» [8]. Цей закон є базовим і визначає правові, організаційні та технічні засади захисту інформації в інформаційно-комунікаційних системах.

Стаття 1. Визначає основні терміни, зокрема «захист інформації», «інформаційно-комунікаційна система», «система захисту інформації».

Стаття 2. Встановлює об’єкти захисту інформації, до яких належать, зокрема, інформація з обмеженим доступом, відкрита інформація, вимога щодо захисту якої встановлена законом, та інформаційні ресурси.

Стаття 8. Визначає вимоги до створення та функціонування систем захисту інформації.

2. Закон України «Про основи національного спротиву» [9]. Хоча цей закон безпосередньо не регулює роботу з електронними документами, він має значний вплив на кібербезпеку, оскільки визначає правові та організаційні засади національного спротиву, частиною якого є кіберспротив.

Стаття 1. Визначає поняття «національний спротив» та «територіальна оборона».

Стаття 4. Визначає, що складовими національного спротиву є територіальна оборона, рух опору та підготовка громадян України до національного спротиву. Кіберспротив є однією з форм, що може бути реалізована в рамках цих складових.

3. Закон України «Про основні засади забезпечення кібербезпеки України» [10]. Цей закон є ключовим у сфері кібербезпеки, оскільки визначає правові та організаційні засади забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі.

Стаття 1. Визначає ключові терміни: «кібербезпека», «кібератака», «кіберзахист», «критична інформаційна інфраструктура», «державні інформаційні ресурси».

Стаття 5. Встановлює принципи забезпечення кібербезпеки.

Стаття 7. Визначає об’єкти критичної інформаційної інфраструктури (КІІ) та їх категоризацію. Це має пряме відношення до ДІР, оскільки багато державних інформаційних ресурсів належать до КІІ.

Стаття 8. Регулює діяльність державних органів та суб’єктів приватного сектору щодо забезпечення кібербезпеки.

Стаття 10. Встановлює основні функції Національної системи кібербезпеки.

Стаття 12. Визначає особливості захисту інформації в державних інформаційних ресурсах та об’єктах критичної інформаційної інфраструктури.

4. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [11]. Цей закон регулює правові відносини у сфері надання електронних довірчих послуг, що є фундаментальним для забезпечення юридичної значущості електронних документів.

Стаття 1. Визначає основні терміни, зокрема «електронний підпис», «електронна печатка», «електронна позначка часу», «кваліфікований надавач електронних довірчих послуг».

Стаття 18. Встановлює правовий статус електронного підпису та порядок його використання. Електронний підпис є обов’язковим елементом для надання електронному документу юридичної сили.

Стаття 19. Регулює питання використання електронної печатки.

Стаття 20. Визначає вимоги до кваліфікованого електронного підпису та кваліфікованої електронної печатки.

Стаття 24. Визначає порядок надання електронних довірчих послуг та вимоги до їх безпеки.

5. Закон України «Про електронні документи та електронний документообіг» [12]. Цей закон є безпосереднім регулятором роботи з електронними документами.

Стаття 5. Визначає термін «електронний документ».

Стаття 9. Визначає термін «електронний документообіг».

Стаття 6. Визначає поняття електронний підпис та електронна печатка.

Стаття 5. Встановлює правовий статус електронного документа. Зокрема, зазначається, що електронний документ (документ в електронній формі) за юридичною силою прирівнюється до документу на папері.

Стаття 7. Регулює питання використання електронного підпису. Зазначається, що накладанням електронного підпису завершується створення електронного документа.

Стаття 8. Визначає зберігання електронних документів.

Стаття 9. Регулює питання електронного документообігу та обміну електронними документами.

6. Закон України «Про доступ до публічної інформації» [7]. Даний закон встановлює порядок доступу до публічної інформації та визначає категорії інформації з обмеженим доступом.

Стаття 6. Визначає інформацію з обмеженим доступом (конфіденційна, таємна, службова інформація).

Стаття 9. Регулює порядок обмеження доступу до інформації.

7. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [13]. Дана постанова є одним з ключових підзаконних актів, що конкретизує положення Закону України «Про основні засади забезпечення кібербезпеки України». Затверджує Порядок проведення аудиту інформаційної безпеки на об’єктах критичної інформаційної інфраструктури. Визначає механізми взаємодії між суб’єктами забезпечення кібербезпеки у разі виявлення кіберінцидентів. Встановлює вимоги до створення та функціонування системи управління інформаційною безпекою (УІБ) на об’єктах КІІ та в державних інформаційних ресурсах.

8. Постанова Кабінету Міністрів України від 09 листопада 2020 р. № 1184 (зі змінами №447 від 28.03.2025) «Деякі питання об’єктів критичної інформаційної інфраструктури» [4]. Дана постанова деталізує питання кіберзахисту об’єктів критичної інформаційної інфраструктури. Затверджує Порядок категоризації об’єктів критичної інфраструктури та встановлення вимог до їх кіберзахисту. Визначає заходи з кіберзахисту, що мають бути реалізовані на об’єктах КІІ.

Національне законодавство України щодо захисту інформації та кібербезпеки є комплексним та включає як загальні закони, що регулюють питання інформаційної безпеки, так і спеціалізовані акти, що стосуються кібербезпеки, електронних документів та критичної інфраструктури. Узагальнена система, яка в цілому регулює дане питання висвітлена на рисунку 1.4.

ДІР підпадають під дію Закону України «Про захист інформації в інформаційно-комунікаційних системах» [8] та Закону України «Про основні засади забезпечення кібербезпеки України» [10]. Захист ДІР передбачає впровадження систем захисту інформації, регулярний аудит безпеки, а також реагування на кіберінциденти.

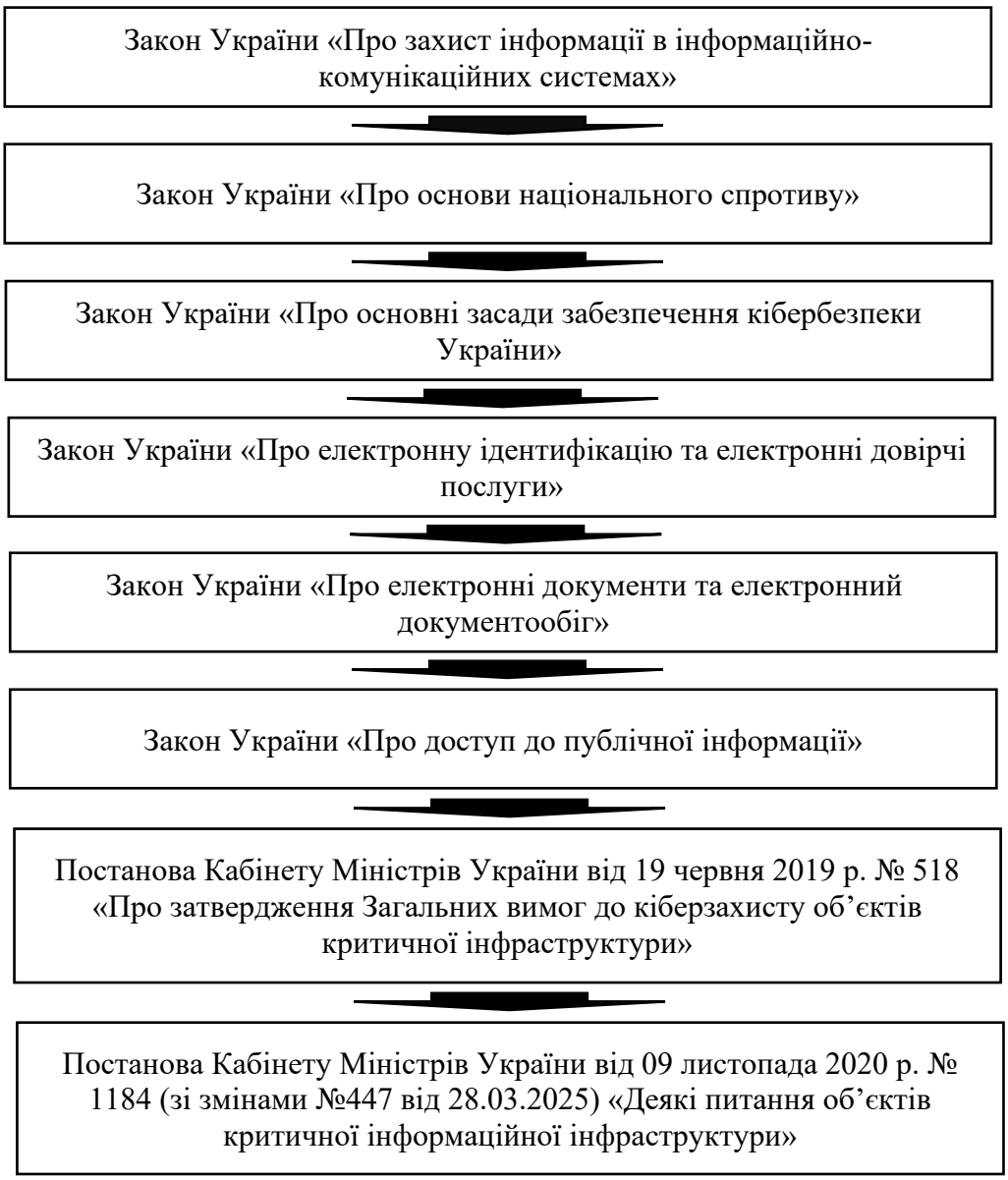


Рисунок 1.4 – Основні нормативно-правові акти, що регулюють сферу захисту інформації та кібербезпеки в Україні

Критична інформаційна інфраструктура (КІІ) має особливий статус та регулюється Законом України «Про основні засади забезпечення кібербезпеки України» [10] та відповідними постановами Кабінету Міністрів України [4]. До КІІ висуваються підвищені вимоги до кіберзахисту, включаючи категоризацію, впровадження систем УІБ та постійний моніторинг.

Робота з електронними документами регулюється Законами України «Про електронні документи та електронний документообіг» [12] та «Про електронну ідентифікацію та електронні довірчі послуги» [14]. Дані закони встановлюють

юридичну силу електронних документів, вимоги до їх створення, підписання (за допомогою КЕП), зберігання та обміну, що є критично важливим для забезпечення цілісності та конфіденційності інформації в ДІР та КІІ.

Важливо зазначити, що сфера кібербезпеки та захисту інформації постійно розвивається, тому необхідно відслідковувати зміни в законодавстві та дотримуватися актуальних нормативно-правових актів.

СЕДО в КІ відіграє надзвичайно важливу роль, оскільки забезпечує функціонування життєво важливих систем та сервісів. Забезпечення безпеки, конфіденційності, цілісності та доступності інформації в СЕДО КІ є пріоритетом. Для досягнення даних цілей організації використовують міжнародні стандарти та фреймворки.

Нижче наведено огляд ключових міжнародних стандартів та фреймворків, а також їх застосовуваність до СЕДО в КІ (складова 2, рис.1.2).

1. ДСТУ ISO/IEC 27001 – Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою [15].

Поняття «Система управління інформаційною безпекою» (СУІБ) визначено в ДСТУ EN ISO/IEC 27000:2022 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів [16].

ДСТУ ISO/IEC 27001 – це державний стандарт України, який імплементований з аналогічного міжнародного. Визначає вимоги до створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та постійного вдосконалення СУІБ. Базується на підході, заснованому на ризиках, і допомагає організаціям оцінювати та управляти ризиками для інформаційної безпеки.

Ключовими аспектами даного стандарту є те, що стандарт фокусується на захисті трьох основних властивостей інформації: конфіденційність, цілісність та доступність. Управління ризиками вимагає проведення регулярних оцінок ризиків та впровадження заходів контролю для їх зниження до прийнятного рівня. СУІБ є динамічною системою, тому передбачає її постійне вдосконалення, що потребує постійного моніторингу та адаптації до нових загроз.

Додаток А стандарту ДСТУ ISO/IEC 27001 [15] містить набір контролів безпеки, які можуть бути застосовані для управління ризиками, включаючи контроль доступу, криптографію, фізичну безпеку та управління інцидентами.

Розглянемо застосовуваність ДСТУ ISO/IEC 27001 до СЕДО в критичній інфраструктурі.

По-перше, це захист документів протягом всього життєвого циклу. ДСТУ ISO/IEC 27001 забезпечує системний підхід до захисту електронних документів від створення до архівування та знищення. Це критично важливо для КІ, де цілісність та незмінність даних є обов'язковою.

По-друге, управління доступом. Дозволяє впровадити строгі політики контролю доступу до конфіденційних електронних документів, що є особливо важливим для операційних даних КІ.

По-третє, забезпечення цілісності та автентичності. Допомагає гарантувати, що електронні документи не були змінені несанкціонованим чином, що є життєво важливим для юридично значущих документів та операційних інструкцій у КІ.

По-четверте, безперервність бізнесу та відновлення після інцидентів. Вимоги стандарту щодо безперервності та відновлення допомагають забезпечити доступність електронних документів навіть у разі кіберінцидентів або інших надзвичайних ситуацій, що є вирішальним для безперебійного функціонування КІ.

По-п'яте, відповідність законодавству. ДСТУ ISO/IEC 27001 допомагає організаціям відповідати національним та міжнародним вимогам щодо захисту даних та інформаційної безпеки, що часто є суворими для об'єктів КІ.

2. NIST Cybersecurity Framework (CSF) – Основа кібербезпеки NIST [17]. NIST CSF – це фреймворк, розроблений Національним інститутом стандартів і технологій США, призначений для управління та зниження ризиків кібербезпеки. Він був створений з особливим акцентом на критичну інфраструктуру, хоча згодом його застосовуваність розширилася на організації

будь-якого розміру та сектора. Фреймворк є гнучким і дозволяє організаціям адаптувати свої практики IT-безпеки до своїх унікальних потреб.

NIST CSF базується на п’яти основних функціях, які формують життєвий цикл управління кіберризиками (рис. 1.5):

- ідентифікувати (Identify) – розуміння організаційних ризиків для систем, активів, даних та можливостей;
- захистити (Protect) – розробка та впровадження відповідних гарантій для забезпечення доставки критично важливих послуг;
- виявити (Detect) – впровадження заходів для своєчасного виявлення кібербезпекових подій;
- реагувати (Respond) – розробка та впровадження відповідних заходів у разі виявлення кібербезпекової події;
- відновити (Recover) – розробка та впровадження заходів для відновлення пошкоджених можливостей або послуг.

Рисунок 1.5 – Життєвий цикл управління кіберризиками згідно NIST CSF

Розглянемо застосовуваність NIST CSF до СЕДО в КІ.

1. Комплексний підхід до ризиків СЕДО. NIST CSF надає структурований підхід до ідентифікації та управління кіберризиками, пов’язаними з електронними документами та системами документообігу в КІ.

2. Проактивний захист. Функції «Ідентифікувати» та «Захистити» допомагають розробити стратегії для запобігання несанкціонованому доступу, зміні або знищенню електронних документів, що включає впровадження контролю доступу, шифрування, резервного копіювання та інших заходів.

3. Швидке реагування на інциденти. Функції «Виявити», «Реагувати» та «Відновити» є критично важливими для КІ, де швидкість реагування на кіберінциденти в СЕДО може мінімізувати шкоду та забезпечити безперервність операцій.

4. Гнучкість та адаптивність. Фреймворк NIST CSF є гнучким, що дозволяє організаціям КІ адаптувати його до специфічних потреб та загроз, з якими вони стикаються у своїй галузі, що дозволяє враховувати особливості СЕДО в різних секторах КІ (наприклад, енергетика, транспорт, фінанси).

5. Спільна мова для комунікації. Надає спільну термінологію для обговорення та управління ризиками кібербезпеки, що полегшує співпрацю між різними стейкхолдерами в рамках КІ.

Хоча ISO/IEC 27001 та NIST CSF є одними з найбільш поширених, існують й інші стандарти, які можуть бути релевантними для СЕДО в КІ. Розглянемо деякі з них.

ДСТУ EN ISO 22301:2021 Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги [18]. Даний стандарт фокусується на забезпеченні безперервності бізнесу та відновленні після інцидентів. Для СЕДО в КІ це означає здатність продовжувати операції з документами навіть після збоїв, що є критично важливим для безперебійного функціонування КІ.

