

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені Вадима Гетьмана**

**Навчально-науковий інститут “Інститут інформаційних технологій
в економіці”**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

Галузь знань 12 «Інформаційні технології»

Спеціальність 124 «Системний аналіз»

Форма навчання: очна(денна)
очна (денна), заочна, дистанційна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему «Системний аналіз управління захистом інформації в
комп'ютерних мережах»
(назва теми)

здобувача Долженкова Сергія Сергійовича _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник доктор економічних наук, професор, Галіцин В.К.
(науковий ступінь, учене звання, ПІБ)

(niɔnuɔ)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: доктор фізико–математичних наук,
професор Джалладова Ірада Агаверді-кизи

(*nidnuc*)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені Вадима Гетьмана

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»
СПЕЦІАЛЬНІСТЬ 124 «СИСТЕМНИЙ АНАЛІЗ»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми
д.економ.н., проф. Галіцин
Володимир Костянтинович

(підпис)

_____ 2024 р.

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерної
д.фіз.-мат.н., проф. Джалладова
Ірада Агаверді-кизи

(підпис)

_____ 2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Долженкову Сергію Сергійовичу
прізвище, ім'я, по батькові)

 очної (денної) форми навчання
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

на тему «Системний аналіз управління захистом інформації в комп'ютерних мережах»

Тему затверджено наказом ректора Університету від «__» _____ 2024 р. № _____

Кваліфікаційна бакалаврська робота виконується на матеріалах

ТОВ «Перша Депозитарна Установа»

План кваліфікаційної бакалаврської роботи	
Розділ 1	Теоретичний аспект управління захистом інформації в комп'ютерних мережах (назва розділу)
Розділ 2	Аналіз стану захисту інформації в комп'ютерній мережі об'єкту дослідження (назва розділу)
Розділ 3	Розробка заходів щодо підвищення ефективності управління захистом інформації (назва розділу)
Об'єкт дослідження:	ТОВ "Перша Депозитарна Установа"
Предмет дослідження:	захист інформації та управління захистом інформації в комп'ютерних мережах підприємства
Мета кваліфікаційної бакалаврської роботи:	визначення можливостей використання системного аналізу для покращення ефективності управління захистом інформації в комп'ютерних мережах

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	Теоретичний аспект управління захистом інформації в комп'ютерних мережах - Теоретичні засади галузі захисту інформації; - Огляд існуючих методологій системного аналізу захисту інформації; - Використання системного аналізу для вивчення критеріїв ефективності систем захисту інформації.
У розділі 2	Аналіз стану захисту інформації в комп'ютерній мережі об'єкту дослідження - Характеристика комп'ютерної мережі об'єкта дослідження. - Аналіз вразливостей та загроз для інформаційної безпеки в комп'ютерній мережі. - Оцінка ефективності існуючої системи захисту інформації.
У розділі 3	Розробка заходів щодо підвищення ефективності управління захистом інформації - Оптимізація процесів управління захистом інформації. - Розробка рекомендацій щодо вдосконалення захисту інформації на основі системного аналізу.

Завдання підготував науковий керівник

(підпис)

(ініціали, прізвище)

« ____ » _____ 2024 р.

Завдання одержав здобувач

(підпис)

(ініціали, прізвище)

« ____ » _____ 2024 р.

Реферат

Кваліфікаційна бакалаврська робота містить 3 розділи, 57 сторінок, 12 таблиць, 3 рисунка, список використаних джерел з 30 найменувань.

«Системний аналіз управління захистом інформації в комп'ютерних мережах»

Об'єктом дослідження є ТОВ "Перша Депозитарна Установа".

Предметом дослідження є захист інформації та управління захистом інформації в комп'ютерних мережах підприємства.

Мета кваліфікаційної бакалаврської роботи – визначення можливостей використання системного аналізу для покращення ефективності управління захистом інформації в комп'ютерних мережах.

Відповідно до поставленої мети були визначені такі завдання:

- Аналіз поточного стану захисту інформації в комп'ютерних мережах підприємства.
- Виявлення проблем та недоліків у існуючій системі захисту.
- Розробка пропозицій щодо вдосконалення та впровадження системного підходу до управління захистом інформації.

Практичне значення отриманих результатів. Висновки та рекомендації, запропоновані у цій бакалаврській роботі, мають значну практичну важливість для підприємств, що прагнуть впровадити системний аналіз в процеси управління захистом інформації в комп'ютерних мережах. Дослідження підкреслює, що використання розроблених методик може значно оптимізувати управління інформаційною безпекою, зменшити час на аналіз та реагування на безпекові інциденти, а також зберегти ресурси підприємства. Рекомендації з впровадження системного підходу до захисту інформації допоможуть покращити робочі процеси та забезпечити більш високий рівень захищеності інформаційних ресурсів. Застосування запропонованих методів дозволить організаціям не лише ефективно виявляти та нейтралізувати потенційні загрози, а й підвищити загальну обізнаність та компетентність у сфері інформаційної безпеки. Це, в свою чергу, сприятиме створенню більш стійкої інформаційної інфраструктури та забезпеченню відповідності до національних та міжнародних стандартів безпеки.

Рік виконання кваліфікаційної бакалаврської роботи 2024. Рік захисту роботи 2024.

Ключові слова: системний аналіз, управління захистом інформації, комп'ютерні мережі, інформаційна безпека, вразливості мережі, кібербезпека, ризики інформаційної безпеки, захист даних, методології захисту інформації, оптимізація процесів, ефективність системи, рекомендації, підприємство, організація.

В і д г у к
про кваліфікаційну бакалаврську роботу
здобувача освітньо-професійної програми «Системний аналіз»
навчально-наукового інституту
«Інститут інформаційних технологій в економіці»
Долженкова Сергія Сергійовича

На тему: «Системний аналіз управління захистом інформації в комп'ютерних мережах».

1. Актуальність теми: Кваліфікаційна бакалаврська робота є самостійним дослідженням, яке присвячено застосуванню засобів і методів системного аналізу в управлінні захистом інформації в комп'ютерних мережах. В умовах швидкого розвитку інформаційних технологій та зростаючої кількості кібератак тема роботи є вкрай актуальною.
2. Позитивні риси кваліфікаційної бакалаврської роботи: Відповідність методів дослідження, оригінальність та обґрунтованість висновків і рекомендацій, якість оформлення й логічність викладу матеріалу.
3. Наявність самостійних розробок автора: Проведена оцінка ефективності існуючої в досліджуваній установі системи захисту інформації.
4. Цінність теоретичних висновків та практичних рекомендацій: Полягає в проведенні комплексного дослідження, яке дозволяє рекомендувати його результати як основу для оптимізації процесів управління захистом інформації в досліджуваній установі.
5. Наявність недоліків: Кваліфікаційна бакалаврська робота містить певну кількість недоліків, які не впливають на загальну якість виконаної роботи.
6. Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК: Тема роботи розкрита, основні положення та висновки достатньо обґрунтовані. Робота Долженкова Сергія Сергійовича на тему «Системний аналіз управління захистом інформації в комп'ютерних мережах» може бути допущена до захисту перед ЕК і заслуговує високої позитивної оцінки.

Науковий керівник професор кафедри системного аналізу та кібербезпеки д.е.н. професор
(посада, учене звання, науковий ступінь)

Галіцин В.К.

(підпис)

(прізвище, ініціали)

“ ____ ” _____ 20 24 р.

Рецензія

на кваліфікаційну бакалаврську роботу здобувача вищої освіти
Долженкова Сергія Сергійовича

Тема

Системний аналіз управління захистом інформації в комп'ютерних мережах

Актуальність теми кваліфікаційної роботи і доцільність її розроблення

Тема має велику актуальність у сучасних умовах, де захист інформації стає важливою складовою успішної діяльності будь-якого підприємства. Автором було обгрунтовано актуальність теми та її значення для підприємств різного масштабу, що свідчить про доцільність розроблення даної бакалаврської роботи.

Позитивні риси кваліфікаційної бакалаврської роботи

Автор виконав роботу на високому науково-методичному рівні, детально дослідивши теоретичні аспекти системного аналізу в управлінні захистом інформації. Робота містить зріз сучасних методів та інструментів системного аналізу, які можуть бути застосовані у практиці підприємств. Велика увага приділена аналізу поточного стану захисту інформації, виявленню його недоліків та загроз, а також запропоновано шляхи їх вирішення.

Автор використав різноманітні джерела, включаючи наукову літературу та реальні приклади з практики захисту інформації. Це сприяє поглибленню розуміння проблематики та впровадженню практичних аспектів у дослідження. Також слід відзначити логічну структуру роботи, чітке формулювання мети та завдань, що дозволяє читачеві зрозуміти основний зміст дослідження.

Зауваження

Хоча бакалаврська робота має багато позитивних рис, є аспект, який все ж потребує удосконалення. Рекомендується більш детально розглянути практичну значимість висновків та рекомендацій, зазначивши, як саме впровадження рекомендацій може покращити захист інформації та підвищити загальний рівень безпеки підприємства.

Практична значимість висновків і рекомендацій

Висновки та рекомендації, що пропонуються в бакалаврській роботі, мають практичну значимість для підприємств, які бажають впровадити системний аналіз в управлінні захистом інформації. Автор зазначає, що застосування запропонованих методик дозволить ефективно організувати роботу із захисту інформації, зменшити ризики та підвищити рівень безпеки підприємства. Рекомендації з вдосконалення системи захисту інформації можуть сприяти покращенню робочих процесів та забезпеченню високої якості управління інформаційною безпекою.

Загалом, дана бакалаврська робота заслуговує визнання за своєю актуальністю, науково-методичним рівнем та практичною значимістю. Зауваження, які були висловлені, можуть бути враховані для подальшого вдосконалення роботи та її практичної реалізації.

Місце роботи та посада рецензента

Науковий ступінь, учене звання

Директор ТОВ "Перша Депозитарна
Установа" Рубанук Р.В.

Підпис засвідчую

Підпис рецензента
(посада, підпис)
Місце печатки організації, де працює рецензент

(місце, підпис)

ЗМІСТ

ВСТУП.....	3
 РОЗДІЛ 1 ТОРЕТИЧНИЙ АСПЕКТ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ.....	 6
1.1. Теоретичні засади галузі захисту інформації.	6
1.2. Огляд існуючих методологій системного аналізу захисту інформації.	10
1.3. Використання системного аналізу для вивчення критеріїв ефективності систем захисту інформації.....	17
 РОЗДІЛ 2 АНАЛІЗ СТАНУ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ОБ'ЄКТУ ДОСЛІДЖЕННЯ.....	 22
2.1. Характеристика комп'ютерної мережі об'єкта дослідження.	22
2.2. Аналіз вразливостей та загроз для інформаційної безпеки в комп'ютерній мережі.	31
2.3. Оцінка ефективності існуючої системи захисту інформації.	37
 РОЗДІЛ 3 РОЗРОБКА ЗАХОДІВ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ.....	 43
3.1. Оптимізація процесів управління захистом інформації.....	43
3.2. Розробка рекомендацій щодо вдосконалення захисту інформації на основі системного аналізу.	45
 ВИСНОВКИ	 52
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	54

ВСТУП

У сучасних умовах швидкої технологічної трансформації та зростаючих загроз в інформаційній сфері, ефективне управління захистом інформації є ключовим фактором успіху підприємства. Із зростанням обсягу даних, що передаються та обробляються в комп'ютерних мережах, постає потреба в надійному захисті інформаційних ресурсів. У зв'язку з цим, тема «Системний аналіз управління захистом інформації в комп'ютерних мережах» є дуже актуальною та важливою для вивчення.

Актуальність теми. У сучасному світі інформаційні ресурси стають одним із найцінніших активів організацій. Втрата або компрометація цих ресурсів може призвести до значних фінансових збитків, шкоди для репутації, а також до правових наслідків. У зв'язку з цим, дослідження системного аналізу управління захистом інформації в комп'ютерних мережах є вкрай актуальним, особливо в умовах швидкого розвитку інформаційних технологій та зростаючої кількості кібератак.

Аналіз останніх досліджень і публікацій. Важливий внесок у розвиток теорії та практики управління інформаційною безпекою зробили такі вчені, як Янчук Т. В., Хамленко І. І., а також міжнародні організації, такі як Інститут програмної інженерії (SEI) та Національний інститут стандартів і технологій (NIST). Їх роботи зосереджені на вивченні методів і моделей системного аналізу, а також на розробці технологій для забезпечення інформаційної безпеки. Проте, існує низка не вирішених питань, пов'язаних з інтеграцією цих методів у комплексні системи захисту інформації на підприємствах .

Мета і завдання дослідження. Метою дослідження є визначення можливостей використання системного аналізу для покращення ефективності управління захистом інформації в комп'ютерних мережах. Завданнями дослідження є:

- Аналіз поточного стану захисту інформації в комп'ютерних мережах підприємства.
- Виявлення проблем та недоліків у існуючій системі захисту.
- Розробка пропозицій щодо вдосконалення та впровадження системного підходу до управління захистом інформації.

Об'єкт дослідження. Об'єктом дослідження є ТОВ "Перша Депозитарна Установа".

Предмет дослідження. Предметом дослідження є захист інформації та управління захистом інформації в комп'ютерних мережах підприємства.

Методи дослідження. Для досягнення мети та розв'язання завдань дослідження були використані методи системного аналізу, такі як SWOT-аналіз, аналіз причин та наслідків (дерево проблем), розробка дерева рішень та інші. Крім того, був проведений аналіз існуючих методологій захисту інформації та оцінка їхньої ефективності для подальшого вдосконалення процесів управління захистом інформації .

Теоретична, методична та практична значущість отриманих результатів. Теоретична значущість роботи полягає в узагальненні знань з питань системного аналізу та захисту інформації, що дозволяє розширити наукову базу для подальших досліджень у цій галузі. Методична значущість полягає у розробці рекомендацій та методів, які можуть бути застосовані для вдосконалення процесів управління захистом інформації в різних організаціях. Практична значущість дослідження полягає в тому, що запропоновані заходи можуть бути безпосередньо впроваджені в ТОВ "Перша Депозитарна Установа" для покращення ефективності захисту інформаційних ресурсів .

Інформаційна база дослідження. Дослідження базувалося на аналізі наукових праць, статистичних даних офіційних сайтів, звітів рейтингових агентств, фінансових звітів, а також на внутрішніх документах ТОВ "Перша Депозитарна Установа" .

Результати дослідження можуть бути використані для покращення процесу управління захистом інформації, що в свою чергу дозволить зменшити ризики, пов'язані з інформаційними загрозами, підвищити рівень безпеки та забезпечити надійність функціонування підприємства в цілому.

РОЗДІЛ 1

ТЕОРЕТИЧНИЙ АСПЕКТ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1. Теоретичні засади галузі захисту інформації.

Захист інформації є критично важливою складовою сучасного інформаційного суспільства, де обсяги передавання та зберігання даних у комп'ютерних мережах постійно зростають. В умовах цифрової трансформації та глобалізації, інформаційні ресурси стають одним із найцінніших активів організацій. Втрата або компрометація цих ресурсів може призвести до значних фінансових збитків, шкоди для репутації, а також до правових наслідків.

Галузь захисту інформації зосереджена на розробці та впровадженні різноманітних технологій, політик, стандартів і процесів, які забезпечують захист даних від несанкціонованого доступу, використання, розкриття, модифікації або знищення. Основною метою захисту інформації є збереження її цінності та забезпечення безпеки в умовах постійних загроз.

Значення захисту інформації полягає у забезпеченні стабільності та безперебійної роботи організацій, збереженні довіри клієнтів і партнерів, а також у дотриманні правових і нормативних вимог. Надійний захист інформаційних ресурсів є фундаментом для успішного функціонування будь-якої організації, незалежно від її розміру чи сфери діяльності [1].

У сучасному світі захист інформації виходить за межі технічного аспекту і стає стратегічною проблемою, яка потребує комплексного підходу. Важливою складовою цього підходу є управління ризиками, яке включає ідентифікацію, оцінку та контроль ризиків, пов'язаних із інформаційними ресурсами. Ефективне управління ризиками дозволяє зменшити ймовірність інцидентів і мінімізувати їхній вплив на організацію. Важливість захисту інформації також зумовлена необхідністю відповідати сучасним правовим та нормативним вимогам. Багато

країн мають закони та регламенти, які регулюють питання захисту даних, і невиконання цих вимог може призвести до серйозних правових наслідків [2].

Захист інформації є не лише технічним завданням, але й важливою складовою стратегії управління організацією, яка забезпечує її стійкість, безпеку та довгостроковий успіх.

Для розуміння теоретичних засад галузі захисту інформації важливо ознайомитися з основними поняттями та термінами, що використовуються в цій сфері. Найважливіші з них включають інформаційну безпеку, конфіденційність, цілісність і доступність [3].

Інформаційна безпека – це сукупність заходів, спрямованих на захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, руйнування, модифікації чи пошкодження. Інформаційна безпека має на меті забезпечити збереження цінності інформації та її безпечне використання в межах організації.

Однією з ключових складових інформаційної безпеки є конфіденційність. Конфіденційність гарантує, що інформація доступна лише авторизованим користувачам або системам. Це означає, що дані не можуть бути доступні або розкриті несанкціонованим особам. Забезпечення конфіденційності досягається за допомогою таких методів, як шифрування даних, контроль доступу та політики безпеки. Наприклад, застосування шифрування дозволяє захистити інформацію під час її передачі через мережу, роблячи її недоступною для сторонніх осіб [4].

Цілісність є ще однією важливою складовою інформаційної безпеки. Цілісність означає, що інформація залишається незмінною та достовірною протягом всього життєвого циклу, і будь-які несанкціоновані зміни або пошкодження можуть бути виявлені. Цілісність забезпечується за допомогою засобів контролю цілісності, таких як цифрові підписи, хешування та контроль версій. Ці заходи дозволяють перевірити, чи не було внесено несанкціонованих змін у дані, і зберегти їх достовірність.