Серія стандарту ДСТУ EN IEC 62443:2022, який стосується безпеки мереж та систем промислової автоматизації та керування. Даний стандарт містить цілу низку стандартів, наприклад, ДСТУ EN IEC 62443-3-3:2022 «Промислові комунікаційні мережі. Безпека мережі та системи». Частина 3-3. Вимоги та рівні безпеки системи [19]. Цей стандарт (його складові) стосується кібербезпеки промислових систем керування (АСУ ТП), які часто використовуються в критичній інфраструктурі. Хоча він не прямо стосується ЕДО, він охоплює

безпеку мереж, через які можуть передаватися електронні документи, і є важливим для загальної кібербезпеки КІ.

Застосування міжнародних стандартів та фреймворків, таких як ISO/IEC 27001 та NIST CSF, є не просто рекомендованим, а життєво необхідним для забезпечення надійного та безпечного функціонування систем електронного документообігу в критичній інфраструктурі. Ці стандарти надають структурований підхід до управління ризиками, захисту конфіденційності, цілісності та доступності інформації, а також забезпечують безперервність операцій. Впровадження цих фреймворків дозволяє організаціям КІ не тільки підвищити свою кіберстійкість, а й відповідати регуляторним вимогам та підвищити довіру з боку зацікавлених сторін.

Захист інформації в державних СЕДО та системах ЕДО, які оперують інформацією КІ, є критично важливим аспектом національної безпеки та стабільності. В Україні ці вимоги регламентуються низкою нормативно-правових актів, які встановлюють порядок створення, функціонування та забезпечення безпеки таких систем.

Основним регулятором у сфері захисту інформації в Україні є Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку), яка розробляє, затверджує та контролює виконання відповідних нормативів [1].

Стаття 2 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України» визначає статус Державної служби спеціального зв’язку та захисту інформації України. Дослівно «Державна служба спеціального зв’язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.

Виходячи з огляду нормативних документів можна визначити певні загальні та специфічні вимоги (специфічні вимоги можуть стосуватись систем захисту інформації в СЕДО, які оперують інформацією КІ).

1. Загальні вимоги до систем захисту інформації (СЗІ) в СЕДО КІ. Вимоги до СЗІ в цих системах ґрунтуються на принципах конфіденційності, цілісності та доступності інформації та включають:

- комплексну систему захисту інформації (КСЗІ). Для державних інформаційних систем та інформації, вимога щодо захисту якої встановлена законом, де обов'язковим є створення КСЗІ з підтвердженою відповідністю. Система має пройти державну експертизу та отримати Атестат відповідності від Держспецзв'язку. Необхідно відмітити, що зараз відбувається процес відмови від створення КСЗІ, підтвердженням цього є прийняття Закону України № 4336-IX про кіберзахист державних інформаційних ресурсів, відповідно до якого передбачена створення цільових профілів безпеки, перехід до створення СУІБ в системах, де відсутня обробка інформації з обмеженим доступом (таємної інформації) [20];
- відповідність нормативно-правовим актам. СЗІ повинна відповідати вимогам чинного законодавства України у сфері захисту інформації, зокрема частині законів, які були розглянуті вище, наприклад, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [8], Закон України «Про основні засади забезпечення кібербезпеки України» [10], Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (щодо використання електронних підписів) [14], Закон України «Про критичну інфраструктуру» (для систем КІ) [2], Постанови Кабінету Міністрів України, накази та інші нормативні документи Держспецзв'язку;
- визначення моделі загроз та моделі порушника. Перед розробкою СЗІ необхідно провести аналіз та визначити актуальні загрози безпеці інформації, а також потенційних порушників та їхні можливості, що є основою для вибору ефективних засобів захисту;

- впровадження засобів технічного та криптографічного захисту. СЗІ має включати комплекс організаційних та технічних заходів, зокрема: засоби криптографічного захисту інформації (КЗІ) та обов'язкове використання КЕП для забезпечення цілісності та автентичності електронних документів. КЗІ повинні мати експертні висновки Держспецзв'язку. Також до СЗІ мають бути включені засоби антивірусного захисту, системи виявлення вторгнень, засоби міжмережевого екранування, системи аудиту та моніторингу подій безпеки;
- засоби контролю доступу. Забезпечення авторизованого доступу до інформації та функцій СЕДО на основі ролей та повноважень користувачів;
- системи резервного копіювання та відновлення. Забезпечення безперервності роботи СЕДО та можливості відновлення інформації після збоїв або інцидентів.

Окремо до організаційних заходів необхідно віднести розробку політик інформаційної безпеки, процедур та інструкцій; навчання персоналу правилам інформаційної безпеки; регулярний аудит та моніторинг ефективності СЗІ; розробка та впровадження планів реагування на інциденти інформаційної безпеки.

2. Специфічні вимоги до СЗІ при роботі СЕДО з ДІР КІ.

Державні СЕДО, як правило, працюють з інформацією, яка може містити інформацію з обмеженим доступом (конфіденційну, службову, або навіть таємну). Тому вимоги до СЗІ є особливо суворими:

- обов'язковість КСЗІ. При роботі СЕДО з ДІР КІ КСЗІ є обов'язковою, що підтверджується Атестатом відповідності;
- дотримання вимог щодо захисту державної таємниці. Якщо в СЕДО обробляється інформація, що становить державну таємницю, застосовуються додаткові вимоги Закону України «Про державну таємницю» [21] та інших нормативно-правових актів у даній сфері;
- захист персональних даних. Необхідно дотримуватися вимог Закону України «Про захист персональних даних» [22], включаючи принципи обробки даних, права суб'єктів даних та заходи безпеки;

- робота з системою взаємодії електронних документів (СВЕД): Державні СЕДО часто інтегровані в єдину систему СВЕД, що вимагає узгоджених заходів безпеки та використання спільних протоколів захисту.

3. Специфічні вимоги до СЗІ в СЕДО, які оперують інформацією критичної інфраструктури.

Об’єкти критичної інфраструктури (ОКІ) є надзвичайно важливими для функціонування держави та суспільства, тому вимоги до захисту їх інформаційних систем, включаючи СЕДО, є підвищеними та знову ж таки регламентуються цілою низкою нормативних, організаційних та інженерно-технічних вимог:

- Закон України «Про критичну інфраструктуру» [2]. Даний закон є основоположним і визначає правові та організаційні засади захисту КІ. Також він встановлює вимоги до кіберзахисту ОКІ;
- Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» [13]. Дана постанова деталізує вимоги до кіберзахисту ОКІ та включає: категоризацію об’єктів КІ; впровадження системи управління кібербезпекою; постійний моніторинг; плани реагування та відновлення; обов’язкове подання інформації суб’єктами КІ про стан кіберзахисту та інциденти до Держспецзв’язку; взаємодія з національною системою кібербезпеки (СЕДО КІ повинні бути інтегровані в національну систему кібербезпеки та взаємодіяти з Центром реагування на кіберзагрози (CERT-UA) та іншими органами); забезпечення безперервності функціонування (крім захисту інформації, для КІ особливо важлива безперервність роботи СЕДО навіть у разі кібератак або надзвичайних ситуацій, що включає резервування систем, географічно розподілені сховища даних, плани безперервності бізнесу та відновлення після катастроф); відповідність міжнародним стандартам (українське законодавство є основним, але організації КІ часто застосовують міжнародні стандарти, такі як NIST CSF та ISO/IEC 27001, для підвищення рівня кібербезпеки та відповідності найкращим світовим практикам).

Таким чином, вимоги до СЗІ в СЕДО, які працюють з ДІР КІ в Україні, є багатогранними та суворими. Вони охоплюють як організаційні, так і технічні аспекти, з особливим акцентом на використання криптографічного захисту, комплексний підхід до управління ризиками та забезпечення безперервності функціонування. Дотримання даних вимог є запорукою надійності, конфіденційності та стабільності обробки електронних документів у життєво важливих сферах державного управління та національної безпеки.

ВИСНОВКИ ДО РОЗДІЛУ 1

У межах першого розділу кваліфікаційної роботи було проведено комплексний аналіз теоретичних засад та визначено ключові концепції, що є фундаментальними для розуміння проблематики захисту ДІР КІ з особливим акцентом на роль СЕДО.

По-перше, було встановлено, що КІ є сукупністю життєво важливих об’єктів та систем, порушення функціонування яких здатне спричинити катастрофічні наслідки для національної безпеки, економічної стабільності та суспільного добробуту. Детальна класифікація секторів КІ, згідно з національним законодавством України, підтверджує багатовекторність та системну взаємозалежність цих елементів. Показано, що ДІР, які оброблюються у межах КІ, є не просто інформацією, а стратегічними активами, що забезпечують оперативне та адміністративне управління. Доведено, що цілісність, конфіденційність та доступність цих ресурсів є основними принципами їхнього захисту.

По-друге, особливу увагу було приділено СЕДО, які еволюціонували до статусу критично важливих інформаційних систем у державному управлінні та КІ. Визначено, що СЕДО не лише автоматизують процеси документообігу, але й виступають центральним інструментом для оперативного прийняття рішень, координації діяльності, дотримання нормативних вимог та забезпечення безперервності бізнес-процесів. Аналіз функціоналу та архітектури сучасних

СЕДО розкрив їхні ключові особливості: можливості функціонування у локальному середовищі, імплементації багаторівневого криптографічного захисту, а також відповідність національним стандартам та здатність до подальшої модернізації без впливу на ядро системи.

По-третє, було деталізовано типи інформації, що обробляється в СЕДО КІ. З'ясовано, що згідно із Законом України «Про доступ до публічної інформації», інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом (конфіденційну, службову, таємну). Підкреслено, що для роботи з таємною інформацією від СЕДО вимагається обов'язкова державна експертиза та отримання відповідного позитивного висновку від Держспецзв'язку, що зумовлює диференційовані вимоги до захисту, які залежать від рівня чутливості інформації.

Нарешті, проведено огляд нормативно-правової бази та міжнародних стандартів, що регулюють захист інформації в КІ. Розглянуто ключові Закони України та постанови Кабінету Міністрів України, які визначають правові та організаційні засади кіберзахисту, електронного документообігу та захисту персональних даних. Імплементація міжнародних стандартів, таких як ДСТУ ISO/IEC 27001 та NIST Cybersecurity Framework, було обґрунтовано як необхідну умову для підвищення кіберстійкості та відповідності найкращим світовим практикам. Визначено загальні та специфічні вимоги до СЗІ в СЕДО, які працюють з ДІР КІ, включаючи необхідність створення КСЗІ та використання засобів криптографічного захисту.

Таким чином, перший розділ заклав фундаментальну теоретичну основу для подальшого дослідження, систематизувавши ключові концепції КІ та ДІР, розкривши роль і специфіку СЕДО як об'єкта захисту, а також окресливши чинні нормативно-правові та стандартизаційні вимоги до забезпечення їхньої безпеки. Отримані результати є необхідним підґрунтям для розробки моделі вибору та аналізу комплексу засобів захисту СЕДО ДІР КІ, що буде деталізовано у наступних розділах роботи.

РОЗДІЛ 2. КЛАСИФІКАЦІЯ ТА АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ СЕДО В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

2.1 Огляд основних категорій засобів захисту інформації, релевантних для СЕДО

Ефективний захист СЕДО при роботі з ДІР КІ - це не просто бажана опція, а життєва необхідність. Дані системи є сховищем та каналом передачі надзвичайно чутливої та критично важливої інформації, будь-яке компрометування якої може призвести до серйозних операційних збоїв, значних фінансових втрат, загрози життю та здоров'ю людей, а також до підриву національної безпеки.

Даний розділ присвячений детальному огляду та класифікації основних категорій засобів захисту інформації, які є релевантними для СЕДО в КІ. Відтак, доцільним є поділ засобів захисту на чотири ключові категорії: організаційні заходи, програмні інструменти, апаратні засоби та комплексні архітектурні рішення, кожна з яких забезпечує окремий, але взаємопов'язаний з іншими, рівень інформаційної безпеки СЕДО.

Наступні підпункти спрямовані на систематичний аналіз кожної з цих категорій із позицій їх функціонального призначення, актуальності для СЕДО в критичній інфраструктурі та відповідності сучасним вимогам захисту інформації.

2.1.1. Організаційні механізми забезпечення інформаційної безпеки в СЕДО

Організаційні механізми інформаційної безпеки в СЕДО, які функціонують у КІ, утворюють не лише фундамент безпечної взаємодії користувача з цифровим середовищем, а й автономний, структурно пов'язаний

блок, що поєднує нормативні моделі, ризик-орієнтовані процеси, поведінкову аналітику та адаптивну навчальну політику, що описана на рисунку 2.1. Ці механізми вже не можуть сприйматися як периферійне доповнення до технічного забезпечення, навпаки, вони дедалі частіше стають ключовим чинником ефективності всієї архітектури інформаційного захисту. У контексті СЕДО ДІР КІ, де обробка документів охоплює відкриту інформацію та інформацію з обмеженим доступом, організаційний рівень виступає центральною віссю управлінської відповідальності та цифрової етики.

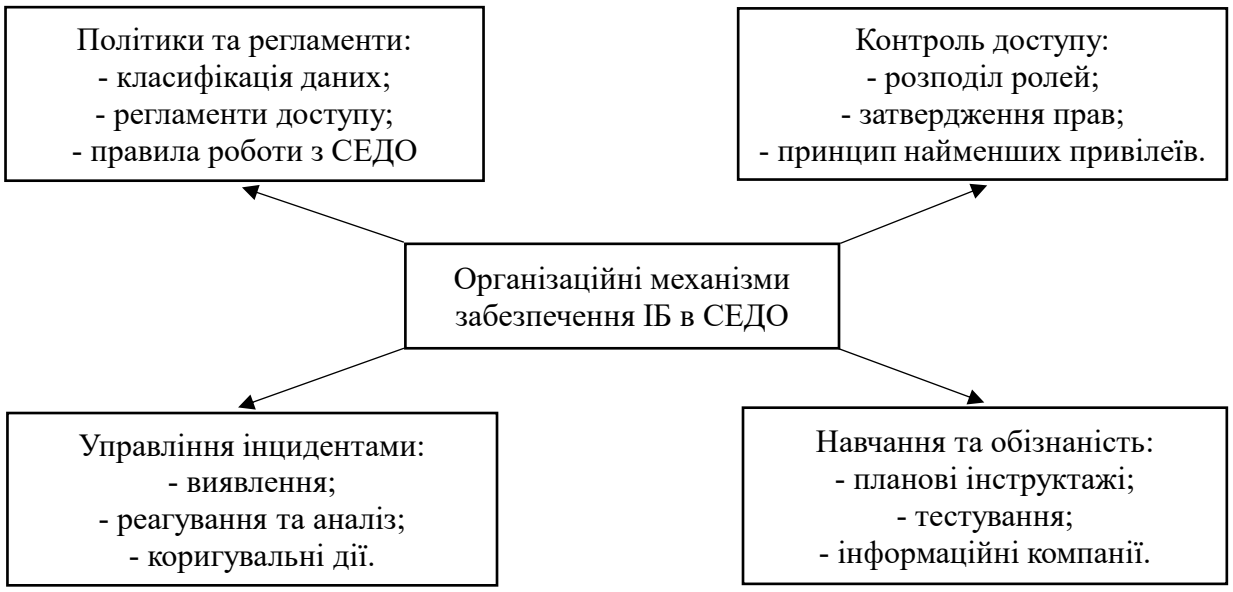


Рисунок 2.1 - Організаційні механізми забезпечення інформаційної безпеки в СЕДО

Сучасна концепція УІБ визначає організаційні засоби як інтегративні інститути, що втілюються у вигляді політик, інструкцій, регламентів, процедур аудиту, правил доступу, механізмів реагування, систем навчання, внутрішніх стандартів та поведінкових практик. Ці інструменти не існують у вакуумі – вони взаємодіють із технологіями та з людським фактором, формуючи єдине середовище стійкого функціонування СЕДО в умовах динамічних загроз. Організаційна безпека, таким чином, є соціотехнічною системою, у межах якої нормативне середовище, ризик-моделювання, цифрова поведінка користувача та адаптивність процедур зливаються в єдину логіку управління.

Одним із ключових напрямів, що визначає ефективність організаційної складової, є впровадження динамічних, контекстно-чутливих політик, що трансформуються відповідно до сценаріїв використання системи, критичності інформаційного активу, ризик-профілю користувача та загального середовища загроз. Політика доступу, сформульована як набір абстрактних правил, втрачає ефективність у момент, коли користувач працює у нестандартному контексті (наприклад, поза межами внутрішньої мережі, у позаробочий час, із пристрою, що не пройшов перевірки). Саме тому передові організації переходять до моделей «Policy-as-Code», у яких політики транслюються не лише на рівень регламенту, а й на рівень коду, що виконується під час кожної транзакції в СЕДО. У такий спосіб реалізується автоматизований контроль відповідності дій політикам у режимі реального часу.

Значущим еволюційним зрушенням стало також поширення архітектури «Zero Trust», що передбачає відмову від презумпції довіри навіть до авторизованих користувачів усередині периметру. Дана парадигма, яку вже імплементували такі структури як Міністерство оборони США, Google та Європейське агентство з кібербезпеки (ENISA), вимагає від організацій, що використовують СЕДО, запровадження контекстно-адаптивного доступу на основі моделей поведінки «User & Entity Behavior Analytics» (UEBA), багатофакторної аутентифікації, мікросегментації середовища та перевірки цілісності сесії на кожному етапі взаємодії з документом. Відтак, управління доступом перестає бути статичною функцією і перетворюється на гнучкий інструмент верифікації наміру та правомірності дій, що реагує на найменші відхилення від очікуваної моделі поведінки.

Поза суто технологічними рамками, вирішального значення набуває здатність організації підтримувати ефективну модель реагування на інциденти, яка включає не лише оперативну реакцію, а й аналітичне осмислення, ревізію політик, перегляд маршрутів доступу та оновлення навчальних програм. Стратегічно ефективною вважається петльова модель реагування, в якій кожен інцидент породжує зворотну хвилю змін у структурі ІБ. Її якість визначається за

показниками MTTD (середній час виявлення), MTTR (середній час до відповіді), а також часткою подій, що призвели до зміни інструкцій, ролей або процедур доступу. Практика провідних аналітичних центрів показує, що вищий рівень організаційної зрілості настає лише тоді, коли інциденти використовуються не як одиничні помилки, а як фактори системної корекції.

Усе більше організацій, у тому числі на рівні державного управління, усвідомлюють, що людський чинник – основна точка вразливості в СЕДО. У зв'язку з цим виникає потреба у трансформації моделі навчання: від формальних курсів і ознайомлень до поведінково-контекстного навчання з підкріпленням практикою. У найрозвиненіших реалізаціях ця модель включає симульовані фішинг-атаки, гейміфіковані кейси, автоматизовані підказки на основі реальних дій користувача та оновлення навчального контенту відповідно до змін у середовищі загроз. Зростаюча практика впровадження внутрішніх рейтингів кіберграмотності, регулярних внутрішніх аудитів знань і контекстуалізованих нагадувань створює середовище, де безпека стає культурною нормою, а не винятком.

Новітнім підходом, що лише починає впроваджуватися на перетині технології та організації, є застосування цифрового двійника інформаційної безпеки. Йдеться про створення віртуальної моделі політик, поведінкових сценаріїв, потоків документів і дій користувачів, на базі якої здійснюється моделювання потенційних інцидентів, прогноз наслідків змін у регламенті, виявлення латентних вразливостей та оптимізація ролей і доступу. Такий підхід уже продемонстровано в пілотних проєктах IBM, Palo Alto Networks та в дослідницьких ініціативах НАТО. Для СЕДО при роботі з ДІР КІ це може означати вихід на принципово новий рівень самоадаптивності – коли організація не лише реагує на ризики, а й проактивно перебудовує власні структури у відповідь на гіпотетичні сценарії.

Найбільш революційним кроком є впровадження цифрового двійника документообігу – поведінкової моделі, що відображає сценарії руху документів, рішення користувачів, вплив процесів на зміну ролей, затримки та відхилення.

AI/ML-двигун аналізує ці сценарії, виявляє патерни ризику, пропонує корекцію політик, попереджає аномальні дії і слугує основою для розвитку моделі самоадаптивної організації [23].

У контексті України, яка унаслідок геополітичної ситуації вимушено стала полем випробування на кіберстійкість, розвиток організаційної складової ІБ у СЕДО КІ є не лише питанням професіоналізму, а й національної безпеки. Створення нормативних баз, запуск платформ «Дія», «Prozorro», впровадження багатофакторної аутентифікації та централізованої реєстрації доступів демонструють, що Україна рухається в напрямку практичної реалізації моделей «Zero Trust» і «Policy-as-Code». Проте повноцінна інтеграція адаптивних механізмів в управлінні СЕДО потребує розгортання систем поведінкової аналітики, створення цифрових двійників, запровадження системного інцидент-менеджменту з рефлексією та оцінки ефективності навчання за поведінковими індикаторами.

2.1.2. Програмне забезпечення як інструмент реалізації технічного захисту інформації в СЕДО

Програмне забезпечення (ПЗ) є центральним елементом реалізації технічного захисту інформації в СЕДО, особливо у випадках, коли мова йде про обробку ДІР у контексті КІ. На відміну від організаційних механізмів, що регулюють поведінку користувачів та адміністративну структуру доступу, саме програмні засоби забезпечують технічну дієвість контролю, фіксації та забезпечення конфіденційності й цілісності цифрових транзакцій.

Сучасні СЕДО реалізовують багаторівневі механізми доступу до документів на основі рольової (RBAC) або атрибутивної (ABAC) моделей. У межах програмного захисту доступність конкретного документа може визначатися не лише правами користувача, а й метаданими об’єкта, фазою маршруту узгодження або умовами бізнес-правил.

Програмна реалізація захисту також включає механізми криптографічної обробки – перш за все, накладання КЕП на документи та їхні атрибути. Важливо, що відповідно до вимог законодавства (Закон України «Про електронні довірчі послуги») та європейського регламенту «eIDAS», ці підписи повинні бути сумісні з сервісами перевірки чинності (OCSP) та з мітками часу (TSP). У багатьох системах, наприклад у «SCHRIFT» або «М.Е.Док», реалізована підтримка мультипідпису та перевірка цифрової ідентичності сертифікатів.

Програмні DLP-рішення (Data Loss Prevention), інтегровані в СЕДО, здійснюють сканування вмісту документів на предмет виявлення конфіденційної інформації (ключові слова, шаблони, реквізити), контроль дій користувачів з високими правами доступу (наприклад, копіювання, пересилання, друк) та блокування витоків за межі дозволеного середовища. Застосування DLP у поєднанні з NLP-модулями дозволяє не лише аналізувати структуру тексту, а й ідентифікувати контекст, наприклад, чи містить документ дані оборонного значення або медичну таємницю.

Ще одним важливим напрямом є використання систем інтегрованого журналювання – SIEM-платформ (Security Information and Event Management), які збирають події з усіх компонентів СЕДО, корелюють їх у часі, виявляють нетипову поведінку користувача та підозрілі аномалії. Зокрема, для СЕДО КІ особливо цінною є можливість SIEM відслідковувати ланцюг узгодження, виявляти невластиві затримки або зміну маршруту, що може бути ознакою саботажу або внутрішньої атаки.

Додатково реалізуються програмні механізми шифрування зберігання та транспортування даних між компонентами СЕДО, шифрування архівів документів на сервері (AES-256) та періодичне створення резервних копій із контрольними хешами. Дані рішення критично важливі в умовах зростання шкідливих програм-шифрувальників (ransomware), які стали ціллю атак на державні СЕДО в період 2022–2024 рр.

Окремим компонентом є технології контролю версій (versioning) та механізми WORM (Write Once, Read Many), які забезпечують доказовість

незмінності документа після його підписання та передачі на архівне зберігання. Це особливо актуально для документів, які мають юридичну силу (накази, розпорядження, регламенти) і потребують збереження впродовж тривалого часу.

Серед сучасних трендів у програмному захисті в СЕДО виділяється впровадження так званих модулів «secure viewer» – обмеженого перегляду документів без можливості копіювання або друку, а також підтримка логіки умовного перегляду: наприклад, частковий доступ до окремих полів у формі з обмеженням перегляду вкладень. Такі технології активно застосовуються в системах документообігу оборонних підприємств країн НАТО.

Варто також зазначити, що повноцінна програмна реалізація захисту можлива лише за умови правильної взаємодії з інфраструктурою відкритих ключів (PKI), централізованими сервісами аутентифікації (LDAP, Kerberos, SSO) та інструментами валідації дій (audit trails). У провідних державних платформах електронної взаємодії між ДІР, таких як «Трембіта», реалізовано окремий модуль контролю цифрової відповідності – так званий «Audit Validator», який перевіряє відповідність усіх дій політиці безпеки й формує підсумковий аудит-файл для верифікації контролюючими органами, який можливо ефективно імплементувати й у СЕДО для роботи з ДІР КІ. [24].

2.1.3. Апаратна складова системи захисту: засоби зберігання та криптографічної обробки даних

Індивідуальні користувачі в СЕДО взаємодіють із апаратним захистом через персональні токени або смарт-карти, що містять особисті закриті ключі. Ці носії – наприклад, сертифіковані «SecureToken» або «Матрікс-3» – забезпечують неможливість підпису без фізичного носія, що підключається до комп’ютера. Система не дозволяє виконати підпис без підтвердження власником: апаратна частина, відповідальна за підпис, блокує виконання функції у разі невідповідності контексту або спроби несанкціонованого доступу.

Серверна інфраструктура СЕДО також потребує апаратного захисту, і тут ключову роль відіграє TPM (Trusted Platform Module) – вбудований у материнську плату чип, який зберігає контрольні хеші етапів запуску системи та дозволяє виконати завантаження лише за умови, що середовище залишилося незмінним. Для серверів СЕДО, які обробляють тисячі документів з підписами щодня, це означає, що ніхто не зможе приховано змінити системне ПЗ або драйвери без втрати криптографічної довіри. У більшості сучасних серверів (зокрема, Dell, Lenovo, HPE) TPM входить до базової комплектації, однак в українському держсекторі він досі майже не використовується [25].

Окрему категорію становлять засоби довгострокового зберігання цифрових документів. Тут найбільш ефективними є WORM-сховища – такі, де запис здійснюється лише один раз, а читання допускається необмежену кількість разів без можливості модифікації чи видалення даних. У СЕДО це особливо важливо для забезпечення достовірності архівів нормативних документів, розпоряджень або матеріалів внутрішніх службових перевірок. У розвинених країнах ці технології вже стандартизовані; в Україні ж досі використовуються лише обмежено (наприклад, у Національному архівному фонді), хоча потенціал їх застосування у СЕДО – надзвичайно високий.

Ще один рівень захисту реалізується через фізичну ізоляцію каналів зв’язку та застосування апаратних VPN-шлюзів. Вони забезпечують шифрування даних «на вході» та «на виході» без залучення операційної системи, а отже, навіть за її компрометації залишаються контрольованими.

2.1.4. Інтегровані архітектури безпеки та концептуальні моделі кіберзахисту СЕДО в критичній інфраструктурі

Zero Trust Architecture (ZTA) є найвідомішим трендом останніх років. Її головна ідея – ніколи не довіряти за замовчуванням. Усі транзакції, навіть внутрішні, мають постійно верифікуватися. Для СЕДО це означає, що не лише користувач, а й кожен документ, запит, підпис або маршрут проходять перевірку

з урахуванням контексту. Вона відзначається високою ефективністю в умовах багаторівневої взаємодії та гібридних хмарних моделей, однак потребує складної інтеграції з механізмами поведінкового аналізу, DLP та логікою ABAC [26].

Secure Access Service Edge (SASE) – це хмарно-орієнтована модель безпеки (застосовується виключно для обробки відкритої інформації, або ж тоді, коли хмарний провайдер пройшов відповідну сертифікацію), яка поєднує мережевий доступ і захист у єдину платформу. Вона дуже ефективна для розподілених СЕДО з великою кількістю віддалених офісів, адже всі точки підключення контролюються централізовано. Її перевага – мобільність, але недоліком є залежність від стабільності хмарного провайдера й складність у реалізації згідно з вимогами нормативно-правової бази України.

Cyber Resilience Architecture (CRA) зміщує фокус від запобігання до стійкості: як швидко система зможе відновитися після інциденту, не втративши при цьому критичної функціональності. Це ключова перевага для СЕДО під час воєнного стану, перебоїв електропостачання або масових атак. CRA дозволяє зберігати доступ до архівів, автоматично перемикатися між вузлами. Недоліком є необхідність надлишкової інфраструктури та сценарного планування на рівні сервісів.

Intent-Based Security Architecture (IBSA) – відносно нова концепція, яка базується не на політиках доступу, а на цілях дій. Наприклад, СЕДО перевіряє не лише «хто відкрив документ», а й запитує: «чи логічна ця дія в межах заявленої мети?» IBSA поєднує елементи штучного інтелекту, сценарного аналізу та цифрового паспорту транзакції. Архітектура надзвичайно перспективна, однак поки що має обмежену практичну реалізацію через складність формалізації цілей у держсекторі, тому також застосовується виключно для обробки відкритої інформації, або ж тоді, коли є відповідний дозвіл на використання від сертифікаційного органу.

Adaptive Security Architecture (ASA) – це модель, у якій кожен компонент (включно із СЕДО) може змінювати поведінку відповідно до загрозового ландшафту. Якщо підпис з’явився занадто швидко, з незвичної IP-адреси –

система може автоматично змінити політику доступу, викликати MFA, перенаправити аудит. ASA вважається ідеальним варіантом для поєднання з UEBA і DLP, особливо коли мова йде про конфіденційні документи.

Порівняльна таблиця архітектур безпеки, у якій зіставлені вищепредставлені моделі Zero Trust, SASE, IBSA, CRA та ASA, наведена у Додатку Б.

Для розроблення ефективної методики засобів захисту СЕДО, що функціонує з ДІР КІ в умовах підвищеної загрози, доцільним є інтегрування найкращих характеристик сучасних архітектур безпеки у єдину концептуальну модель. Від Zero Trust Architecture запозичується принцип відмови від апріорної довіри, що забезпечує постійну перевірку кожної дії користувача з урахуванням контексту взаємодії. Adaptive Security Architecture доповнює цей підхід механізмами автоматичної адаптації політик безпеки до змін у поведінковому шаблоні або загрозливому середовищі, дозволяючи системі самостійно активувати додаткові контрольні механізми (наприклад, багатофакторну автентифікацію чи обмеження функціоналу). У свою чергу, Cyber Resilience Architecture гарантує збереження працездатності СЕДО навіть за умов порушення цілісності окремих вузлів або втрати з’єднання з центральними компонентами, завдяки чому забезпечується юридична та технічна безперервність документообігу.

2.2 Принципи побудови ешелонованої системи захисту для СЕДО в критичній інфраструктурі

У системах електронного документообігу, що функціонують у межах критично важливих організацій, питання захисту інформації потребує не ізольованих рішень, а цілісного архітектурного підходу. У межах СЕДО це передбачає впровадження повної вертикалі захисту – від мережевого сегментування та контролю операційної системи до захисту СУБД прикладного рівня та самих цифрових документів.

2.2.1. Застосування багаторівневого захисту в архітектурі СЕДО КІ

Початковий рівень захисту починається на фізичному та мережевому рівнях. Тут реалізуються міжмережеві екрани, мережеві IPS/IDS, сегментовані підмережі VLAN, DMZ-зони та VPN-шлюзи. СЕДО повинна бути розгорнута таким чином, щоб зовнішній доступ (наприклад, для користувачів або зовнішніх систем, які інтегруються через API) відбувався виключно через проксі або балансувальні шлюзи з контролем контенту. Додатково впроваджуються системи глибокого аналізу трафіку (DPI), що дозволяють виявити підозрілу активність навіть у зашифрованих каналах TLS. У системах класу «e-Delivery» чи «X-Road» таке розділення структуровано на комунікаційний рівень, транспортний та сервісний, де кожен із них передає лише виключно визначені повідомлення, захищені цифровими підписами.

Операційна система має бути конфігурована з урахуванням принципів мінімальної доступності служб, обмеження доступу до ядра, захисту від ескалації привілеїв та цілісності системних файлів. Засоби типу «SELinux», «AppArmor» або «Windows Defender Application Control» можуть бути використані для забезпечення «білого списку» допустимих процесів. Також критично важливо мати журналювання дій з підвищеним привілеєм (наприклад, доступ root/administrator), із інтеграцією у централізовану SIEM-систему. У середовищі виконання – тобто на рівні хостів СЕДО – реалізуються антивірусні платформи з поведінковою евристикою, обмеження доступу до портів і регулярна перевірка контрольних сум бінарних компонентів.