Доступність означає, що авторизовані користувачі мають можливість своєчасного доступу до необхідної інформації та ресурсів. Це особливо важливо

для забезпечення безперебійної роботи бізнес-процесів та оперативного прийняття рішень. Доступність досягається за допомогою резервного копіювання, відновлення після збоїв, розподілу навантаження та захисту від атак типу "відмова в обслуговуванні" (DoS). Наприклад, використання систем резервного копіювання дозволяє швидко відновити дані у разі їх втрати або пошкодження [5].

Ці три основні поняття – конфіденційність, цілісність і доступність – утворюють так звану CIA-тріаду, яка є основою для побудови систем інформаційної безпеки. Вони забезпечують комплексний підхід до захисту інформації, який дозволяє врахувати різноманітні аспекти загроз і ризиків, з якими стикаються сучасні організації.

Забезпечення інформаційної безпеки вимагає комплексного підходу, що включає використання передових технологій, розробку та впровадження політик безпеки, навчання співробітників, а також постійний моніторинг та оцінку ризиків. Впровадження таких заходів дозволяє організаціям зменшити вразливості, підвищити рівень захисту інформації та забезпечити стабільну та безпечну роботу своїх інформаційних систем.

Правові та нормативні основи захисту інформації є важливим аспектом забезпечення інформаційної безпеки. Вони встановлюють загальні принципи, вимоги та стандарти, які повинні дотримуватися організації для захисту своїх інформаційних ресурсів. Дотримання правових і нормативних вимог не лише допомагає захистити інформацію, але й зменшує ризик юридичних санкцій та втрат репутації [6].

В Україні захист інформації регулюється низкою законів і підзаконних актів. Одним з основних є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який встановлює загальні вимоги до захисту інформації в інформаційних системах, порядок організації захисту, а також права та обов'язки суб'єктів захисту інформації. Цей закон визначає основні принципи захисту інформації, такі як конфіденційність, цілісність і доступність, та встановлює вимоги до організаційних і технічних заходів, необхідних для забезпечення інформаційної безпеки. Крім національних законів, важливу роль у

регулюванні захисту інформації відіграють міжнародні стандарти. Одним з найпоширеніших є міжнародний стандарт ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою (СУІБ). ISO/IEC 27001 надає організаціям структурований підхід до впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. Впровадження цього стандарту дозволяє організаціям підвищити рівень захисту інформації та забезпечити відповідність міжнародним вимогам [7].

Європейський регламент Загальний регламент про захист даних (GDPR) є ще одним важливим нормативним актом, який регулює питання захисту персональних даних у країнах Європейського Союзу. GDPR встановлює високі стандарти захисту даних і зобов'язує організації, що обробляють персональні дані громадян ЄС, дотримуватися цих вимог незалежно від їх місцезнаходження. Регламент передбачає серйозні штрафи за порушення вимог, що стимулює організації приділяти велику увагу захисту персональних даних [8].

У США питання захисту інформації регулюються кількома законами та стандартами, серед яких варто відзначити Закон про захист інформації (FISMA), який встановлює вимоги до забезпечення інформаційної безпеки у федеральних агентствах, та стандарти NIST (Національний інститут стандартів і технологій). Стандарти NIST надають детальні рекомендації щодо управління ризиками та впровадження заходів захисту інформації, що робить їх важливим інструментом для забезпечення інформаційної безпеки.

Також варто відзначити стандарт COBIT (Control Objectives for Information and Related Technologies), який надає рамки для управління інформаційними технологіями та забезпечення інформаційної безпеки. COBIT допомагає організаціям оцінювати, управляти та оптимізувати свої ІТ-процеси для досягнення бізнес-цілей та забезпечення відповідності нормативним вимогам.

Дотримання правових і нормативних вимог є ключовим елементом у забезпеченні інформаційної безпеки. Організації повинні постійно стежити за змінами в законодавстві та стандартах, впроваджувати необхідні заходи для відповідності вимогам, а також проводити регулярні аудити та оцінки ризиків. Це

дозволяє не лише забезпечити надійний захист інформаційних ресурсів, але й зменшити ризик юридичних та фінансових санкцій.

1.2. Огляд існуючих методологій системного аналізу захисту інформації.

Системний аналіз захисту інформації є важливим елементом у забезпеченні інформаційної безпеки організацій. Він включає використання різних методів і моделей, що дозволяють ідентифікувати, оцінювати та управляти ризиками, пов'язаними з інформаційними системами та ресурсами. Основні методи і моделі системного аналізу, які застосовуються для управління захистом інформації, включають OCTAVE, COBIT та NIST [9].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – це методологія оцінки ризиків, розроблена Інститутом програмної інженерії (SEI) при Університеті Карнегі-Меллона. OCTAVE фокусується на ідентифікації критичних активів організації, оцінці загроз і вразливостей, а також розробці стратегій управління ризиками. Методологія складається з трьох фаз [10]:

1. Планування і підготовка – визначення цілей оцінки, формування команди оцінки, збір початкової інформації.
2. Ідентифікація і оцінка загроз – аналіз активів, загроз і вразливостей, визначення їх впливу на організацію.
3. Розробка стратегії управління ризиками – формулювання рекомендацій щодо управління ризиками, впровадження заходів захисту.

COBIT (Control Objectives for Information and Related Technologies) – це рамкова методологія, розроблена Інститутом управління інформаційними системами (ISACA). COBIT забезпечує структурований підхід до управління

інформаційними технологіями та забезпечення інформаційної безпеки. Методологія включає чотири основні домени:

1. Планування та організація – визначення стратегій і політик безпеки, планування заходів з управління ризиками.
2. Придбання та впровадження – розробка та впровадження інформаційних систем і технологій.
3. Забезпечення та підтримка – моніторинг та управління інформаційними системами, забезпечення їх безперервної роботи.
4. Моніторинг та оцінка – оцінка ефективності заходів безпеки, проведення аудитів і перевірок.

NIST (National Institute of Standards and Technology) – це набір стандартів і керівництв, розроблених Національним інститутом стандартів і технологій США. NIST надає детальні рекомендації щодо управління ризиками та забезпечення інформаційної безпеки. Основні стандарти NIST включають:

1. NIST SP 800-30 – керівництво з управління ризиками, яке описує процеси і методи ідентифікації, аналізу та оцінки ризиків.
2. NIST SP 800-53 – каталог контролів безпеки та конфіденційності для федеральних інформаційних систем і організацій.
3. NIST Cybersecurity Framework – рамкова модель для управління ризиками кібербезпеки, що включає ідентифікацію, захист, виявлення, реагування та відновлення.

Кожна з цих методологій має свої унікальні особливості та підходи, але всі вони спрямовані на забезпечення комплексного підходу до управління захистом інформації. Використання цих методів дозволяє організаціям ефективно ідентифікувати загрози і вразливості, оцінювати ризики і розробляти стратегії для їх мінімізації.

Методології OCTAVE, COBIT та NIST забезпечують структуру та інструменти, необхідні для ефективного управління захистом інформації. Вибір конкретної методології залежить від потреб та специфіки організації, але

впровадження будь-якої з них допомагає підвищити рівень інформаційної безпеки, забезпечуючи захист критичних активів та ресурсів.

Для ефективного управління захистом інформації в організації важливо вибрати відповідну методологію, яка буде відповідати потребам і специфіці діяльності. У цьому підрозділі розглядаються три популярні методології: OCTAVE, COBIT та NIST, а також їхні основні характеристики та відмінності. Нижче подано порівняльний аналіз цих методологій [11].

Табл. 1.1 – Порівняльний аналіз методологій OCTAVE, COBIT та NIST

Характеристика	OCTAVE	COBIT	NIST
Основний фокус	Управління ризиками	Управління інформаційними технологіями	Управління ризиками та кібербезпекою
Розробник	Інститут програмної інженерії (SEI)	Інститут управління інформаційними системами (ISACA)	Національний інститут стандартів і технологій (NIST)
Основні компоненти	Ідентифікація активів, загроз, вразливостей; розробка стратегії управління ризиками	Планування, організація, придбання, впровадження, забезпечення, підтримка, моніторинг, оцінка	Ідентифікація, захист, виявлення, реагування, відновлення
Підхід	Оцінка ризиків на основі активів	Управління IT-процесами	Управління ризиками на основі контролів
Цільова аудиторія	Організації будь-якого розміру та галузі	Великі організації з розвиненою IT-інфраструктурою	Організації будь-якого розміру та галузі
Основні документи	OCTAVE Method Implementation Guide	COBIT 5	NIST SP 800-30, NIST SP 800-53, NIST Cybersecurity Framework

Продовження табл. 1.1

Гнучкість	Висока	Середня	Висока
Придатність для малих і середніх підприємств (МСП)	Висока	Низька	Висока
Орієнтація на відповідність нормативам	Середня	Висока	Висока
Придатність для державного сектору	Висока	Середня	Висока

Джерело: розроблено автором на основі [11].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) є методологією, яка зосереджена на управлінні ризиками шляхом ідентифікації критичних активів, загроз та вразливостей. OCTAVE підходить для організацій будь-якого розміру та галузі, надаючи гнучкий підхід до оцінки ризиків. Вона добре підходить для малих і середніх підприємств, завдяки своїй простоті впровадження та високій гнучкості. Основним документом методології є "OCTAVE Method Implementation Guide".