На рівні СУБД система має реалізовувати політики поділу обов’язків (separation of duties) і багатогранну систему ролей. Наприклад, адміністратор бази не повинен мати доступ до розшифрованих даних, а бізнес-користувач – до DDL-операцій (створення/видалення таблиць, процедур). Використовуються засоби контролю запитів, моніторинг аномальної активності (наприклад, понаднормові запити до архівів), розмежування доступу до таблиць, а також до

колонок із чутливою інформацією. СЕДО мають також реалізовувати резервне копіювання бази у режимі «write-once-read-many» (WORM) для архівів, де важливо забезпечити незмінність документів після завершення їхнього життєвого циклу.

Це найбільш критичний рівень, оскільки саме тут відбувається авторизація, накладання КЕП, узгодження, передача документів та ініціація бізнес-процесів. Архітектура застосунку має підтримувати атрибутивні моделі контролю доступу (ABAC), при яких права користувача визначаються сукупністю параметрів: його роллю, поточним статусом документа, часом доби, IP-адресою, локалізацією сесії та попередньою поведінкою. Інтерфейс користувача має бути динамічним – лише функції, дозволені згідно з контекстом, мають бути доступні для виконання. Важливою складовою є аудит – автоматичне журналювання всіх операцій із документом із можливістю відтворення маршруту, змісту, часу та контексту кожної дії.

На рівні самого документа реалізується криптографічний захист: кожен документ повинен бути підписаний КЕП, забезпечений хеш-функцією, а в окремих випадках – шифруванням. Мають бути механізми перевірки достовірності підпису та відповідності структури документа еталонним шаблонам. Особливо важливими є timestamp-сервіси для фіксації моменту підпису та механізми валідації довіреного середовища (перевірка актуальності сертифіката, CRL/OCSP-запити). Для високочутливих даних додатково застосовуються політики автоматичного знищення після завершення терміну дії або в разі виходу за межі обробки.

2.2.2. Принцип найменших привілеїв у системах СЕДО

По суті, кожен привілей у СЕДО – це дозвіл на зміну стану цифрового документа: створення, погодження, підпис, делегування, зберігання або знищення. Навіть перегляд документа в захищеній зоні є актом доступу до службової інформації і тому має бути заздалегідь верифікованим,

протоколюваним і юридично виправданим. Таким чином, реалізація PoLP не може зводитися до простого адміністрування ролей – вона потребує прив'язки дозволу до нормативного статусу дії, кадрової функції та організаційної структури.

Однією з найсерйозніших загроз для повноцінної реалізації принципу «PoLP» в українських СЕДО є проблема «правового розриву»: в наявній практиці кадрових ротацій, багато облікових записів продовжують існувати після звільнення працівника або зміни його посадової функції. Доступи залишаються активними, права не переглядаються, і це створює приховану, кумулятивну вразливість системи. Понад 40% інцидентів витоку службової інформації в українських держустановах пов'язані з тим, що облікові дані осіб, які вже не є співробітниками, залишались активними понад 30 днів. Це демонструє, що технічне впровадження «PoLP» є марним без процедурної дисципліни.

Ще одна глибинна проблема – принципова складність ієрархії привілеїв у СЕДО, де права не є лінійними. Наприклад, користувач може мати право накласти КЕП на документ, але не переглядати його вміст; адміністратор може адмініструвати модулі, але не бачити зміст документів у базі даних; керівник має повноваження делегування, але не може втручатися у криптографічний процес. Такі розгалужені, неочевидні взаємозалежності потребують не тільки налаштування ролей, а й формалізації привілейованих маршрутів дій, де кожен крок верифікується через попередній – як у системі транзитивного допуску.

Провідні міжнародні практики (зокрема, урядові системи Естонії та Швейцарії) демонструють тенденцію до побудови детермінованих графів доступу – кожна операція в СЕДО можливе лише тоді, коли зумовлюючі дії вже відбулися у правильному порядку, і ця структура вбудована в архітектуру системи. Наприклад, документ не можна переслати або заархівувати, якщо немає підтвердження від підписувача і timestamp-сервера. Така модель є не просто жорсткою – вона логічно закріплює послідовність дозволів, що унеможливлює інтервенцію з боку технічного персоналу навіть при повному контролі над інфраструктурою.

У стратегічному сенсі, впровадження «PoLP» – це управлінська реформа в цифровому середовищі. Вона вимагає, щоб кадрова політика, штатний розпис, модель відповідальності та внутрішні регламенти документообігу були синхронізовані з цифровими політиками доступу. У протилежному разі система перетворюється на лабільну модель, де формальні дозволи не відповідають реальному статусу посадової особи. Найбільш прогресивні платформи (наприклад, в Іспанії, Сінгапурі та Єврокомісії) вже реалізують рекурсивний аудит привілеїв, коли після кожної значущої дії система автоматично перевіряє, чи відповідав рівень доступу діючого користувача структурі дозволів у момент здійснення операції. Це дозволяє виявити привілейовані "сліпі зони", де зловживання можливі без помітного порушення політики.

2.2.3. Сегментація мережі для ізоляції СЕДО та її компонентів

На відміну від традиційного підходу до ізоляції за VLAN або DMZ, у випадку СЕДО сегментація має бути функціональною: кожна логічна підсистема (реєстр, підписувач, архів, API-шлюз, аналітичний модуль) повинна розгортатися як ізольований сегмент без прямої адресної видимості до інших.

Причина такої вимоги криється у самій природі СЕДО як багатокомпонентної системи, де кожен модуль має власну зону ризику. Наприклад, шлюз API, який обслуговує зовнішні запити (зокрема – від третіх систем через REST або SOAP), є природною точкою потенційного входу шкідливого трафіку. Якщо він розміщений у загальному мережевому середовищі з внутрішнім ядром документообігу, успішна експлуатація вразливості в API одразу відкриває доступ до маршрутизатора документів або сховища. Саме тому, наприклад, у системі «Estonian X-Road» усі критичні модулі розміщуються в транзитивно ізольованих зонах, між якими взаємодія можлива лише через контрольовані криптографічні шлюзи, які не мають зворотнього каналу.

Особливого значення сегментація набуває у державних СЕДО, де часто співіснують внутрішні й міжвідомчі процеси, що працюють на спільному стеку

технологій. Наприклад, маршрути погодження внутрішніх документів установи та взаємодія з зовнішніми системами типу «Трембіта», «eHealth» чи «ЦНАПів» – це суттєво різні рівні довіри. В українських системах, таких як СЕДО Мінсоцполітики або окремі модулі електронного судочинства, дані процеси часто реалізовані у спільній інфраструктурі, що ускладнює побудову логічно захищених контурів.

Критичним елементом сегментації є створення односторонніх потоків (data diode logic) між сегментами з різним рівнем чутливості. Наприклад, архів не повинен мати прямий вихід до мережі – запити надходять через внутрішній обробник, який пересилає заздалегідь схвалений документ, але не дозволяє ініціювати вихідну передачу з боку архіву. Така логіка застосовується, зокрема, у системах оборонного СЕДО в Німеччині та Ізраїлі. Для України доцільним є використання сегментів «pull-only», де віддалені вузли СЕДО мають право лише запитувати інформацію в центрального реєстру, але не «штовхати» дані без перевірки.

Окрім фізичної або віртуальної ізоляції, сегментація повинна бути підтримана інституційно-рольовою політикою: адміністратори окремих зон не повинні мати доступ до систем керування іншими сегментами. Наприклад, технічна команда, відповідальна за криптопроцедури, не повинна мати привілеїв у сегменті маршрутизації або погодження, навіть якщо це – одна організаційна одиниця. У європейській практиці така модель називається administrative isolation domain, і вона особливо ефективна при впровадженні архітектур Zero Trust.

Ще одна особливість, яка рідко враховується у вітчизняній практиці, – технологічна поведінка під час порушення. При правильно реалізованій сегментації інцидент у фронтенд-зоні (наприклад, DoS або CSRF) повинен бути повністю ізольований і не впливати на бекенд-процеси СЕДО. Це досягається не лише мережею, а й асинхронністю передачі даних: міжзонні транзакції повинні проходити через черги повідомлень із контрольованим протоколюванням (message broker + token-based access).

2.3 Методи та моделі аналізу ризиків інформаційної безпеки СЕДО

Оцінка ризиків в інформаційній безпеці СЕДО вимагає врахування низки принципових особливостей, які кардинально відрізняють такі системи від традиційних IT-середовищ. По-перше, об’єкт аналізу в СЕДО не є чисто технічним – ним виступає цифровий документ, який є одночасно даними, транзакцією, об’єктом юридичної відповідальності й доказовим слідом. По-друге, СЕДО не є системою з централізованим життєвим циклом даних – вона інтегрує мережі прийняття рішень, маршрути між людьми, служби обробки, криптографічні інструменти та модулі архівування.

2.3.1. Специфіка адаптації методів оцінки ризиків до особливостей документоорієнтованих систем

У контексті СЕДО, які функціонують у КІ, традиційні методи аналізу ризиків (таких як ISO/IEC 27005, OCTAVE, NIST SP 800-30, FAIR) виявляються лише частково релевантними, оскільки більшість із них були розроблені для IT-інфраструктур загального призначення, де дані виступають у формі абстрактних інформаційних об’єктів. Натомість документоорієнтовані системи мають справу з конкретними цифровими артефактами, що несуть юридичну, регуляторну й функціональну відповідальність, а це потребує включення додаткових змінних до моделей оцінки ризику – таких як маршрут документа, стадія життєвого циклу, правовий статус, роль ініціатора та ступінь довіри до джерела.

Аналіз ризиків у СЕДО має бути побудований не лише навколо інформаційних активів, а й навколо процесних точок – «вузлів уразливості», пов’язаних із транзакційними подіями (наприклад, передача на підпис, делегування прав, архівування тощо). Саме тому підходи накшталт OCTAVE Allegro, що орієнтуються на активи з урахуванням контексту використання, доцільно адаптувати через їх інтеграцію з моделюванням поведінки користувачів

(UEBA) та логікою цифрових слідів. Крім того методи монетаризації загроз із FAIR можуть бути релевантними при побудові ризик-карт у СЕДО, однак вимагають переосмислення категорій впливу – юридичні, регуляторні, комунікаційні втрати стають тут важливішими за суто фінансові [27].

Однією з перспективних моделей адаптації виступає Document Flow Risk Mapping (DFRM), яка моделює документ як динамічний актив, що змінює свій рівень ризику залежно від маршрутної логіки, ролей учасників, середовища обміну та криптографічного статусу. У межах DFRM кожен етап – створення, погодження, підписання, архівація – оцінюється з точки зору вразливості до чотирьох типів атак: підробка, витік, блокування, модифікація.

Іншою інноваційною практикою є застосування «cyber-risk twin» – цифрового двійника маршруту документа, який у тестовому середовищі імітує стандартну поведінку документа, дозволяючи моделювати вплив втручання (наприклад, несанкціонованої зміни маршруту, обхідного підпису, повторного використання шаблону тощо) та прогнозувати потенційні вектори компрометації. Дана методика вже апробована в пілотному проєкті на базі платформи «Трембіта» і може бути масштабована для комплексних СЕДО.

Водночас доцільно впроваджувати методи «Bayesian risk scoring», які дозволяють оцінити ймовірність реалізації загрози на основі історії документопотоків та поведінкових патернів. У СЕДО це особливо важливо, оскільки навіть одна нетипова дія (наприклад, змінений маршрут документа в позаробочий час із зовнішнього IP) може бути маркером атаки зсередини.

2.3.2. Контекстуалізація сучасних моделей управління ризиками у середовищі СЕДО

Такі системи, як СЕДО, потребують методології, здатної фіксувати не лише інцидент, а передумову небезпеки, яка ще не реалізувалася, але вже є структурною аномалією. Для задоволення цієї потреби у межах даного

дослідження розроблено модель «CSAR-D» (Contextual and Semantic Adaptive Risk for Documents).

Суть моделі «CSAR-D» полягає у трактуванні ризику не як суми факторів загроз, а як відхилення цифрової події від очікуваної норми. У даній моделі документ оцінюється не як файл, а як носій дії у цифровій процедурі, що має атрибути (роль, маршрут, підпис, час, зміст) та формується відповідно до заданого нормативного шаблону. Якщо подія – наприклад, погодження документа – відбувається поза цим шаблоном (не тим підписантом, не в той час, без належної послідовності або зі зміненим змістом), то система трактує це як контекстну аномалію, навіть якщо всі дії технічно дозволені.

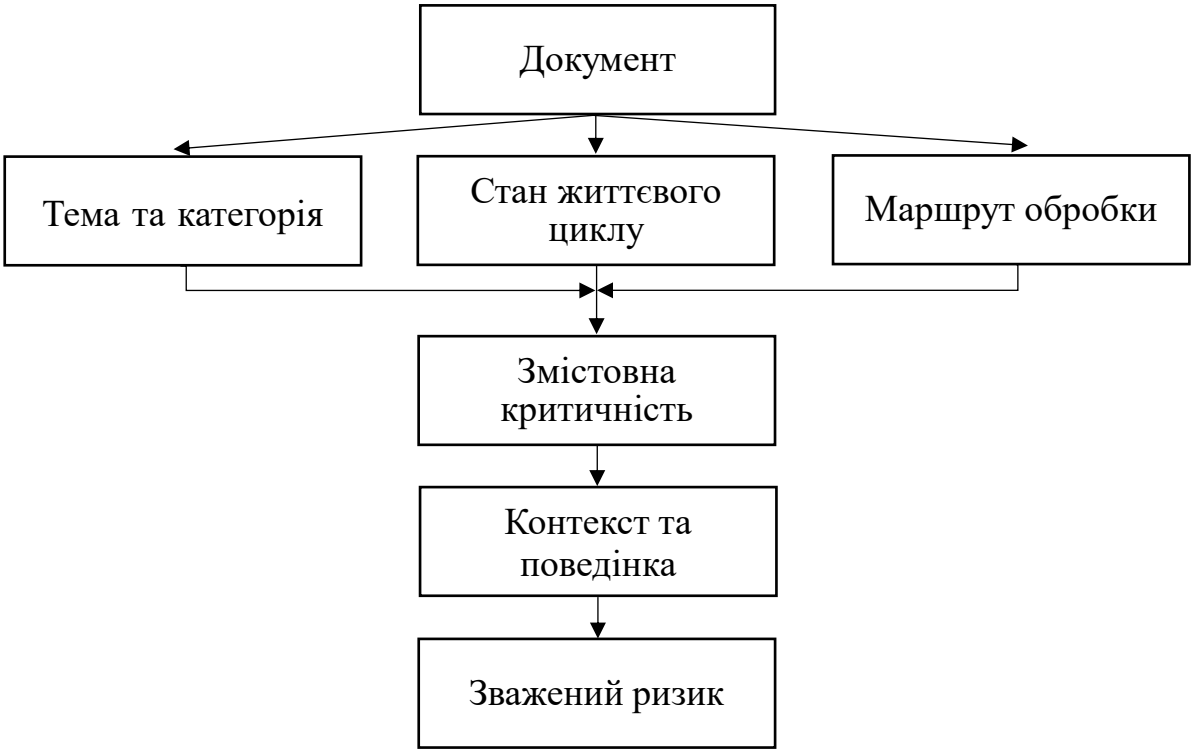


Рисунок 2.2 – Схема критичності цифрових дій

На відміну від класичних моделей ризик-менеджменту, «CSAR-D», представлена схема критичності на рисунку 2.2, не оперує лише категоріями вразливість/наслідок. У її основі – динамічна семантична логіка, де кожен документ має «критичний профіль», що змінюється в залежності від:

- Етапу життєвого циклу (чернетка, у погодженні, підписаний, архівований);
- Типу взаємодії (внутрішній/зовнішній обмін);
- Ролі користувача (ініціатор, рецензент, підписант);
- Поведінкової відповідності (частота, часові рамки, пристрій);
- Нормативного контексту (регламент/наказ/контракт).

Модель «CSAR-D» дозволяє не лише оцінити ризик, а й автоматично моделювати відповідь системи: наприклад, активувати додаткову перевірку, змінити маршрут, відкласти дію до схвалення вищим рівнем або заборонити операцію з фіксацією причин. Завдяки цьому «CSAR-D» може діяти не як інструмент реагування, а як запобіжна логіка цифрової поведінки, вбудована у саму структуру СЕДО.