COBIT (Control Objectives for Information and Related Technologies) є методологією, орієнтованою на управління інформаційними технологіями. Вона охоплює всі аспекти ІТ-процесів, включаючи планування, організацію, придбання, впровадження, забезпечення, підтримку, моніторинг та оцінку. COBIT підходить переважно для великих організацій з розвиненою ІТ-інфраструктурою, де важливо забезпечити ефективне управління ІТ-ресурсами та процесами. Основний документ методології – COBIT 5. Хоча COBIT має високу орієнтацію на відповідність нормативам, його впровадження може бути складним і менш гнучким для малих і середніх підприємств.

NIST (National Institute of Standards and Technology) пропонує стандарти та керівництва, зосереджені на управлінні ризиками та кібербезпекою. Основні документи, такі як NIST SP 800-30, NIST SP 800-53 та NIST Cybersecurity

Framework, надають детальні рекомендації щодо впровадження контролів безпеки та управління ризиками. NIST підходить для організацій будь-якого розміру та галузі, надаючи високу гнучкість та придатність як для малих, так і для великих підприємств. Вона особливо корисна для державного сектору завдяки своїй орієнтації на відповідність нормативним вимогам.

Кожна з методологій – OCTAVE, COBIT та NIST – має свої унікальні особливості та переваги, які можуть бути корисними для різних організацій залежно від їхніх потреб і специфіки діяльності. OCTAVE надає гнучкий підхід до управління ризиками, підходить для малих і середніх підприємств. COBIT забезпечує комплексне управління ІТ-процесами, орієнтоване на великі організації. NIST пропонує детальні стандарти та керівництва для управління ризиками та кібербезпекою, що підходить для організацій будь-якого розміру та особливо корисно для державного сектору. Вибір конкретної методології залежить від специфіки організації, її ресурсів та цілей у сфері інформаційної безпеки.

Для ефективного управління захистом інформації та оцінки ризиків організації використовують різноманітні інструменти і техніки системного аналізу. Ці інструменти дозволяють ідентифікувати, оцінювати та управляти загрозами і вразливостями інформаційних систем. Розглянемо основні інструменти і техніки, зокрема SWOT-аналіз та дерево проблем, які є важливими складовими системного аналізу.

Табл. 1.2 – Основні інструменти і техніки системного аналізу

Інструмент/Техніка	Опис	Приклад використання
SWOT-аналіз	Методика оцінки сильних (Strengths), слабких (Weaknesses) сторін, можливостей (Opportunities) та загроз (Threats).	Оцінка стану інформаційної безпеки в організації.
Дерево проблем	Візуалізація проблем у вигляді діаграми з метою аналізу причинно-наслідкових зв'язків.	Виявлення основних причин вразливостей та загроз для інформаційних систем.

Аудит безпеки	Систематичний огляд і оцінка заходів безпеки та політик в організації.	Оцінка відповідності вимогам безпеки та стандартам.
Сканування вразливостей	Використання програмного забезпечення для автоматичного виявлення вразливостей.	Використання інструментів типу Nessus, OpenVAS для сканування мережі.
Тестування на проникнення (Penetration Testing)	Імітація атак на інформаційні системи з метою виявлення вразливостей.	Використання Metasploit для перевірки надійності захисту системи.
Моніторинг безпеки	Безперервний нагляд за мережевою активністю для виявлення аномалій і загроз.	Використання систем SIEM (Security Information and Event Management).
Аналіз журналів подій	Огляд та аналіз лог-файлів для виявлення підозрілої активності.	Використання Splunk для аналізу журналів подій у реальному часі.
Управління патчами	Впровадження оновлень програмного забезпечення для усунення вразливостей.	Використання Microsoft SCCM для управління патчами.

Джерело: розроблено автором на основі [12].

SWOT-аналіз є ефективним інструментом для оцінки поточного стану інформаційної безпеки в організації. Він допомагає виявити внутрішні сильні та слабкі сторони, а також зовнішні можливості та загрози. SWOT-аналіз дозволяє організаціям розробити стратегії для підвищення ефективності захисту інформації. Сильні сторони можуть включати високий рівень мережевої безпеки, впроваджені політики безпеки, наявність систем резервного копіювання. Слабкі сторони можуть бути пов'язані з недостатнім автоматичним оновленням програмного забезпечення, обмеженим фінансуванням на нові технології, нестачею кваліфікованих кадрів. Можливості включають впровадження нових технологій, підвищення кваліфікації співробітників, співпрацю з зовнішніми фахівцями. Загрози можуть бути представлені зростанням кількості кібератак, соціальною інженерією,

вразливостями в програмному забезпеченні, внутрішніми загрозами від інсайдерів [12].

Дерево проблем є ще одним важливим інструментом системного аналізу, що дозволяє візуалізувати та аналізувати причинно-наслідкові зв'язки між різними аспектами безпеки. Дерево проблем допомагає виявити основні причини вразливостей та загроз, а також їхні наслідки. Основна проблема може бути, наприклад, високий ризик витоку конфіденційної інформації. Ця проблема може мати кілька причин, таких як незахищені мережеві пристрої, недостатня захищеність програмного забезпечення, людський фактор та інші. Виявивши основні причини проблеми, організація може розробити ефективні заходи для їх усунення та мінімізації ризиків.

Аудит безпеки є систематичним оглядом і оцінкою заходів безпеки та політик в організації. Він допомагає визначити, наскільки ефективно організація дотримується встановлених вимог безпеки та стандартів. Аудит безпеки дозволяє виявити слабкі місця в системі безпеки і розробити рекомендації щодо їх усунення.

Сканування вразливостей включає використання спеціалізованого програмного забезпечення для автоматичного виявлення вразливостей у мережевих пристроях та програмному забезпеченні. Це дозволяє швидко ідентифікувати слабкі місця і вжити заходів для їх усунення. Тестування на проникнення (Penetration Testing) передбачає імітацію атак на інформаційні системи з метою виявлення вразливостей і перевірки ефективності існуючих заходів безпеки.

Моніторинг безпеки є безперервним наглядом за мережевою активністю для виявлення аномалій і загроз. Він дозволяє своєчасно виявляти підозрілу активність і реагувати на потенційні загрози. Аналіз журналів подій включає огляд та аналіз лог-файлів для виявлення підозрілої активності та відстеження інцидентів безпеки. Використання таких систем, як SIEM (Security Information and Event Management), дозволяє централізовано управляти безпекою та швидко реагувати на інциденти.

Управління патчами включає впровадження оновлень програмного забезпечення для усунення вразливостей. Це важливий процес для підтримки

безпеки системи, оскільки нові вразливості можуть бути виявлені в програмному забезпеченні, і своєчасне оновлення допомагає знизити ризики їх експлуатації злоумисниками.

Загалом, використання інструментів і технік системного аналізу дозволяє організаціям ефективно управляти ризиками і забезпечувати високий рівень інформаційної безпеки. SWOT-аналіз і дерево проблем є важливими інструментами для ідентифікації та аналізу загроз і вразливостей, що дозволяє розробити стратегії для їх усунення та мінімізації впливу на організацію.

1.3. Використання системного аналізу для вивчення критеріїв ефективності систем захисту інформації.

Визначення критеріїв ефективності захисту інформації є важливим етапом в оцінці та вдосконаленні систем інформаційної безпеки. Ці критерії дозволяють виміряти успішність впроваджених заходів захисту і виявити області, що потребують покращення. Для досягнення цієї мети, необхідно чітко визначити, які саме показники будуть використовуватися для оцінки ефективності.

Ефективність систем захисту інформації зазвичай оцінюється за такими основними критеріями: конфіденційність, цілісність, доступність, надійність, відповідність нормативам, масштабованість та стійкість до загроз. Кожен з цих критеріїв має свої особливості та вимірюється за допомогою відповідних показників [13].

Конфіденційність визначається здатністю системи захищати інформацію від несанкціонованого доступу. Це можна оцінити за допомогою показників, які вимірюють кількість успішних і невдалих спроб доступу до конфіденційної інформації, а також наявність і ефективність механізмів контролю доступу.

Цілісність оцінюється на основі здатності системи зберігати інформацію в її оригінальному вигляді, без несанкціонованих змін або пошкоджень. Критерії оцінки включають кількість виявлених і виправлених помилок, а також наявність і ефективність механізмів перевірки цілісності даних.

Доступність визначається можливістю своєчасного доступу до інформаційних ресурсів для авторизованих користувачів. Критеріями оцінки можуть бути час простою системи, середній час відновлення після збоїв, а також рівень задоволеності користувачів.

Надійність включає здатність системи безперебійно працювати в умовах різних загроз і забезпечувати захист інформації протягом тривалого часу. Критерії оцінки включають показники часу безперебійної роботи (uptime), частоту і тривалість збоїв.

Відповідність нормативам вимірюється здатністю системи дотримуватись встановлених стандартів та регуляторних вимог. Це може включати кількість виявлених порушень нормативів під час аудитів, а також рівень відповідності внутрішнім і зовнішнім політикам безпеки.