Центральним інструментом «CSAR-D» є «схема критичності цифрових дій», яка узгоджує тип документа, тип дії та поведінковий контекст. Наприклад, погодження документа категорії «фінансове розпорядження» у позаробочий час із нового пристрою – це подія високої критичності; натомість перегляд чернетки службового листа з робочої станції – подія низького ризику. Така матриця дає змогу автоматизувати ризик у реальному часі, замість того щоб покладатися на формальні звіти або ручний аудит.

ВИСНОВКИ ДО РОЗДІЛУ 2

У межах другого розділу кваліфікаційної роботи було проведено глибокий аналіз та систематизацію існуючих підходів і засобів захисту інформації, що є релевантними для СЕДО в КІ. Дослідження підтвердило, що ефективний захист СЕДО є не опціональним, а життєво необхідним, зважаючи на критичну важливість інформації, яка в ній обробляється.

По-перше, здійснено огляд основних категорій засобів захисту, поділених на організаційні, програмні, апаратні та інтегровані архітектурні рішення . Визначено, що організаційні механізми забезпечують не лише нормативну базу,

а й формують безпеки, адаптуючись до динамічного середовища загроз через впровадження контекстно-чутливих політик та архітектури Zero Trust. Підкреслено, що ефективність цих заходів залежить від системного інтегрування з людським фактором, вимірюється показниками оперативного реагування та постійної адаптації. Запропонована концепція «цифрового двійника інформаційної безпеки» є перспективним напрямом для проактивного моделювання ризиків та оптимізації захисту.

По-друге, розглянуто програмне забезпечення як ключовий інструмент технічного захисту СЕДО. Деталізовано механізми рольового та атрибутивного контролю доступу, криптографічної обробки даних, включаючи накладання КЕП та його сумісність із сервісами перевірки чинності. Особливу увагу приділено функціоналу DLP-рішень, SIEM-платформ та механізмів контролю версій, що є критично важливими для виявлення аномалій, запобігання витокам та забезпечення незмінності документів.

По-третє, проаналізовано апаратну складову системи захисту, що включає засоби зберігання та криптографічної обробки даних. Визначено роль персональних токенів та смарт-карт для безпечного підпису, а також значення TPM-модулів для контролю цілісності серверної інфраструктури. Окрема увага приділена ефективності WORM-сховищ для довгострокового архівування незмінних цифрових документів та застосуванню апаратних VPN-шлюзів для ізоляції каналів зв’язку.

По-четверте, проведено аналіз інтегрованих архітектур безпеки та концептуальних моделей кіберзахисту СЕДО в КІ. Розглянуто такі підходи, як «Zero Trust Architecture» (ZTA), «Secure Access Service Edge» (SASE), «Cyber Resilience Architecture» (CRA), «Intent-Based Security Architecture» (IBSA) та «Adaptive Security Architecture» (ASA). Обґрунтовано, що для запобігання підвищеній загрозі КІ доцільним є інтегрування найкращих характеристик цих архітектур: принципу відмови від апріорної довіри (ZTA), механізмів автоматичної адаптації політик безпеки (ASA) та гарантування працездатності системи навіть за умови порушення окремих вузлів (CRA).

По-п’яте, деталізовано принципи побудови ешелонованої системи захисту для СЕДО. Це включає багаторівневий захист (від фізичного та мережевого до рівня застосунку та документа), застосування принципу найменших привілеїв, що вимагає прив’язки дозволів до нормативного статусу та кадрової функції, а також функціональну сегментацію мережі для ізоляції логічних підсистем СЕДО.

Нарешті, було розглянуто методи та моделі аналізу ризиків інформаційної безпеки СЕДО. Доведено, що традиційні методи оцінки ризиків є лише частково релевантними для документоорієнтованих систем, що вимагає адаптації підходів до врахування юридичної, регуляторної та функціональної відповідальності цифрових артефактів. Запропоновано нову модель – «CSAR-D» (Contextual and Semantic Adaptive Risk for Documents), яка трактує ризик як відхилення цифрової події від очікуваної норми та дозволяє динамічно оцінювати критичність дій на основі етапу життєвого циклу документа, ролі користувача та поведінкової відповідності. Це забезпечує можливість не лише виявлення вразливостей, а й оперативної ідентифікації системних відхилень від безпечного маршруту обробки даних.

Таким чином, у даному розділі не лише класифіковано та проаналізовано засоби захисту, а й сформульовано концептуальну вимогу до ешелонованої, семантично-чутливої та подієво-контекстуальної архітектури безпеки. Кожна дія над документом у цій архітектурі розглядається як транзакція довіри з динамічним рівнем ризику, що є фундаментальним підґрунтям для формування власної моделі забезпечення інформаційної безпеки СЕДО.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ ВИБОРУ ТА АНАЛІЗУ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ СЕДО ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Загальна концепція моделі вибору та аналізу засобів захисту СЕДО для критичної інфраструктури

При виборі та аналізі КЗЗ СЕДО для КІ необхідно керуватися низкою фундаментальних принципів. Ці принципи допомагають забезпечити ефективність, відповідність та сталість системи захисту в умовах високих ризиків, характерних для КІ. Загальна система принципів наведена на рис. 3.1.

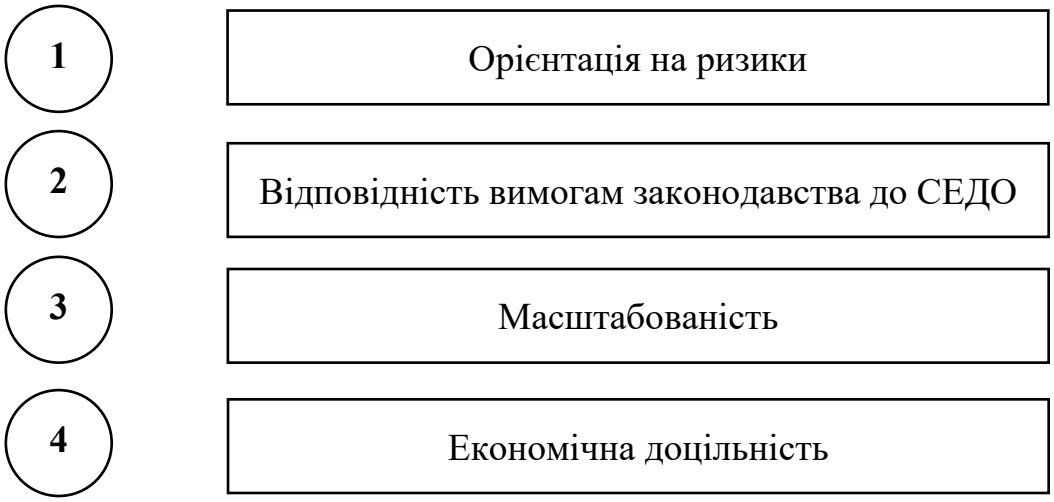


Рисунок 3.1 – Загальна система принципів вибору та аналізу КЗЗ СЕДО для КІ

Розглянемо дані принципи більш детально.

1. Орієнтація на ризики. Захист СЕДО КІ має бути побудований на основі ретельного аналізу та управління ризиками. Це означає, що заходи безпеки обираються та впроваджуються пропорційно до ідентифікованих загроз, вразливостей та потенційних наслідків для функціонування КІ.

Застосування до СЕДО КІ:

- Ідентифікація активів. Визначення всіх критично важливих електронних документів, даних, програмного забезпечення, апаратного забезпечення та інфраструктури, задіяних у СЕДО.
- Оцінка загроз і вразливостей. Виявлення потенційних загроз (наприклад, кібератаки, відмови обладнання, людські помилки) та вразливостей у системі.
- Аналіз впливу. Оцінка потенційних наслідків (фінансових, репутаційних, операційних, для безпеки життя) у разі реалізації загрози. Для КІ це може означати порушення роботи життєво важливих послуг.
- Вибір контрзаходів. Впровадження захисних заходів, які ефективно знижують ризики до прийнятного рівня. Наприклад, для захисту конфіденційності критичних документів може бути обрано сильне шифрування та строгий контроль доступу.
- Постійний моніторинг. Ризики змінюються, тому система захисту повинна постійно переглядатися та адаптуватися до нових загроз.

2. Відповідність вимогам законодавства до СЕДО. Комплекс засобів захисту повинен відповідати всім чинним національним та міжнародним нормативно-правовим актам, стандартам та регуляторним вимогам, що стосуються захисту інформації в СЕДО, особливо в контексті КІ [28].

Застосування до СЕДО КІ:

- Закони України. Дотримання вимог Законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про електронні довірчі послуги», «Про критичну інфраструктуру», «Про захист персональних даних».
- Нормативні документи Держспецзв’язку. Обов’язкове виконання вимог НД ТЗІ, зокрема щодо створення КСЗІ з підтвердженою відповідністю для державних СЕДО та СЕДО КІ, які обробляють інформацію, вимога щодо захисту якої встановлена законом.
- Галузеві стандарти. Врахування специфічних вимог безпеки для конкретного сектору КІ (енергетика, транспорт, фінанси тощо).

- Міжнародні стандарти. Розглядались в першому розділі.

3. Масштабованість. Обрані засоби захисту та архітектура СЗІ повинні бути здатними до розширення та адаптації до зростаючих обсягів даних, збільшення кількості користувачів, зміни бізнес-процесів та технологічного розвитку СЕДО.

Застосування до СЕДО КІ:

- Зростання обсягів документів. СЕДО КІ можуть генерувати та обробляти величезні обсяги електронних документів. Система захисту має бути спроможною ефективно захищати ці зростаючі обсяги без значного зниження продуктивності.
- Збільшення кількості користувачів. Масштабованість має враховувати можливе збільшення кількості користувачів та їхніх ролей, забезпечуючи при цьому гнучке управління доступом.
- Інтеграція з іншими системами. Можливість інтеграції СЕДО з іншими критично важливими системами КІ без компрометації безпеки.
- Адаптація до нових технологій. Засоби захисту повинні бути достатньо гнучкими, щоб адаптуватися до впровадження нових технологій у СЕДО (наприклад, хмарні рішення, мобільний доступ).
- Гнучкість архітектури. Побудова модульної та гнучкої архітектури СЗІ, яка дозволяє додавати або оновлювати окремі компоненти без повного перероблення системи.

4. Економічна доцільність. Вибір та впровадження комплексу засобів захисту повинні бути економічно обґрунтованими, тобто витрати на безпеку мають бути пропорційними до рівня ризиків та цінності інформації, що захищається.

Застосування до СЕДО КІ:

- аналіз «витрати-вигода». Порівняння потенційних збитків від реалізації ризиків з вартістю впровадження та підтримки заходів безпеки. Для КІ вартість наслідків може бути надзвичайно високою, тому інвестиції в безпеку є критично важливими;

- оптимізація інвестицій. Вибір рішень, які забезпечують максимальний рівень захисту за прийнятну вартість, без надлишкових витрат на захист від малоймовірних або незначних загроз;
- ефективне використання ресурсів. Забезпечення того, щоб засоби захисту не створювали невиправданого навантаження на операційні процеси та не вимагали надмірних людських ресурсів для управління;
- довгострокове планування. Врахування не тільки початкових витрат, але й витрат на підтримку, оновлення, навчання персоналу та ліцензування протягом усього життєвого циклу СЕДО.

Дотримання цих принципів дозволяє створити надійну, ефективну та адаптивну систему захисту СЕДО для КІ, яка зможе протистояти сучасним кіберзагрозам і забезпечити безперебійне функціонування життєво важливих систем. Окрім основних принципів, необхідно визначити етапи функціонування моделі вибору та аналізу КЗЗ СЕДО для КІ.

Етапи функціонування моделі вибору та аналізу КЗЗ СЕДО для КІ логічно випливають з її базових принципів і формують безперервний цикл, спрямований на постійне підвищення рівня кібербезпеки (рис. 3.2). Ця модель є ітеративною та гнучкою, що дозволяє адаптуватися до змін у середовищі загроз і вимог.

Рисунок 3.2 – Етапи функціонування моделі вибору та аналізу КЗЗ СЕДО для КІ

Розглянемо етапи, представлені на рис. 3.2 більш детально.

1. Етап підготовки та планування. Цей етап є фундаментальним для успішного впровадження СЗІ. Він включає збір необхідної інформації, формування команди та визначення цілей.

1.1 Визначення області застосування (Scope). Чітке окреслення меж СЕДО, що підлягає захисту. Це включає всі компоненти системи: апаратне забезпечення, програмне забезпечення, мережеву інфраструктуру, дані, інтеграції з іншими системами та користувачів.

1.2 Формування команди. Залучення ключових стейкхолдерів, включаючи керівництво, фахівців з інформаційної безпеки, IT-спеціалістів, юристів та представників бізнес-підрозділів, які користуються СЕДО.

1.3 Визначення цілей безпеки. Формулювання конкретних, вимірюваних, досяжних, релевантних та обмежених у часі (SMART) цілей захисту інформації (наприклад, забезпечення доступності СЕДО на рівні 99.9%, зниження кількості інцидентів з витоком даних на 20%).

1.4 Вивчення регуляторних вимог. Детальне вивчення всіх чинних законів, нормативних актів (ДСТУ, НД ТЗІ), галузевих стандартів та політик, що застосовуються до СЕДО в КІ.

2. Етап аналізу ризиків та оцінки потреб. На цьому етапі відбувається глибокий аналіз поточного стану та потенційних загроз. Це є ядром принципу орієнтації на ризики.

2.1 Ідентифікація активів. Складання повного переліку інформаційних активів, що обробляються в СЕДО (електронні документи, метадані, бази даних), а також пов’язаних з ними IT-ресурсів.

2.2 Оцінка цінності активів. Визначення важливості кожного активу для функціонування КІ та оцінка потенційних наслідків (фінансових, репутаційних, оперативних, безпекових) у разі їх компрометації.

2.3 Ідентифікація загроз та вразливостей. Виявлення потенційних джерел небезпеки (кібератаки, внутрішні загрози, технічні збої, природні

катастрофи) та слабких місць у поточній системі (відсутність шифрування, слабкі паролі, неоновлене ПЗ).

2.4 Аналіз ризиків. Оцінка ймовірності реалізації кожної загрози через виявлені вразливості та масштабу можливого збитку. Це дозволяє визначити рівень ризику (низький, середній, високий, критичний).

2.5 Визначення допустимого рівня ризику. Узгодження з керівництвом організації рівня ризику, який вважається прийнятним.

2.6 Оцінка поточного стану захисту. Аналіз вже існуючих засобів та заходів захисту, їх ефективності та відповідності виявленим ризикам.

3. Етап вибору та проєктування засобів захисту. Базуючись на результатах попереднього аналізу, відбувається безпосередній вибір та планування конкретних рішень. Тут активно застосовуються принципи відповідності вимогам законодавства, масштабованості та економічної доцільності.

3.1 Вибір стратегії управління ризиками. Вирішення, як реагувати на кожен ризик: уникнути, зменшити, передати (застрахувати) або прийняти.

3.2 Вибір та обґрунтування засобів захисту. Підбір конкретних технічних (наприклад, засоби криптографічного захисту, системи контролю доступу, DLP-системи, антивіруси) та організаційних (політики, процедури, навчання) заходів безпеки, які дозволять знизити ризики до прийнятного рівня.

3.3 Проєктування архітектури СЗІ. Розробка детальної схеми розташування та взаємодії всіх компонентів захисту в рамках СЕДО. Врахування можливості масштабування системи в майбутньому.

3.4 Розробка технічного завдання (ТЗ). Формулювання детальних вимог до системи захисту, що стане основою для її впровадження.

3.5 Аналіз економічної доцільності. Оцінка витрат на впровадження, експлуатацію та підтримку обраних засобів захисту у співвідношенні з потенційними збитками від нереалізованих ризиків.

4. Етап впровадження та реалізації. Це практичний етап, під час якого відбувається фізична реалізація запланованих заходів.

4.1 Закупівля та налаштування. Придбання необхідного обладнання та програмного забезпечення, його інсталяція та конфігурація відповідно до розробленого проєкту.

4.2 Розробка та впровадження політик і процедур. Створення внутрішніх документів, що регламентують порядок використання СЕДО та дотримання правил безпеки.

4.3 Навчання персоналу. Проведення тренінгів для всіх користувачів СЕДО та ІТ-персоналу щодо правил роботи з системою, політик безпеки та дій у разі інцидентів.

4.4 Тестування СЗІ. Проведення комплексного тестування всіх компонентів СЗІ для перевірки їх функціональності та ефективності.

5. Етап моніторингу, аудиту та підтримки. Цей етап є безперервним і критично важливим для підтримання високого рівня безпеки, що відповідає динамічній природі загроз.

5.1 Моніторинг подій безпеки. Постійний збір та аналіз журналів безпеки, виявлення підозрілої активності та інцидентів.

5.2 Реагування на інциденти. Розробка та виконання планів реагування на кіберінциденти, включаючи виявлення, стримування, усунення та відновлення.

5.3 Регулярний аудит та перевірки. Проведення внутрішніх та зовнішніх аудитів СЗІ для оцінки її ефективності, відповідності вимогам та виявлення нових вразливостей.

5.4 Актуалізація загроз та ризиків. Постійний перегляд моделі загроз та моделі порушника, оскільки кіберландшафт постійно змінюється.

5.5 Оновлення та вдосконалення. Систематичне оновлення програмного забезпечення, апаратного забезпечення та організаційних заходів захисту у відповідь на нові загрози, технологічні зміни та результати аудитів. Це забезпечує принцип постійного вдосконалення.

Ці етапи формують цикл управління безпекою, який дозволяє організації КІ адаптувати свою систему захисту СЕДО до нових викликів та забезпечувати стабільне й безпечне функціонування в довгостроковій перспективі.

3.2 Модель вибору та аналізу комплексу засобів захисту для систем електронного документообігу в критичній інфраструктурі

Модель вибору та аналізу КЗЗ для систем електронного документообігу (СЕДО) в КІ, ґрунтуючись на принципах, які були представлені в 3.1, а саме: орієнтація на ризики, відповідність вимогам законодавства, масштабованість та економічна доцільність. Ця модель є циклічною, що дозволить постійно вдосконалювати систему захисту.

Представимо модель у вигляді направленого графа (рис. 3.3). Для цього визначмо елементи графа:

A – Етап 1. Підготовка та планування;

B – Визначення області застосування та цілей безпеки;

C – Етап 2. Аналіз ризиків та оцінка потреб;

D – Ідентифікація активів та загроз. Аналіз ризиків. Визначення допустимого ризику;

E – Етап 3. Вибір та проєктування засобів захисту;

F – Вибір стратегії управління ризиками. Обґрунтування засобів захисту. Проєктування архітектури СЗІ. Економічна доцільність;

G – Етап 4. Впровадження та реалізація;

H – Закупівля, налаштування та інтеграція. Розробка політик та процедур. Навчання персоналу;

I – Етап 5. Моніторинг, аудит та підтримка;

J – Моніторинг подій. Реагування на інциденти. Регулярний аудит. Актуалізація загроз та ризиків. Оновлення та вдосконалення;

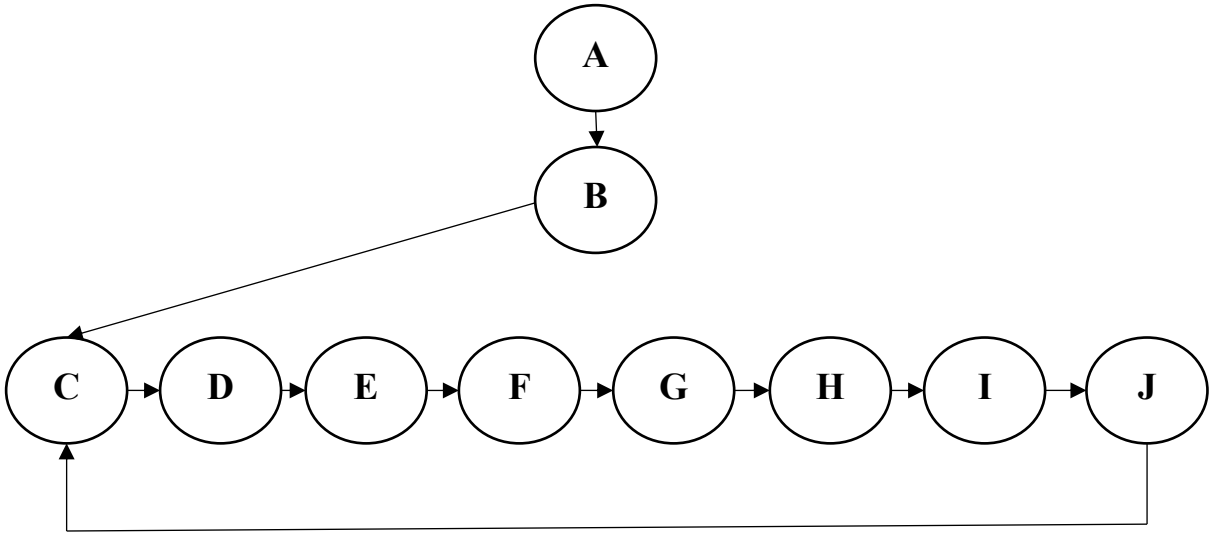


Рисунок 3.3 – Модель вибору та аналізу комплексу засобів захисту для систем електронного документообігу в критичній інфраструктурі

Дана модель є послідовним, але ітеративним процесом, що дозволяє системно підходити до захисту СЕДО в КІ, враховуючи небезпеку та динамічність кіберзагроз.

Розкриємо етапи представленої моделі.

Етап 1: Підготовка та планування. Цей етап закладає фундамент усієї моделі, визначаючи рамки та цілі для подальшої роботи.

Визначення області застосування (Scope):

- чітке окреслення всіх компонентів СЕДО, що потребують захисту (апаратне та програмне забезпечення, мережі, бази даних, електронні документи, метадані, інтеграції з іншими системами, користувачі);
- встановлення меж відповідальності за безпеку СЕДО, особливо у випадках зовнішнього підрядника або хмарних рішень.

Формування команди:

- залучення ключових фахівців: керівництво, IT-безпека, IT-операції, юристи, представники бізнес-процесів (користувачі СЕДО);
- призначення відповідальних осіб за кожен етап процесу.

Визначення цілей безпеки:

- формулювання конкретних, вимірюваних, досяжних, релевантних та обмежених у часі (SMART) цілей (наприклад, «забезпечити цілісність усіх електронних документів на 99.9%»);
- узгодження цілей із загальною стратегією кібербезпеки організації та вимогами для КІ.

Вивчення нормативно-правової бази:

- детальний аналіз чинних законів України («Про захист інформації», «Про кібербезпеку», «Про електронні довірчі послуги», «Про критичну інфраструктуру»);
- вивчення нормативно-технічних документів Держспецзв'язку (НД ТЗІ), постанов Кабінету Міністрів України, що стосуються захисту інформації в державних системах та об'єктах КІ;
- врахування галузевих стандартів та міжнародних фреймворків (ISO/IEC 27001, NIST CSF) як найкращих практик.

Етап 2: Аналіз ризиків та оцінка потреб. Це ключовий етап, що реалізує принцип орієнтації на ризики та формує основу для вибору конкретних заходів захисту.

Ідентифікація та оцінка цінності активів:

- складання реєстру всіх інформаційних активів (електронні документи, шаблони, метадані, логіни, конфігураційні файли тощо) та системних компонентів СЕДО;
- оцінка критичності кожного активу для функціонування КІ (наприклад, вплив на безперервність послуг, безпеку людей, екологію, фінансову стабільність).

Визначення моделі загроз та моделі порушника:

- модель загроз. Ідентифікація потенційних кіберзагроз у кіберпросторі [29] (наприклад, DDoS-атаки, фішинг, шкідливе ПЗ, інсайдери, технічні збої, стихійні лиха) та їхніх джерел;

- модель порушника. Аналіз потенційних внутрішніх та зовнішніх порушників (наприклад, кіберзлочинці, хактивісти, державні спонсоровані групи, недбалий персонал) та їхніх можливих мотивів, ресурсів та можливостей.

Виявлення вразливостей:

- аналіз слабких місць у поточній архітектурі СЕДО, конфігурації, програмному забезпеченні, мережах;
- проведення сканування вразливостей, тестів на проникнення (пентестів), аудитів безпеки.

Аналіз та оцінка ризиків:

- кількісна або якісна оцінка ймовірності реалізації кожної загрози через виявлені вразливості;
- оцінка потенційного впливу (збитку) у разі реалізації ризику для КІ;
- розрахунок рівня ризику (ймовірність впливу);
- визначення допустимого рівня ризику;
- узгодження з керівництвом організації рівня ризику, який вважається прийнятним для функціонування СЕДО в КІ, враховуючи галузеві особливості та регуляторні вимоги.

Оцінка поточного стану захисту:

- аудит існуючих заходів безпеки, їх відповідності нормативним вимогам та ефективності у зниженні виявлених ризиків.

Етап 3: Вибір та проєктування засобів захисту. На цьому етапі відбувається розробка конкретних рішень, з урахуванням принципів масштабованості та економічної доцільності, а також відповідності вимогам законодавства.

Вибір стратегії управління ризиками. Для кожного ідентифікованого ризику обирається стратегія – уникнення (усунення джерела ризику), зменшення (впровадження контролів), передача (страхування, аутсорсинг), прийняття (якщо ризик нижчий за допустимий).

Вибір та обґрунтування засобів захисту:

- технічні засоби. Криптографічний захист інформації (КЕП та печатки, шифрування даних у стані спокою та в русі), системи контролю доступу, міжмережеві екрани (Firewall), системи виявлення/запобігання вторгнень (IDS/IPS), системи управління подіями безпеки та інформацією (SIEM), антивірусні рішення, DLP-системи, системи резервного копіювання та відновлення;
- організаційні заходи. Розробка політик (парольної політики, політики використання ресурсів), процедур (реагування на інциденти, управління змінами), навчання персоналу, фізична безпека об’єктів.

Всі засоби повинні бути сертифіковані або мати експертні висновки Держспецзв’язку, якщо це вимагається законодавством для КІ.

Проєктування архітектури СЗІ:

- розробка детальної схеми розташування та взаємодії всіх елементів СЗІ в рамках СЕДО та її інтеграції з загальною ІТ-інфраструктурою КІ;
- врахування можливості подальшого масштабування системи без значних архітектурних змін;
- розробка технічного завдання (ТЗ) на КСЗІ;
- формулювання детальних вимог до системи захисту, що включає функціональні та нефункціональні вимоги, критерії приймання, вимоги до документування.

Аналіз економічної доцільності:

- розрахунок початкових витрат (закупівля, впровадження) та операційних витрат (підтримка, ліцензії, навчання);
- порівняння цих витрат з потенційними збитками, яких можна уникнути завдяки впровадженню заходів безпеки. Обґрунтування інвестицій.

Етап 4: Впровадження та реалізація. Даний етап включає практичне втілення розроблених рішень.

Закупівля, налаштування та інтеграція:

- придбання обраних засобів захисту;
- їх встановлення, конфігурація та інтеграція в існуючу інфраструктуру СЕДО;
- виконання робіт згідно з розробленим ТЗ на КСЗІ.

Розробка та впровадження політик і процедур. Розробка та затвердження внутрішніх документів, що деталізують правила використання СЕДО та вимоги безпеки для користувачів та адміністраторів. Наприклад, політики доступу, політики використання мобільних пристроїв, процедури резервного копіювання.

Навчання персоналу:

- проведення обов'язкових тренінгів для всіх категорій користувачів СЕДО та ІТ-персоналу;
- навчання правилам безпечного використання СЕДО, розпізнавання загроз (наприклад, фішингу), порядку дій у разі інцидентів.

Документування СЗІ. Підготовка повного пакету документів щодо КСЗІ, необхідного для її атестації. Атестація КСЗІ (для державних СЕДО та СЕДО КІ з підвищеними вимогами). Проходження державної експертизи КСЗІ та отримання Атестата відповідності від Держспецзв'язку, що підтверджує належний рівень захисту інформації.

Етап 5: Моніторинг, аудит та підтримка. Це безперервний цикл, що гарантує підтримання актуального рівня безпеки та постійне вдосконалення системи.

Моніторинг подій безпеки:

- безперервний збір та аналіз логів (журналів) подій з усіх компонентів СЕДО та СЗІ;
- використання SIEM-систем для кореляції подій та виявлення аномалій та потенційних інцидентів.
- Реагування на інциденти:

- розробка та регулярне оновлення планів реагування на кіберінциденти;
- швидке та ефективне реагування на виявлені інциденти: ідентифікація, стримування, усунення наслідків, відновлення та аналіз причин;
- взаємодія з CERT-UA та іншими державними органами, як того вимагає законодавство для КІ.

Регулярний аудит та перевірки:

- проведення планових внутрішніх та зовнішніх аудитів безпеки для оцінки ефективності СЗІ, її відповідності політикам та нормативним вимогам;
- проведення тестів на проникнення, сканування вразливостей для виявлення нових слабких місць.

Актуалізація загроз та ризиків:

- постійний моніторинг кіберландшафту, нових загроз та атак;
- регулярний перегляд моделі загроз та моделі порушника;
- переоцінка ризиків з урахуванням змін у системі, бізнес-процесах та зовнішньому середовищі.

Оновлення та вдосконалення:

- систематичне оновлення програмного та апаратного забезпечення СЗІ, застосування патчів безпеки;
- адаптація політик, процедур та інших організаційних заходів у відповідь на нові виклики та результати аудитів;
- впровадження нових технологій та рішень для підвищення рівня захисту.

Дана модель дозволяє організаціям КІ побудувати надійну, гнучку та економічно виправдану систему захисту СЕДО, що є ключовим для їхньої кіберстійкості та безперебійного функціонування.

3.3 Рекомендації, що лежать в основі побудови моделі вибору та аналізу комплексу засобів захисту СЕДО для критичної інфраструктури

Побудова ефективної моделі вибору та аналізу комплексу засобів захисту СЕДО для КІ вимагає не лише розуміння етапів, а й дотримання низки ключових рекомендацій (рис. 3.4). Ці рекомендації допомагають забезпечити те, що процес є не тільки формальним, а й глибоко інтегрованим у життєвий цикл організації та адаптованим до специфіки КІ.

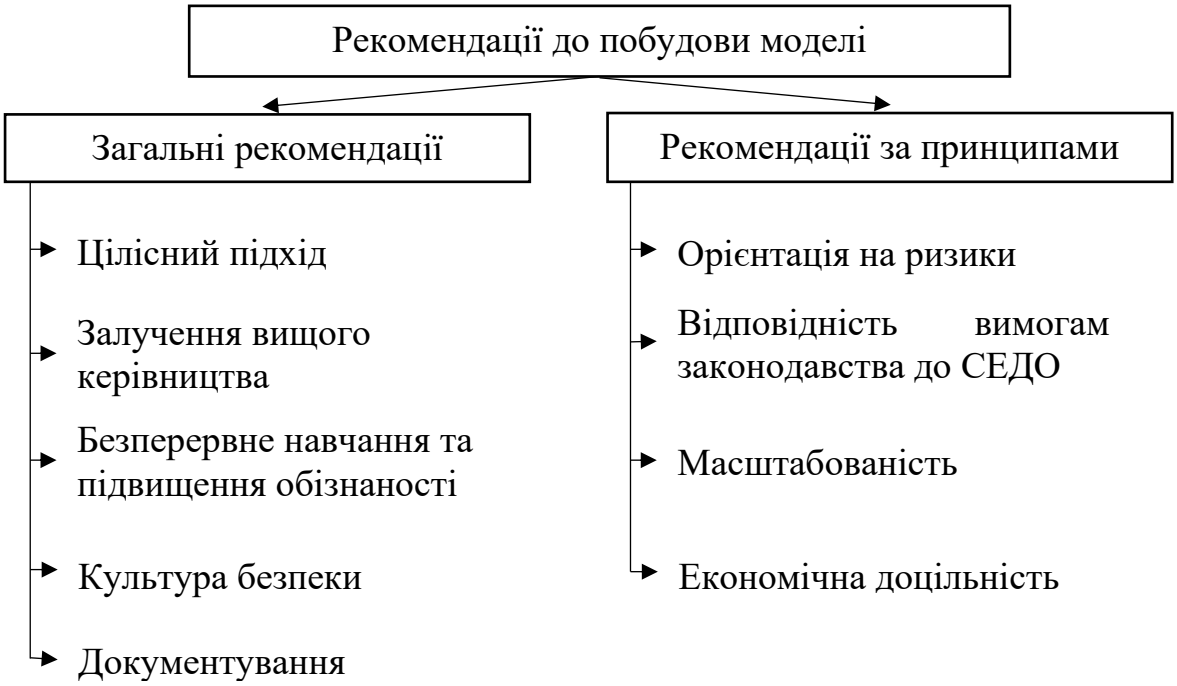


Рисунок 3.4 – Система рекомендацій, що лежать в основі побудови моделі вибору та аналізу комплексу засобів захисту СЕДО для критичної інфраструктури

Загальні рекомендації до побудови ефективної моделі вибору та аналізу комплексу засобів захисту СЕДО для КІ:

- Цілісний підхід. Розглядати безпеку СЕДО не як окрему функцію, а як інтегровану частину загальної стратегії кібербезпеки організації та її операційної діяльності. Захист документів має бути невіддільним від процесів їх створення, обробки, зберігання та архівування.
- Залучення вищого керівництва. Без активної підтримки та залучення вищого керівництва, будь-яка ініціатива з кібербезпеки, особливо в КІ,

приречена на провал. Керівництво повинно розуміти ризики, виділяти необхідні ресурси та встановлювати пріоритети.