Масштабованість визначається здатністю системи адаптуватися до збільшення навантаження та розширення обсягів оброблюваної інформації. Критеріями оцінки можуть бути гнучкість і адаптивність системи при збільшенні кількості користувачів або обсягу даних.

Стійкість до загроз включає здатність системи протистояти новим та існуючим загрозам, забезпечуючи безпеку інформації. Це може включати кількість виявлених і нейтралізованих загроз, а також ефективність впроваджених заходів безпеки.

Для ефективного визначення критеріїв ефективності захисту інформації важливо враховувати специфіку діяльності організації, її структуру та рівень ризиків. Критерії повинні бути адаптовані до конкретних умов і вимог організації, що дозволить точно оцінити стан захисту і визначити напрямки для вдосконалення.

Загалом, чітко визначені критерії ефективності захисту інформації дозволяють організаціям об'єктивно оцінювати стан своїх систем безпеки, виявляти

слабкі місця і розробляти стратегії для їх усунення. Це забезпечує комплексний підхід до управління інформаційною безпекою і сприяє постійному вдосконаленню систем захисту інформації.

Оцінка ефективності систем захисту інформації є невід'ємною частиною управління інформаційною безпекою в організації. Вона дозволяє визначити, наскільки ефективно впроваджені заходи захищають інформаційні ресурси від загроз і вразливостей. Для цього використовуються як кількісні, так і якісні показники [14].

Таблиця 1.3 – Методи оцінки ефективності систем захисту [14]

Методи оцінки	Показники	Опис
Кількісні показники	Кількість виявлених вразливостей	Кількість виявлених вразливостей за певний період.
	Кількість успішних/невдалих атак	Кількість успішних та невдалих спроб атак на інформаційну систему.
	Час реакції на інциденти	Середній час, необхідний для реагування на інциденти безпеки.
	Відсоток систем, що пройшли аудит	Частка систем, які успішно пройшли аудит безпеки.
	Рівень відповідності нормативам	Відсоток відповідності встановленим нормативним вимогам і стандартам безпеки.
	Кількість проведених тренінгів	Кількість навчальних заходів для співробітників з питань інформаційної безпеки.
	Кількість відновлених даних	Обсяг даних, успішно відновлених після інцидентів або втрат.
	Рівень використання антивірусу	Частка пристроїв, захищених антивірусним програмним забезпеченням.
	Рівень оновлення систем	Відсоток систем з актуальними оновленнями та патчами.

Продовження табл. 1.3

Якісні показники	Оцінка рівня обізнаності	Рівень обізнаності співробітників щодо політик та процедур безпеки.
	Оцінка якості політик	Якість впроваджених політик і процедур безпеки, відповідність найкращим практикам.
	Задоволеність користувачів	Рівень задоволеності користувачів інформаційними системами та заходами безпеки.
	Оцінка ризиків	Якість та точність проведеної оцінки ризиків і впроваджених заходів для їх мінімізації.

Кількісні показники включають об'єктивні метрики, які можна виміряти та проаналізувати. Одним з основних кількісних показників є кількість виявлених вразливостей у системі. Цей показник дозволяє оцінити ефективність впроваджених засобів виявлення вразливостей та визначити слабкі місця, які потребують покращення. Іншим важливим показником є кількість успішних та невдалих спроб атак на інформаційну систему. Це допомагає оцінити рівень захищеності системи та ефективність заходів безпеки.

Час реакції на інциденти безпеки є ще одним важливим кількісним показником. Швидка реакція на інциденти дозволяє знизити потенційний збиток і запобігти поширенню загроз. Відсоток систем, що пройшли аудит безпеки, дозволяє оцінити рівень відповідності організації встановленим стандартам та вимогам безпеки. Рівень відповідності нормативам також є важливим показником, який демонструє, наскільки добре організація дотримується правових і регуляторних вимог.

Кількість проведених тренінгів для співробітників з питань інформаційної безпеки свідчить про рівень обізнаності та підготовленості персоналу до роботи з інформаційними системами. Кількість відновлених даних після інцидентів або втрат показує ефективність систем резервного копіювання та відновлення. Рівень використання антивірусного програмного забезпечення і рівень оновлення систем

є показниками, які демонструють, наскільки добре організація підтримує актуальність своїх засобів захисту.

Якісні показники базуються на суб'єктивній оцінці та експертних висновках. Оцінка рівня обізнаності співробітників щодо політик та процедур безпеки дозволяє визначити, наскільки добре персонал розуміє і виконує вимоги безпеки. Оцінка якості політик і процедур безпеки включає їх відповідність найкращим практикам та стандартам галузі.

Задоволеність користувачів інформаційними системами та заходами безпеки свідчить про те, наскільки зручними і ефективними є впроваджені заходи. Оцінка ризиків включає аналіз якості та точності проведеної оцінки ризиків, а також впроваджених заходів для їх мінімізації [15].

Використання кількісних та якісних показників дозволяє організаціям здійснювати комплексний підхід до оцінки ефективності систем захисту інформації. Поєднання об'єктивних метрик та суб'єктивних оцінок забезпечує більш повну картину стану безпеки і дозволяє своєчасно виявляти проблеми та розробляти стратегії для їх усунення.

РОЗДІЛ 2

АНАЛІЗ СТАНУ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ОБ'ЄКТУ ДОСЛІДЖЕННЯ

2.1. Характеристика комп'ютерної мережі об'єкта дослідження.

Об'єктом дослідження є Товариство з обмеженою відповідальністю "Перша Депозитарна Установа" (ТОВ "Перша депозитарна установа"). Це підприємство надає депозитарні послуги, що включають зберігання цінних паперів, облік прав власності на цінні папери та здійснення інших операцій, пов'язаних із депозитарною діяльністю. Керівником організації є Рубанчук Роман Володимирович. Ідентифікаційний код ЄДРПОУ: 40164260.

ТОВ "Перша депозитарна установа" має складну організаційну структуру, яка включає різні відділи та підрозділи, кожен з яких відповідає за певний аспект діяльності [16]. Основні структурні підрозділи організації включають:

1. Керівництво

- Генеральний директор: Рубанчук Роман Володимирович
- Заступники директора
- Адміністративний відділ

2. Фінансовий відділ

- Бухгалтерія
- Відділ фінансового контролю та звітності

3. Відділ інформаційних технологій (ІТ)

- Адміністратори систем
- Інженери з мережевої інфраструктури

- Спеціалісти з кібербезпеки
- Програмісти та розробники ПЗ

4. Відділ депозитарних операцій

- Операційний відділ
- Відділ обліку та звітності

5. Юридичний відділ

- Юристи
- Спеціалісти з регуляторних питань

6. Відділ кадрів

- Відділ управління персоналом
- Відділ навчання та розвитку

Підприємство використовує сучасну комп'ютерну мережу для забезпечення безперервної та надійної роботи всіх своїх підрозділів. Архітектура комп'ютерної мережі розроблена для забезпечення високої надійності, безпеки та ефективності обробки даних. Мережа складається з кількох рівнів і компонентів, що взаємодіють між собою для забезпечення стабільної роботи всіх бізнес-процесів.

Архітектура мережі включає такі основні елементи:

- Центральний серверний вузол
- Клієнтські комп'ютери та робочі станції
- Мережеве обладнання (маршрутизатори, комутатори, точки доступу Wi-Fi)
- Системи зберігання даних
- Системи захисту інформації (брандмауери, антивірусне ПЗ, системи виявлення вторгнень)
- Зовнішнє підключення до Інтернету через захищений шлюз.

Табл. 2.1 - Основні компоненти мережі

Компонент	Опис	Кількість	Примітки
Центральні сервери	Високопродуктивні сервери для додатків та баз даних.	5	Віртуалізація, резервне копіювання
Віртуалізація серверів	Підвищення ефективності використання ресурсів за допомогою віртуалізаційного програмного забезпечення.	-	Використання VMware, Hyper-V
Резервне копіювання	Засоби резервного копіювання та відновлення даних для забезпечення безпеки інформації.	-	Щоденні інкрементні, щотижневі повні копії
Робочі станції	ПК та ноутбуки для співробітників організації, включаючи термінаційні пристрої для віддаленого доступу.	100	Висока продуктивність, безпека доступу
Маршрутизатори	Пристрої для управління трафіком між сегментами мережі та Інтернетом.	4	Захищені канали
Комутатори	Устаткування для внутрішньої комунікації між пристроями, підтримка VLAN.	10	Підтримка VLAN, QoS
Точки доступу Wi-Fi	Бездротові точки доступу для підключення мобільних пристроїв.	20	Підтримка WPA3
NAS	Мережеві сховища даних для забезпечення надійного зберігання великих обсягів інформації.	3	Реплікація даних
SAN	Системи зберігання на основі мереж SAN для	2	Підтримка високої доступності

Продовження табл. 2.1

	масштабованого і надійного зберігання даних.		
Брандмауери	Засоби захисту мережі від зовнішніх атак.	3	Підтримка VPN, IDS/IPS
Антивірусне ПЗ	Програмне забезпечення для захисту від шкідливих програм.	-	Постійне оновлення, централізоване управління
IDS/IPS	Системи виявлення та запобігання вторгненням для моніторингу та захисту мережевої інфраструктури.	2	Моніторинг в реальному часі

Джерело: розроблено автором на основі [17].