- Безперервне навчання та підвищення обізнаності. Людський фактор є однією із найслабших ланок у безпеці. Регулярні тренінги та програми підвищення обізнаності для всього персоналу (від кінцевих користувачів до ІТ-спеціалістів) щодо загроз, політик та процедур безпеки є обов'язковими.
- Культура безпеки. Сприяти формуванню культури безпеки в організації, де кожен співробітник усвідомлює свою роль у захисті інформації та відповідальність за її безпеку.
- Документування. Ведення повної та актуальної документації на всіх етапах: політик, процедур, результатів аналізу ризиків, архітектури СЗІ, протоколів тестування, звітів про інциденти, що важливо для відповідності аудиту та безперервності.

Рекомендації за принципами моделі.

1. Орієнтація на ризики.

- Постійний моніторинг загроз. Регулярно оновлювати модель загроз та моделі порушників, враховуючи нові тактики, техніки та процедури, кіберзлочинців, геополітичні зміни та розвиток технологій.
- Реалістична оцінка впливу. При оцінці впливу при реалізації ризиків для КІ враховувати не лише фінансові, а й операційні збитки, потенційну шкоду для життя та здоров'я населення, екологічні наслідки, репутаційні втрати та вплив на національну безпеку.
- Пріоритизація ризиків. Фокусувати ресурси на захисті від найвищих та найбільш ймовірних ризиків, а не намагатися захистити все однаково. Визначати критичні активи та зосереджуватися на їхньому захисті першочергово.
- Врахування ланцюга постачання. Оцінювати ризики, пов'язані з третіми сторонами (постачальники ПЗ, хмарні провайдери, партнери), які мають доступ до СЕДО або чиї продукти використовуються в ній.

2. Відповідність вимогам законодавства до СЕДО.

- Юридичний аудит. Регулярно проводити аудити на відповідність СЕДО та її СЗІ чинному законодавству України та міжнародним зобов'язанням.
- «Security by Design». Забезпечувати відповідність вимогам безпеки вже на етапі проєктування СЕДО, а не намагатися «накласти» їх зверху пізніше. Це дешевше та ефективніше.
- Використання сертифікованих/атестованих засобів [30], приклади яких наведено у додатку В. Для захисту інформації в СЕДО КІ (особливо якщо вони обробляють інформацію з обмеженим доступом) використовувати лише засоби криптографічного та технічного захисту інформації, які мають позитивні експертні висновки або сертифікати відповідності Держспецзв'язку.
- Постійний моніторинг змін у законодавстві. Призначити відповідальну особу або відділ, який відстежує зміни в нормативно-правовій базі щодо кібербезпеки та захисту інформації, особливо для КІ, та забезпечує їх впровадження.

3. Масштабованість.

- Модульний підхід. При проєктуванні СЗІ використовувати модульний підхід, який дозволяє додавати або оновлювати окремі компоненти без необхідності повної перебудови системи.
- Гнучкість архітектури. Забезпечити гнучкість архітектури СЕДО та СЗІ для адаптації до змін у технологіях, бізнес-процесах та обсягах даних.
- Тестування навантаження. Регулярно проводити тестування навантаження та продуктивності СЗІ, щоб переконатися, що вона може ефективно функціонувати при збільшенні обсягів даних або кількості користувачів без зниження рівня безпеки.
- Планування зростання. Враховувати потенційне майбутнє зростання організації та розширення СЕДО на етапі вибору рішень, щоб уникнути дорогих переробок у майбутньому.

4. Економічна доцільність.

- Комплексна оцінка вартості володіння. Враховувати не лише початкові витрати на придбання та впровадження, а й витрати на ліцензування, підтримку, оновлення, навчання персоналу, аудит та можливі штрафи за недотримання вимог.
- Баланс між безпекою та функціональністю. Не допускати, щоб заходи безпеки створювали надмірні незручності для користувачів або суттєво сповільнювали бізнес-процеси, якщо це не виправдано рівнем ризику. Оптимізувати баланс.
- Використання відкритих стандартів та рішень. Де це можливо, розглядати використання відкритих стандартів та рішень, що може зменшити залежність від одного постачальника та потенційно знизити витрати.
- Запровадження метрик ефективності. Визначити чіткі метрики для вимірювання ефективності інвестицій у безпеку та оцінки рівня зниження ризиків. Це дозволить обґрунтовувати подальші інвестиції.
- Проведення регулярного перегляду. Періодично переглядати ефективність та економічну доцільність впроваджених заходів безпеки, адаптуючи їх за потреби.
- Дотримання цих рекомендацій дозволить організаціям КІ створити не просто захищену, а й ефективну, гнучку та стійку СЕДО, що є запорукою національної безпеки та стабільності.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі кваліфікаційної роботи було здійснено розробку концепції та деталізацію моделі вибору та аналізу КЗЗ для СЕДО в КІ. Центральним елементом даного розділу стало визначення фундаментальних принципів, які мають керувати процесом забезпечення кібербезпеки в умовах підвищених ризиків, характерних для КІ.

По-перше, обґрунтовано, що запропонована модель базується на чотирьох ключових принципах: орієнтація на ризики, відповідність вимогам

законодавства, масштабованість та економічна доцільність. Принцип орієнтації на ризики передбачає, що заходи безпеки обираються пропорційно до ідентифікованих загроз, вразливостей та потенційних наслідків, які можуть вплинути на функціонування КІ, з обов'язковим постійним моніторингом ризиків. Відповідність вимогам законодавства до СЕДО гарантує, що КЗЗ відповідає всім чинним національним та міжнародним нормативно-правовим актам та регуляторним вимогам. Принцип масштабованості забезпечує здатність архітектури СЗІ адаптуватися до зростаючих обсягів даних, збільшення кількості користувачів та інтеграції з новими технологіями без втрати ефективності. Економічна доцільність вимагає обґрунтованого співвідношення витрат на безпеку з потенційними збитками, яких можна уникнути, оптимізуючи інвестиції та враховуючи довгострокове планування.

По-друге, розроблено та деталізовано п'ятиетапний циклічний процес функціонування моделі вибору та аналізу КЗЗ СЕДО для КІ. До цих етапів відносяться:

1. Підготовка та планування. Початковий етап є фундаментальним для успішної імплементації, що включає чітке визначення області застосування СЕДО, формування експертної команди, визначення конкретних цілей безпеки та детальне вивчення всіх релевантних регуляторних вимог.

2. Аналіз ризиків та оцінка потреб – етап, на якому здійснюється глибока ідентифікація та оцінка цінності інформаційних активів, виявлення загроз та вразливостей (включаючи моделювання порушників), а також кількісний або якісний аналіз ризиків. Кінцевою метою є визначення допустимого рівня ризику та оцінка поточного стану захисту.

3. Вибір та проєктування засобів захисту. Він базується на результатах аналізу ризиків, відбувається обґрунтований вибір технічних та організаційних засобів безпеки. Даний етап охоплює проєктування архітектури СЗІ, розробку технічного завдання та комплексний аналіз економічної доцільності обраних рішень.

4. Впровадження та реалізація. Етап здійснення практичної реалізації запланованих заходів, що включає закупівлю, інсталяцію та конфігурацію обраних засобів захисту. Важливими елементами є розробка та впровадження внутрішніх політик і процедур безпеки, проведення навчання персоналу, а також тестування СЗІ та, за необхідності, її атестація відповідно до національних вимог.

5. Моніторинг, аудит та підтримка – етап, який є безперервним і має циклічний характер, забезпечуючи постійне підтримання високого рівня безпеки. Він включає моніторинг подій безпеки, оперативне реагування на кіберінциденти, регулярні аудити та перевірки ефективності СЗІ, актуалізацію моделей загроз та ризиків, а також безперервне оновлення та вдосконалення системи захисту.

По-третє, було сформовано комплекс рекомендацій, що лежать в основі побудови ефективної моделі вибору та аналізу КЗЗ СЕДО для КІ. Ці рекомендації охоплюють загальні аспекти (цілісний підхід, залучення вищого керівництва, безперервне навчання, формування культури безпеки, документування) та специфічні рекомендації, що корелюють з принципами моделі (постійний моніторинг загроз, реалістична оцінка впливу, пріоритизація ризиків, врахування ланцюга постачання, юридичний аудит, "Security by Design", використання сертифікованих засобів, модульний підхід, гнучкість архітектури, тестування навантаження, довгострокове планування, комплексна оцінка вартості володіння та баланс між безпекою і функціональністю).

Таким чином, розроблена у даному розділі модель вибору та аналізу комплексу засобів захисту СЕДО для критичної інфраструктури є послідовним, ітеративним та адаптивним процесом. Вона забезпечує системний підхід до захисту ДІР КІ, враховуючи небезпеку та динамічність кіберзагроз, та дозволяє підвищити рівень кіберстійкості та забезпечити безперебійне функціонування життєво важливих державних систем.

ВИСНОВКИ

Дана кваліфікаційна робота мала на меті розробити ефективну модель для відбору та аналізу комплексу засобів захисту інформаційних ресурсів критичної інфраструктури (КІ), що функціонують у середовищі систем електронного документообігу (СЕДО). Для досягнення цієї цілі було визначено та реалізовано низку послідовних завдань, що охоплювали глибоке вивчення концептуальних основ КІ та державних інформаційних ресурсів (ДІР), аналіз позиції СЕДО як об’єкта кіберзахисту, систематизацію чинної нормативно-правової бази та міжнародних стандартів, а також комплексний розгляд наявних механізмів безпеки. Дослідження зосередилося на ДІР КІ, що обробляються та зберігаються в СЕДО, тоді як основним об’єктом вивчення були методології, підходи та інструментарій для захисту СЕДО як інтегральної складової КІ. У процесі роботи були застосовані методи системного та порівняльного аналізу, що дозволило узагальнити та систематизувати значний обсяг даних, а також метод моделювання для побудови запропонованої архітектури.

У ході виконаної роботи було отримано низку ключових наукових результатів, які формують комплексне розуміння архітектури кібербезпеки СЕДО у критично важливих секторах.

По-перше, встановлено, що КІ є фундаментом стабільності держави, а її порушення спричинить деструктивні наслідки для національної безпеки, економічної сфери та суспільного порядку. Обґрунтовано, що ДІР у КІ є не просто пасивними відомостями, а стратегічними активами, захищеність яких безпосередньо залежить від забезпечення конфіденційності, цілісності та доступності. Ці висновки цілком корелюють із загальновизнаними принципами інформаційної безпеки. Крім того, показано, що СЕДО трансформувалися у критично значущі інформаційні системи в державному управлінні та КІ, виступаючи центральним інструментом для оперативного ухвалення рішень та гарантування безперервності функціонування.

По-друге, проведено деталізацію типів інформації, що обробляється у СЕДО КІ, згідно з українським законодавством. Здійснено поділ на відкриту інформацію та інформацію з обмеженим доступом, яка, своєю чергою, диференціюється на конфіденційну, службову та таємну. Особливо акцентовано, що обробка таємної інформації у СЕДО вимагає обов'язкового проходження державною системою експертизи та отримання відповідного позитивного висновку від Держспецзв'язку, що свідчить про найвищі вимоги до захисту такої категорії даних.

По-третє, систематизовано нормативно-правову базу та міжнародні стандарти, які регулюють сферу захисту інформації в КІ. Визначено, що національне законодавство України, зокрема закони «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України» та «Про електронну ідентифікацію та електронні довірчі послуги», є комплексною регуляторною рамкою. Обґрунтовано, що імплементація міжнародних стандартів, таких як ДСТУ ISO/IEC 27001 [321, 1179] та NIST Cybersecurity Framework, є необхідним кроком для підвищення кіберстійкості та відповідності передовим світовим практикам. Це повністю підтверджує висунуту гіпотезу щодо необхідності інтеграції як національних вимог, так і міжнародного досвіду для забезпечення ефективного захисту.

По-четверте, здійснено класифікацію та аналіз існуючих категорій засобів захисту, що мають безпосереднє відношення до СЕДО. Було виокремлено організаційні заходи (включаючи принципи Zero Trust, механізми управління інцидентами, програми підвищення обізнаності персоналу), програмні інструменти (системи контролю доступу на основі ролей та атрибутів, використання КЕП, DLP-рішення, SIEM-платформи, криптографічні механізми) та апаратні засоби (персональні токени, модулі TPM, WORM-сховища для довгострокового архівування, апаратні VPN-шлюзи). Показано доцільність інтеграції ключових характеристик сучасних архітектур безпеки (ZTA, ASA, CRA) для підвищення кіберзахисту СЕДО. Розглянуті принципи ешелонованої

оборони, реалізації найменших привілеїв та функціональної сегментації мережі повністю відповідають поточним викликам, що стосуються безпеки СЕДО в КІ.

По-п’яте, обґрунтовано, що традиційні методи аналізу ризиків лише частково відображають специфіку документоорієнтованих систем. У відповідь на цю прогалину, була запропонована нова модель CSAR-D (Contextual and Semantic Adaptive Risk for Documents). Її інноваційність полягає у трактуванні ризику не як сукупності факторів, а як відхилення цифрової події від очікуваної норми, що дозволяє здійснювати динамічну оцінку критичності дій, виходячи з етапу життєвого циклу документа, ролі користувача та відповідності його поведінки встановленим шаблонам. Ця модель забезпечує не тільки виявлення вразливостей, а й оперативну ідентифікацію системних аномалій, що відхиляються від безпечного маршруту обробки даних.

Нарешті, кульмінацією дослідження стала розробка п’ятиетапної циклічної моделі вибору та аналізу комплексу засобів захисту СЕДО для КІ. Ця модель включає етапи підготовки та планування, аналізу ризиків та оцінки потреб, вибору та проєктування засобів захисту, впровадження та реалізації, а також безперервного моніторингу, аудиту та підтримки. Модель ґрунтується на принципах орієнтації на ризики, відповідності законодавству, масштабованості та економічної доцільності. Таким чином, поставлена у роботі мета щодо розробки моделі для вибору та аналізу КЗЗ ДІР КІ була повністю досягнута.

Результати проведеного дослідження мають значну практичну цінність, оскільки запропонована модель надає системну методологію для підвищення кібербезпеки СЕДО, що функціонують у критичній інфраструктурі, що є невід’ємним для гарантування національної безпеки та стабільності. Рекомендації щодо її застосування можуть слугувати основою для розробки нових методичних вказівок для державних органів та суб’єктів КІ, сприяти підвищенню кваліфікації фахівців у галузі кібербезпеки та формуванню ефективних національних політик і стратегій захисту ДІР КІ.

Перспективи подальших досліджень у даній предметній області можуть бути спрямовані на:

- Розробку програмного прототипу або автоматизованого інструментарію, що здатен реалізувати запропоновану модель CSAR-D для динамічної оцінки ризиків у режимі реального часу;
- Поглиблене дослідження економічної ефективності впровадження конкретних комплексів засобів захисту, обґрунтованих розробленою моделлю, для різних секторів КІ;
- Розробку деталізованих методик інтеграції СЕДО в національну систему кібербезпеки України, враховуючи особливості взаємодії з CERT-UA та іншими державними регуляторними органами.

Підсумовуючи, дана робота підтверджує, що постійне впровадження та вдосконалення комплексних систем захисту СЕДО, які обробляють державні інформаційні ресурси критичної інфраструктури, є не лише актуальним завданням, а й життєво необхідним імперативом для забезпечення сталого функціонування держави в умовах постійно зростаючих кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.12.2024).