Таблиця основних компонентів мережі описує ключові елементи мережевої інфраструктури, які забезпечують її ефективну роботу. До складу центрального серверного вузла входять високопродуктивні сервери, що обслуговують критично важливі додатки та бази даних. Використання віртуалізації (наприклад, VMware або Hyper-V) дозволяє підвищити ефективність використання серверних ресурсів, що забезпечує гнучкість і масштабованість мережевої інфраструктури.

Робочі станції включають ПК та ноутбуки, які використовуються співробітниками для виконання повсякденних завдань. Ці пристрої підключені до мережі через комутатори, які забезпечують внутрішню комунікацію та підтримують сегментацію трафіку за допомогою VLAN (Virtual Local Area Network).

Для управління трафіком між сегментами мережі та Інтернетом використовуються маршрутизатори, які забезпечують захищені канали зв'язку. Точки доступу Wi-Fi дозволяють забезпечити бездротове підключення мобільних пристроїв, підтримуючи сучасні стандарти безпеки, такі як WPA3.

Мережеві сховища даних NAS та системи зберігання на основі SAN використовуються для надійного зберігання великих обсягів інформації. Вони забезпечують високу швидкість передачі даних та підтримку реплікації для забезпечення безпеки даних.

Засоби захисту інформації включають брандмауери, антивірусне програмне забезпечення та системи виявлення і запобігання вторгненням (IDS/IPS). Брандмауери захищають мережу від зовнішніх атак, а IDS/IPS системи забезпечують моніторинг мережевої активності в реальному часі, що дозволяє своєчасно виявляти та нейтралізувати загрози.

Табл. 2.2 – Рівні архітектури мережі

Рівень	Опис
Фізичний рівень	Фізичне з'єднання пристроїв за допомогою кабелів, оптоволокна, бездротових технологій.
Канальний рівень	Забезпечує надійну передачу даних між двома безпосередньо з'єднаними вузлами.
Мережевий рівень	Відповідає за маршрутизацію пакетів даних через різні мережі.
Транспортний рівень	Забезпечує надійність передачі даних, контроль помилок та управління потоком.
Сеансовий рівень	Відповідає за встановлення, підтримку і завершення сеансів зв'язку.
Рівень представлення	Забезпечує перетворення даних у формат, що може бути оброблений прикладними програмами.
Прикладний рівень	Містить протоколи, що використовуються програмами для зв'язку через мережу.

Джерело: розроблено автором на основі [18].

Для забезпечення стабільної та надійної роботи комп'ютерної мережі ТОВ "Перша депозитарна установа" використовуються сучасні технології та мережеві протоколи.

Табл. 2.3 - Основні технології

Технологія	Опис
Віртуалізація	Використання віртуалізаційного програмного забезпечення, такого як VMware або Hyper-V, для підвищення ефективності використання серверних ресурсів.
Резервне копіювання	Засоби резервного копіювання даних для забезпечення їх збереження та відновлення у разі збою. Застосовуються як щоденні інкрементні, так і щотижневі повні копії.

Wi-Fi	Бездротові точки доступу з підтримкою сучасних стандартів (наприклад, 802.11ac, WPA3) для забезпечення безпечного бездротового підключення.
SAN (Storage Area Network)	Мережа зберігання даних, що забезпечує високу швидкість передачі даних і надійне зберігання інформації.
NAS (Network Attached Storage)	Мережеві сховища даних для зберігання великих обсягів інформації та забезпечення легкого доступу до них.
IDS/IPS (Intrusion Detection/Prevention Systems)	Системи для виявлення та запобігання вторгненням, що забезпечують моніторинг мережевої активності в реальному часі.
VPN (Virtual Private Network)	Віртуальні приватні мережі для забезпечення захищеного віддаленого доступу до корпоративної мережі.
VLAN (Virtual Local Area Network)	Віртуальні локальні мережі для сегментації мережевого трафіку, підвищення безпеки та ефективності управління.

Джерело: розроблено автором на основі [19].

Використання віртуалізації (VMware, Hyper-V) дозволяє підвищити ефективність використання серверних ресурсів за рахунок одночасного запуску декількох віртуальних машин на одному фізичному сервері. Резервне копіювання даних здійснюється за допомогою інкрементних та повних копій, що забезпечує збереження інформації та можливість її відновлення у разі втрати або пошкодження.

Технологія Wi-Fi (802.11ac, WPA3) дозволяє забезпечити безпечний бездротовий доступ до мережі, що особливо важливо для мобільних пристроїв. Мережі зберігання даних, такі як SAN (Storage Area Network) та NAS (Network Attached Storage), забезпечують надійне та масштабоване зберігання великих обсягів даних з високою швидкістю передачі. Системи виявлення та запобігання вторгненням (IDS/IPS) забезпечують моніторинг мережевої активності в реальному часі, що дозволяє своєчасно виявляти та нейтралізувати загрози.

Віртуальні приватні мережі (VPN) забезпечують захищений віддалений доступ до корпоративної мережі, що є критично важливим для безпеки даних при роботі співробітників з віддалених місць. Використання віртуальних локальних

мереж (VLAN) дозволяє сегментувати мережевий трафік, підвищуючи безпеку та ефективність управління.

Табл. 2.4 - Основні протоколи

Протокол	Опис
TCP/IP	Основний набір протоколів для передачі даних в Інтернеті та внутрішніх мережах. Забезпечує адресацію і маршрутизацію пакетів даних.
HTTP/HTTPS	Протоколи для передачі гіпертексту (веб-сторінок). HTTPS забезпечує шифрування даних для захисту інформації під час передачі.
SMTP/IMAP/POP3	Протоколи для передачі та отримання електронної пошти. SMTP використовується для відправки, IMAP та POP3 – для отримання пошти.
FTP/SFTP	Протоколи для передачі файлів між клієнтом і сервером. SFTP забезпечує захищену передачу даних.
SNMP (Simple Network Management Protocol)	Протокол для управління мережевими пристроями та моніторингу їх роботи.
NTP (Network Time Protocol)	Протокол для синхронізації годин на комп'ютерах у мережі.
RDP (Remote Desktop Protocol)	Протокол для віддаленого доступу до робочих станцій та серверів.
LDAP (Lightweight Directory Access Protocol)	Протокол для доступу до і управління інформацією в розподіленій довідковій службі.
DNS (Domain Name System)	Система для перетворення доменних імен на IP-адреси.
DHCP (Dynamic Host Configuration Protocol)	Протокол для автоматичного присвоєння IP-адрес пристроям у мережі.
802.1X	Протокол контролю доступу до мережі, що забезпечує аутентифікацію пристроїв перед їх підключенням.

Джерело: розроблено автором на основі [20].

Протоколи TCP/IP є основним набором для передачі даних в Інтернеті та внутрішніх мережах, забезпечуючи адресацію та маршрутизацію пакетів даних. Протоколи HTTP/HTTPS забезпечують передачу гіпертексту (веб-сторінок) з шифруванням для захисту інформації під час передачі.

Протоколи SMTP, IMAP та POP3 використовуються для передачі та отримання електронної пошти. FTP та SFTP забезпечують передачу файлів між клієнтом і сервером, причому SFTP забезпечує захищену передачу даних. Протокол SNMP використовується для управління мережевими пристроями та моніторингу їх роботи, що важливо для ефективного управління мережею [20].

Протокол NTP забезпечує синхронізацію годин на комп'ютерах у мережі, що є критично важливим для коректної роботи додатків і систем. RDP забезпечує віддалений доступ до робочих станцій та серверів, що дозволяє співробітникам ефективно працювати з віддалених місць. Протоколи LDAP забезпечують доступ до інформації в розподіленій довідковій службі, DNS перетворює доменні імена на IP-адреси, а DHCP автоматично присвоює IP-адреси пристроям у мережі. Протокол 802.1X забезпечує аутентифікацію пристроїв перед їх підключенням до мережі, що підвищує безпеку мережі.

Табл. 2.5 - Таблиця технологій та протоколів

Категорія	Технологія/Протокол	Опис
Віртуалізація	VMware/Hyper-V	Підвищення ефективності використання серверних ресурсів за допомогою віртуалізації.
Резервне копіювання	Інкрементні/Повні копії	Регулярне резервне копіювання даних для забезпечення їх збереження та відновлення.
Безпроводний доступ	Wi-Fi (802.11ac, WPA3)	Забезпечення безпечного бездротового підключення для мобільних пристроїв.
Мережі зберігання даних	SAN, NAS	Надійне та масштабоване зберігання даних з високою швидкістю передачі.
Системи захисту	IDS/IPS	Моніторинг та захист мережевої інфраструктури в реальному часі.
Віддалений доступ	VPN	Захищений віддалений доступ до корпоративної мережі через віртуальні приватні мережі.

Продовження табл. 2.5

Сегментація мережі	VLAN	Сегментація мережевого трафіку для підвищення безпеки та ефективності управління.
Протоколи передачі даних	TCP/IP, HTTP/HTTPS	Адресація, маршрутизація та безпечна передача даних у мережі та через Інтернет.
Протоколи електронної пошти	SMTP, IMAP, POP3	Передача та отримання електронної пошти між серверами і клієнтами.
Протоколи передачі файлів	FTP, SFTP	Передача файлів між клієнтом і сервером, забезпечення захищеної передачі даних через SFTP.
Протоколи управління мережею	SNMP	Управління та моніторинг мережевих пристроїв.
Протоколи синхронізації часу	NTP	Синхронізація годин на комп'ютерах у мережі.
Протоколи віддаленого доступу	RDP	Віддалений доступ до робочих станцій та серверів.
Протоколи доступу до довідкових служб	LDAP	Доступ до і управління інформацією в розподіленій довідковій службі.
Протоколи іменування	DNS	Перетворення доменних імен на IP-адреси для зручності навігації в мережі.
Протоколи конфігурації	DHCP	Автоматичне присвоєння IP-адрес пристроям у мережі.
Протоколи контролю доступу	802.1X	Аутентифікація пристроїв перед їх підключенням до мережі для забезпечення безпеки.

Джерело: розроблено автором на основі [20].

В цій таблиці містяться основні технології та протоколів, які використовуються в мережі ТОВ "Перша депозитарна установа". Ця таблиця надає цілісне уявлення про різноманітні засоби та методи, що забезпечують безпеку та ефективність мережевої інфраструктури. Використання віртуалізації (VMware/Hyper-V) дозволяє ефективно використовувати серверні ресурси.

Регулярне резервне копіювання (інкрементні/повні копії) забезпечує збереження даних.

Бездротовий доступ (Wi-Fi 802.11ac, WPA3) забезпечує безпечне підключення мобільних пристроїв. Мережі зберігання даних (SAN, NAS) гарантують надійне зберігання та швидку передачу даних. Системи захисту (IDS/IPS) та віддалений доступ (VPN) підвищують безпеку мережі. Сегментація мережі (VLAN) сприяє ефективному управлінню та підвищенню безпеки. Протоколи передачі даних (TCP/IP, HTTP/HTTPS), електронної пошти (SMTP, IMAP, POP3), передачі файлів (FTP, SFTP), управління мережею (SNMP), синхронізації часу (NTP), віддаленого доступу (RDP), доступу до довідкових служб (LDAP), іменування (DNS), конфігурації (DHCP) та контролю доступу (802.1X) забезпечують різноманітні аспекти функціонування та безпеки мережі.

2.2. Аналіз вразливостей та загроз для інформаційної безпеки в комп'ютерній мережі.

Ідентифікація потенційних загроз і вразливостей є критично важливим етапом у процесі забезпечення інформаційної безпеки в комп'ютерній мережі ТОВ. Вона дозволяє визначити слабкі місця мережі та розробити відповідні заходи для їх усунення або мінімізації ризиків.

Загрози для інформаційної безпеки можна поділити на зовнішні та внутрішні. Зовнішні загрози включають мережеві атаки, злом і несанкціонований доступ, а також шкідливе програмне забезпечення. Мережеві атаки, такі як DDoS (Distributed Denial of Service), можуть призвести до перевантаження мережі та відмови в обслуговуванні. Такі атаки можуть здійснюватися зловмисниками ззовні з метою порушення роботи мережі. Злом і несанкціонований доступ передбачає атаки хакерів, які намагаються отримати несанкціонований доступ до мережевих

ресурсів через атаки на облікові записи користувачів, використання вразливостей програмного забезпечення або соціальну інженерію. Шкідливе програмне забезпечення включає віруси, трояни, руткіти та інші види шкідливого ПЗ, що можуть бути занесені в мережу через Інтернет, електронну пошту або змінні носії. Вони можуть спричинити втрату даних, порушення роботи систем та крадіжку інформації.

Внутрішні загрози можуть бути пов'язані з невірно налаштованими системами, недотриманням політик безпеки та інсайдерськими загрозами. Невірно налаштовані системи можуть містити помилки в конфігурації мережевих пристроїв, серверів та програмного забезпечення, що створює вразливості для атак. Недотримання політик безпеки співробітниками, наприклад, використання слабких паролів, відсутність двофакторної аутентифікації або недбале поводження з конфіденційною інформацією, може також створити вразливості. Інсайдерські загрози виникають, коли співробітники або колишні співробітники, які мають доступ до конфіденційної інформації, зловживають своїм доступом. Це може призвести до крадіжки даних або їх знищення.

Вразливості мережі можна поділити на мережеві та програмні. Мережеві вразливості включають незахищені мережеві пристрої та відкриті порти та сервіси. Незахищені мережеві пристрої, такі як комутатори, маршрутизатори та точки доступу Wi-Fi, можуть мати вразливі налаштування або застаріле програмне забезпечення, що робить їх ціллю для атак. Відкриті порти та сервіси, які залишаються доступними для зовнішнього доступу, можуть бути використані зловмисниками для проникнення в мережу. Програмні вразливості включають використання застарілого програмного забезпечення, яке містить відомі вразливості, та недостатній контроль доступу, що дозволяє несанкціонованим користувачам отримати доступ до конфіденційної інформації.

Людський фактор також відіграє важливу роль у виникненні загроз та вразливостей. Атаки фішингу та соціальної інженерії спрямовані на обман співробітників з метою отримання конфіденційної інформації або доступу до систем. Співробітники, які не дотримуються встановлених політик безпеки,

можуть створити додаткові вразливості, використовуючи особисті пристрої для роботи або недбало поводячись з паролями.

Для ідентифікації потенційних загроз і вразливостей використовуються різні методи та інструменти, такі як аудити безпеки, сканування вразливостей, тестування на проникнення та моніторинг та аналіз журналів подій. Аудити безпеки передбачають регулярні перевірки мережевої інфраструктури, конфігурацій та політик безпеки для виявлення потенційних вразливостей. Сканування вразливостей включає використання спеціалізованого програмного забезпечення для автоматичного виявлення вразливостей у мережевих пристроях та програмному забезпеченні. Тестування на проникнення передбачає проведення імітованих атак для перевірки захищеності систем та виявлення потенційних слабких місць. Моніторинг та аналіз журналів подій дозволяють виявляти підозрілу активність у мережі та своєчасно реагувати на можливі загрози [21].

Ідентифікація потенційних загроз і вразливостей є важливою складовою системи інформаційної безпеки, яка дозволяє ТОВ "Перша депозитарна установа" підтримувати рівень захисту своєї мережі та даних.

Для ілюстрації виявлення і вирішення проблем(загроз) створимо для ТОВ "Перша депозитарна установа" дерево проблем. Дерево проблем – це метод системного аналізу, який використовується для візуалізації проблем у вигляді діаграми з тим, щоб допомогти побачити та проаналізувати причинно-наслідкові зв'язки [22].



Рисунок 2.1 – Дерево проблем для ТОВ "Перша депозитарна установа"
Джерело: розроблено автором.

Загрози інформаційній безпеці ТОВ "Перша депозитарна установа" можуть мати серйозні наслідки для організації. Ідентифікація та аналіз цих загроз і вразливостей дозволяє розробити відповідні заходи для їх усунення або мінімізації ризиків, що є важливою складовою системи інформаційної безпеки організації.

Для забезпечення високого рівня інформаційної безпеки в ТОВ проводиться ретельний аналіз ризиків і оцінка впливу вразливостей на інформаційну інфраструктуру. Хоча ці заходи іноді можуть бути не достатньо ефективними, вони є важливими для визначення потенційних загроз, оцінки їх впливу на організацію та розробки ефективних заходів для мінімізації ризиків.

Кількісний аналіз ризиків базується на використанні числових значень для оцінки ймовірності виникнення ризиків і потенційних збитків від їх реалізації. У компанії використовується методика розрахунку очікуваних втрат (Annual Loss Expectancy, ALE), яка допомагає оцінити фінансовий вплив потенційних загроз. Формула $ALE = SLE \text{ (Single Loss Expectancy)} \times ARO \text{ (Annual Rate of Occurrence)}$, де SLE – потенційний збиток від однієї події, а ARO – частота виникнення події за

рік [21]. Цей підхід дозволяє отримати точніші дані для прийняття рішень щодо управління ризиками.

Також застосовується ймовірнісний аналіз, який включає використання ймовірнісних моделей, таких як дерево рішень або метод Монте-Карло, для оцінки ймовірності виникнення ризиків та їх впливу на організацію. Ці методи допомагають більш точно передбачити можливі сценарії розвитку подій та їх наслідки [23].

Якісний аналіз ризиків заснований на експертних оцінках і класифікації ризиків за категоріями, такими як висока, середня і низька ймовірність виникнення або впливу. У компанії використовується саме матриця ризиків, яка дозволяє класифікувати ризики за їх ймовірністю та впливом. Це допомагає визначити пріоритети у вирішенні питань безпеки та зосередити зусилля на найбільш критичних загрозах.