2. Закон України «Про критичну інфраструктуру». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 07.12.2024).

3. S. Toliupa, S. Buchyk, O. Kulinich, O. Buchyk. PROTECTION OF STATE MANAGEMENT OF CRITICAL INFRASTRUCTURE OBJECTS UNDER THE INFLUENCE OF CYBER ATTACKS. Інфокомунікаційні технології та електронна інженерія, Вип. 2, № 2, 2022. – С. 33–41. – (DOI: https://doi.org/10.23939/ictee2022.02.033).

4. Постанова Кабінету Міністрів України від 09 листопада 2020 р. № 1184 (зі змінами №447 від 28.03.2025) «Деякі питання об'єктів критичної інформаційної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 13.12.2024).

5. Б'юкенен Б. (2024). Хакери і держава (Ю. Каздобіна пер. з англ.). Київ: НашФормат.

6. Наказом Міністерства освіти і науки, молоді та спорту України від 20.10.2011 № 1207 «Про вимоги до форматів даних електронного документообігу в органах державної влади. Формат електронного повідомлення». URL: https://zakon.rada.gov.ua/laws/show/z1306-11#Text (дата звернення: 25.12.2024).

7. Закон України «Про доступ до публічної інформації». URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 31.12.2024).

8. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 06.01.2025).

9. Закон України «Про основи національного спротиву». URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text (дата звернення: 12.01.2025).

10. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 18.01.2025).

11. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 24.01.2025).

12. Закон України «Про електронні документи та електронний документообіг». URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 30.01.2025).

13. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 05.02.2025).

14. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» зі змінами № 2801-IX від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 11.02.2025).

15. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 17.02.2025)

16. ДСТУ EN ISO/IEC 27000:2022 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (EN ISO/IEC 27000:2020, IDT; ISO/IEC 27000:2018, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=103330 (дата звернення: 23.02.2025).

17. The NIST Cybersecurity Framework (CSF) 2.0 (2024), National Institute of Standards and Technology, pp.32, DOI: https://doi.org/10.6028/NIST.CSWP.29 (дата звернення: 29.02.2025).

18. ДСТУ EN ISO 22301:2021 Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO

22301:2019, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=96909 (дата звернення: 06.03.2025).

19. ДСТУ EN IEC 62443-3-3:2022 Промислові комунікаційні мережі. Безпека мережі та системи. Частина 3-3. Вимоги та рівні безпеки системи (EN IEC 62443-3-3:2019, IDT; IEC 62443-3-3:2013, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=107733 (дата звернення: 12.03.2025).

20. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 18.03.2025).

21. Закон України «Про державну таємницю» зі змінами № 40190-IX від 10.10.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 24.03.2025).

22. Закону України «Про захист персональних даних» зі змінами № 4240-IX від 12.02.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 30.03.2025).

23. Sabat, V., Durnyak, B., Dytko, T., & Onufrei, O. (2023). Risk assessment of an automated document management system in a hierarchical management system. Acta Avionica, 25(2), 5–14. DOI: 10.35116/aa.2023.0009. URL: https://acta-avionica.tuke.sk/ojs/index.php/aavionica/article/view/1144. (дата звернення: 05.04.2025).

24. Lu, Z., & Sagduyu, Y. E. (2018). Risk assessment based access control with text and behavior analysis for document management. IEEE Conference. URL: https://www.researchgate.net/publication/311919979_Risk_assessment_based_access_control_with_text_and_behavior_analysis_for_document_management (дата звернення: 11.04.2025).

25. Focardi, R., & Luccio, F. L. (2021). A formally verified configuration for hardware security modules in the cloud. Proceedings of the 2021 ACM International

Conference on Management of Data (SIGMOD '21). arXiv:2109.13631. URL: https://arxiv.org/abs/2109.13631 (дата звернення: 17.04.2025).

26. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. "Zero Trust Architecture." NIST Special Publication 800-207 (2020). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 23.04.2025).

27. Allodi, L., & Massacci, F. "Security events and vulnerability data for cybersecurity risk estimation." Risk Analysis, 37(8), 1606–1627 (2017). DOI: 10.1111/risa.12710. URL: https://www.researchgate.net/publication-/319070904_Security_Events_and_Vulnerability_Data_for_Cybersecurity_Risk_Estimation_Cybersecurity_Risk_Estimation (дата звернення: 29.04.2025).

28. Buchyk O., Toliupa S. Regulatory and legal support for the selection of a set of means to protect state information resources of critical infrastructure (Satellite): Conference Proceedings, November 21, 2024, Kyiv, Ukraine / Ministry of Education and Science of Ukraine, Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). – Kyiv: Publishing House «Caravela», 2024. pp. 110-111.

29. Стратегія кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 11.05.2025).

30. Перелік протестованих систем електронного документообігу URL: https://se.diia.gov.ua/sedlist (дата звернення: 17.05.2025).

ДОДАТОК А
ГЛОСАРІЙ ТЕРМІНІВ

1. Державні інформаційні ресурси – систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [1].

2. Доступність – властивість бути доступним і використовуваним на вимогу уповноваженого суб'єкта [16].

3. Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [12].

4. Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [12].

5. Електронний підпис – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис [11].

6. Електронна печатка – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються для забезпечення достовірності походження пов'язаних електронних даних, або для засвідчення електронних підписів підписувачів на електронних документах, або для засвідчення відповідності копій документів оригіналам та виявлення порушення цілісності [11].

7. Електронна позначка часу – електронні дані, що пов’язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу [11].

8. Захист інформації в системі – діяльність, спрямована на запобігання порушенню цілісності, конфіденційності і доступності інформації в системі [8].

9. Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле. [8].

10. Кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше кваліфікованих електронних довірчих послуг та відомості про яку внесені до Довірчого списку [11].

11. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [29].

12. Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [29].

13. Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки [29].

14. Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [29].

15. Кіберстійкість – набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури [10].

16. Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [8].

17. Конфіденційність – властивість інформації не надаватися та не розкриватися не уповноваженим особам, організаціям або процесам [16].

18. Критична інфраструктура – сукупність об'єктів критичної інфраструктури [29].

19. Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури [3].

20. Національний спротив – комплекс заходів, які організовуються та здійснюються з метою сприяння обороні України шляхом максимально широкого залучення громадян України до дій, спрямованих на забезпечення воєнної безпеки, суверенітету і територіальної цілісності держави, стримування і відсіч агресії та завдання противнику неприйнятних втрат, з огляду на які він буде змушений припинити збройну агресію проти України [9].

21. Об’єкти критичної інфраструктури – об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [29].

22. Система електронного документообігу – комплекс програмних засобів і технологій, призначених для автоматизації процесів обробки документів в електронному форматі [12].

23. Система управління інформаційною безпекою – сукупність взаємопов’язаних або взаємодіючих елементів організації для встановлення політики та цілей, а також процесів для досягнення цих цілей щодо інформаційної безпеки [16].

24. Територіальна оборона – система загальнодержавних, воєнних і спеціальних заходів, що здійснюються у мирний час та в особливий період з метою протидії воєнним загрозам, а також для надання допомоги у захисті населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій [9].

25. Цілісність – властивість точності та повноти [16].

ДОДАТОК Б

ПОРІВНЯЛЬНА ТАБЛИЦЯ АРХІТЕКТУР БЕЗПЕКИ

Архітектура	Основна ідея	Призначення для СЕДО	Основні переваги	Обмеження / недоліки
Zero Trust Architecture (ZTA)	Не довіряти за замовчуванням; постійна перевірка всіх дій	Захист користувача, документу, підпису, запиту з урахуванням контексту	Високий рівень безпеки, контекстна перевірка, сумісність із ABAC, DLP, UEBA	Складність впровадження, висока вартість інтеграції
Secure Access Service Edge (SASE)	Інтеграція мережевого доступу та захисту у хмарі	Безпечний доступ до СЕДО з віддалених офісів через хмару	Централізоване керування доступом, мобільність	Залежність від хмарного провайдера, обмежена відповідність українському законодавству
Cyber Resilience Architecture (CRA)	Стійкість до інцидентів і швидке відновлення	Збереження функціональності СЕДО в умовах інцидентів або атак	Автоматичне перемикання вузлів, мінімізація простоїв	Потребує надлишкової інфраструктури, сценарного планування
Intent-Based Security Architecture (IBSA)	Безпека на основі аналізу намірів, а не лише доступу	Аналізує логічність дій користувача щодо документів у контексті заявленої мети	Виявлення аномальних або нелогічних дій, глибокий інтелектуальний аналіз	Висока складність реалізації в держсекторі, обмежене впровадження
Adaptive Security Architecture (ASA)	Динамічна зміна поведінки системи відповідно до середовища	Автоматичне реагування на аномальну поведінку у роботі з документами СЕДО	Реагування в реальному часі, інтеграція з UEBA, MFA, DLP	Необхідність складних правил адаптації та поведінкового аналізу

ДОДАТОК В

ПЕРЕЛІК ПРОТЕСТОВАНИХ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

№	Розробник	Назва та версія платформи	Інтеграційна взаємодія з СЕВ ОВВ	НПА
1.	ТОВ «Софтлайн-ІТ»	Мегаполіс v.2.57	+	-
2.	ТОВ «Софтлайн-ІТ»	«Megapolis. DocNet» v.1.x	+	-
3.	ТОВ «Інтекресі Бейз»	«Megapolis. DocNet» v.1.x	+	+
4.	ТОВ «Айкюжн ІТ»	«Megapolis. DocNet» v.1.x	+	-
5.	АТ «ІнфоПлюс»	АСКОД II v 10.3.8.141	+	-
6.	АТ «ІнфоПлюс»	АСКОД Корпоративний v.10	+	+
7.	ТОВ «Транс Лінк Консалтинг»	ДОК ПРОФ™ СТЕП 2.0	+	-
8.	ТОВ «Транс Лінк Консалтинг»	«Автоматизована система управління документами «ДОК ПРОФ 3»	+	+
9.	ТОВ «Інтерактивні системи»	InterDoc v 4.2	+	-
10.	ТОВ НВП «Інформаційні технології»	«IT-Enterprise»(IT Підприємство)	+	+
11.	ТОВ «Алтерсайн»	Документаріум	+	-
12.	ТОВ «Софт Експаншен Україна»	«SX-Government» v 3	+	-
13.	ТОВ «ФОСС-ОН-ЛАЙН»	FossDoc Enterprize v 6.42	+	+
14.	ТОВ «Новатум»	«ДОК ПРОФ ВЕБ»	+	-
15.	ТОВ "СМАРТ БІЗНЕС"	"Система електронного документообігу Міністерства освіти і науки України Версія 4.0"	+	-

Продовження таблиці

16.	Укрпатент	АС "Загальне діловодство"	+	-
17.	ТОВ "Е-ДОКС"	e-Docs.Platform	+	-
18.	ТОВ «Адвертайзінг Експрес»	Комп'ютерна програма «CleverForms Document» 2.4	+	-
19.	ТОВ "ІРБЕКС СОЛЮШНС"	«БД ДОКУМЕНТООБІГ"V.1.2.x»	+	-
20.	ТОВ "ІРІС"	Стратег.Смарт ("Стратег.Смарт)" версія 4.0	+	-
21.	ТОВ "МАСТЕР:ГЛОБАЛ"	Система електронного документообігу "MASTER:Документообіг" версія 2019	+	-
22.	ДП «ІНФОТЕХ»	СЕД системи МВС, версія 2019.x.x	+	-
23.	ТОВ "НЕВДА"	СЕД Deka office	+	-
24.	ТОВ "АйКор Технолоджі"	СЕД "Айдок"	+	-
25.	ДП Адміністрація морських портів України	СЕД "АМПУ" версія 1.0	+	-
26.	ДП «ІНФОТЕХ»	СЕД "МІА:Документообіг" версія 1.0	+	+
27.	ТОВ "МЕДИРЕНТ"	АСЕДО версія 2	+	-
28.	ТОВ «СОФТ ПРОДАКШН»	Ком'пютерна програма «Альфа.Про»	+	+
29.	ТОВ «МІАЦ»	СЕД «Електронне самоврядування 3.0»	+	-
30.	ПАТ "ВФ Україна"	СЕД «Lotus Notes Domino»	+	-
31.	ПП «КАІ»	«КАІ-Документообіг»	+	-
32.	ТОВ науково - виробнича фірма «ГРІС»	«Інтранет - портал електронного документообігу Верховної Ради України» версія 1.0	+	-
33.	ТОВ «М.Е.Д.О.К»	СЕД «M.E.Doc»,11.XX.XXX	+	-

Продовження таблиці

34.	ТОВ "Інформаційно-аналітичний центр"	Комп'ютерна програма "TDocs" версії 3.x	+	-
35.	Приватне акціонерне товариство «ВФ Україна»	Система електронного документообігу «OpenText» Приватного акціонерного товариства «ВФ Україна»	+	-
36.	Товариство з обмеженою відповідальністю «ІНТЕЛЕКТ-СЕРВІС»	Система електронного документообігу «Комп’ютерна програма «Комплексна система автоматизації підприємства «IS-pro» («ІС-ПРО») версія 8.XX.XXX»	+	-
37.	ТОВ "ІТ ПРО"	СЕД Deka office	+	-
38.	**ТОВ "Острін ЛТД"**	**Хмарний сервіс «ШРИФТ»**	**+**	**-**
39.	Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України	Комп'ютерна програма "Веб-додаток "Система судових експертів ПЛАТФОРМА"	+	-

ДОДАТОК Г

СЕРТИФІКАТ АДМІНІСТРАТОРА СЕДО «SCHRIFT»

SCHRIFT

СЕРТИФІКАТ

засвідчує, що

Бучик Олександр Сергійович

Пройшов навчання щодо використання системи електронного документообігу «Schrift» та отримав знання щодо:

- Адміністрування СЕДО;
- Виконання робіт щодо створення компанії в СЕДО, формування внутрішньої структури компанії, організації документообігу компанії;
- Управління організаційною структурою, переліком ролей, журналами реєстрації документів, типами та шаблонами документів та іншими довідковими даними системи.

На підставі отриманих знань та вмінь може виконувати функції адміністратора системи електронного документообігу «Schrift».

Директор «Острін ЛТД»
Г.Луцай

Директор «Авалекс Сольюшн»
О.Кохановський

Подпись с квалифицированным сертификатом действительна
Подписан: КОХАНОВСЬКИЙ ОЛЕКСІЙ ІГОРОВИЧ
Организация: ФІЗИЧНА ОСОБА
Дата, время: 12.06.2024 15:14 (UTC+03:00)
SCHRIFT

Подпись с квалифицированным сертификатом действительна
Подписан: ЛУЦАЙ ГРИГОРІЙ КІМОВИЧ
Организация: ТОВ ОСТРІН ЛТД, 32496838
Должность: ДИРЕКТОР
Дата, время: 12.06.2024 15:
SCHRIFT

ДОДАТОК Д
СЕРТИФІКАТ АДМІНІСТРАТОРА СЕДО «SCHRIFT»

ДОДАТОК ДО СЕРТИФІКАТУ
(без сертифікату недійсний)

Бучик Олександр Сергійович

успішно пройшов навчання на курсі «Адміністратор СЕДО» щодо адміністрування та використання системи електронного документообігу "Schrift". Отримав компетенції та знання з наступних аспектів:

Адміністрування СЕДО:

1. Навички адміністрування системи електронного документообігу "Schrift".
2. Уміння налаштовувати та керувати параметрами системи відповідно до потреб організації.
3. Навички створення та використання типів, шаблонів документів для ефективного використання електронного документообігу при створенні та обробці різноманітних документів.

Виконання робіт щодо створення компанії в СЕДО:

1. Знання про процедури та кроки, необхідні для успішного створення компанії в системі "Schrift".
2. Вміння формувати внутрішню структуру компанії, включаючи підрозділи, підрозділи підрозділів та інші організаційні одиниці.
3. Навички організації ефективного документообігу в компанії з використанням системи "Schrift".

Управління організаційною структурою, ролями та документами:

1. Знання про процеси управління організаційною структурою в системі "Schrift".
2. Вміння налаштовувати та управляти переліком ролей, прав доступу та привілеїв для користувачів системи.
3. Здатність використовувати журнали реєстрації документів для контролю та відстеження процесу обігу документів.