Матриця ризиків складається з осей "Ймовірність" та "Вплив", де кожен ризик оцінюється за цими критеріями та розміщується у відповідному квадраті матриці. Це дозволяє візуально оцінити пріоритети та розробити стратегії для зниження впливу найкритичніших ризиків.

Табл. 2.6 - Методи оцінки впливу вразливостей ТОВ "Перша депозитарна установа"

Метод	Опис
Аудити безпеки	Регулярні аудити безпеки проводяться для оцінки стану мережевої інфраструктури, конфігурацій та політик безпеки. Аудити допомагають виявити потенційні вразливості та розробити заходи для їх усунення.
Сканування вразливостей	Використання спеціалізованого програмного забезпечення для автоматичного виявлення вразливостей у мережевих пристроях та програмному забезпеченні. Це дозволяє швидко ідентифікувати слабкі місця та вжити заходів для їх усунення.
Тестування на проникнення	Проведення імітованих атак для перевірки захищеності систем та виявлення потенційних слабких місць. Цей метод допомагає

Продовження табл. 2.6

	оцінити, наскільки ефективні існуючі заходи безпеки і де вони потребують покращення.
Моніторинг та аналіз журналів	Регулярний моніторинг мережевої активності та аналіз журналів подій дозволяють виявляти підозрілу активність у мережі та своєчасно реагувати на можливі загрози. Це забезпечує безперервний контроль над станом мережі та своєчасне виявлення інцидентів безпеки.

Джерело: розроблено автором.

Усі ці методи спрямовані на те, щоб підтримувати високий рівень інформаційної безпеки та мінімізувати ризики, пов'язані з можливими загрозами та вразливостями в мережі ТОВ "Перша депозитарна установа".

Для забезпечення високого рівня інформаційної безпеки використовуються різноманітні інструменти та методи для виявлення вразливостей в інформаційній інфраструктурі. Ці інструменти та методи допомагають ідентифікувати потенційні загрози, оцінювати їх вплив та вживати заходів для усунення або мінімізації ризиків.

Табл. 2.7 - Інструменти та методи для виявлення вразливостей в інформаційній інфраструктурі

Інструмент/Метод	Опис
Сканування вразливостей	Використання спеціалізованого програмного забезпечення, такого як Nessus, OpenVAS або QualysGuard, для автоматичного виявлення вразливостей у мережевих пристроях, серверах та додатках. Цей метод дозволяє швидко ідентифікувати слабкі місця та вжити заходів для їх усунення.
Тестування на проникнення (Penetration Testing)	Проведення імітованих атак на інформаційні системи з метою виявлення та оцінки вразливостей. Використовуються такі інструменти, як Metasploit, Burp Suite та Kali Linux. Це дозволяє оцінити ефективність існуючих заходів безпеки та виявити області, які потребують покращення.

Аналіз конфігурацій	Перевірка конфігурацій мережевих пристроїв, серверів та додатків на відповідність політикам безпеки та найкращим практикам. Це допомагає виявити неправильні налаштування, які можуть створити вразливості.
Моніторинг безпеки та аналіз журналів (SIEM)	Використання систем моніторингу безпеки та управління журналами подій (Security Information and Event Management, SIEM), таких як Splunk, ArcSight або QRadar, для виявлення підозрілої активності в реальному часі та аналізу інцидентів безпеки.
Інструменти управління патчами	Використання програмного забезпечення для автоматичного управління оновленнями та патчами, таких як Microsoft SCCM або Ivanti, що забезпечує своєчасне встановлення оновлень безпеки для операційних систем та додатків.
Веб-сканери	Використання інструментів для аналізу безпеки веб-додатків, таких як OWASP ZAP або Acunetix, для виявлення вразливостей, пов'язаних із веб-інтерфейсами та веб-сервісами.

Джерело: розроблено автором.

Ці інструменти та методи забезпечують комплексний підхід до виявлення та усунення вразливостей.

2.3. Оцінка ефективності існуючої системи захисту інформації.

Оцінка ефективності існуючої системи захисту інформації в ТОВ "Перша депозитарна установа" починається з аналізу поточних заходів захисту та їх відповідності встановленим вимогам безпеки. Це дозволяє виявити сильні та слабкі сторони системи захисту і визначити напрямки для її вдосконалення.

Поточні заходи захисту:

- 1) Мережеві брандмауери та системи запобігання вторгненням (IPS/IDS)

Використовуються для захисту від зовнішніх атак та моніторингу мережевої активності. Вони блокують несанкціоновані спроби доступу та аналізують трафік для виявлення підозрілої активності [18].

2) Антивірусне та антишпигунське програмне забезпечення

Встановлене на всіх робочих станціях і серверах для виявлення та видалення шкідливих програм. Це забезпечує захист від вірусів, троянів, руткітів та інших шкідливих програм.

3) Системи резервного копіювання даних

Регулярне резервне копіювання критичних даних на зовнішні носії або хмарні сховища. Це дозволяє відновити дані у разі втрати або пошкодження через інциденти безпеки.

4) Шифрування даних

Використовується для захисту конфіденційної інформації під час передачі через мережу та зберігання на носіях. Це знижує ризик несанкціонованого доступу до даних.

5) Політики безпеки та навчання співробітників

Впроваджені політики безпеки, що регулюють використання інформаційних ресурсів. Регулярні навчання проводяться для підвищення обізнаності співробітників щодо питань безпеки.

Поточні заходи захисту в ТОВ "Перша депозитарна установа" відповідають основним вимогам інформаційної безпеки, таким як конфіденційність, цілісність та доступність інформації. Впроваджені заходи також відповідають нормативним вимогам та стандартам, таким як ISO/IEC 27001, які регулюють управління інформаційною безпекою.

Табл. 2.8 - Аналіз відповідності вимогам

Вимога	Відповідність
Конфіденційність	Забезпечується за допомогою шифрування даних та політик доступу, що обмежують доступ до конфіденційної інформації лише уповноваженим користувачам.

Цілісність	Підтримується за допомогою антивірусного ПЗ та систем моніторингу, які виявляють і запобігають спробам змінити або пошкодити дані.
Доступність	Гарантується за рахунок систем резервного копіювання та відновлення, що забезпечують безперервну доступність інформаційних ресурсів навіть у разі інцидентів.

Джерело: розроблено автором.

Для більш детальної оцінки ефективності існуючої системи захисту інформації доцільно провести SWOT-аналіз, який дозволить виявити сильні та слабкі сторони системи, а також можливості для її покращення і потенційні загрози [24].



Рисунок 2.2 - SWOT-аналіз ефективності існуючої системи захисту інформації ТОВ "Перша депозитарна установа".

Джерело: розроблено автором.

Однією з ключових сильних сторін існуючої системи захисту інформації є високий рівень мережевої безпеки, забезпечений завдяки використанню брандмауерів та систем запобігання вторгненням (IPS/IDS). Ці засоби дозволяють

блокувати несанкціоновані спроби доступу та аналізувати мережевий трафік для виявлення підозрілої активності. Також в компанії впроваджені політики безпеки, які регулюють використання інформаційних ресурсів, і проводяться регулярні навчання для співробітників, що підвищують їх обізнаність щодо загроз та методів захисту. Системи резервного копіювання даних забезпечують надійне зберігання інформації та можливість її відновлення у разі втрати або пошкодження через інциденти безпеки. Крім того, використання шифрування для захисту конфіденційної інформації під час передачі та зберігання знижує ризик несанкціонованого доступу до даних.

Серед слабких сторін існуючої системи захисту інформації варто виділити недостатнє автоматичне оновлення програмного забезпечення та патчів, що може призвести до вразливостей. Обмеженість у фінансуванні на придбання нових інструментів та технологій для захисту інформації також є значним недоліком. Це обмежує можливості для впровадження сучасних засобів захисту та підвищення рівня безпеки. Відсутність централізованої системи управління журналами подій та моніторингу мережевої активності в режимі реального часу ускладнює своєчасне виявлення та реагування на інциденти безпеки. Крім того, недостатня кількість кваліфікованих кадрів у сфері кібербезпеки може впливати на ефективне управління системою захисту та швидкість реагування на загрози.

Серед можливостей для покращення системи захисту інформації варто відзначити впровадження нових технологій і засобів захисту, таких як SIEM-системи (Security Information and Event Management). Використання таких систем дозволить централізувати управління безпекою, покращити моніторинг мережевої активності та підвищити швидкість реагування на інциденти. Збільшення фінансування та ресурсів для розвитку інфраструктури безпеки може сприяти впровадженню нових технологій та підвищенню рівня захисту інформації. Підвищення кваліфікації співробітників через спеціалізовані тренінги та сертифікаційні програми дозволить покращити їх навички та обізнаність у сфері кібербезпеки. Співпраця з зовнішніми фахівцями та консультантами також

сприятиме вдосконаленню системи захисту, адже вони можуть надати свіжий погляд на існуючі проблеми та запропонувати нові рішення.

Серед загроз, які можуть впливати на систему захисту інформації, варто виділити зростання кількості і складності кібератак. Постійно зростаючий рівень кіберзлочинності потребує постійного вдосконалення засобів захисту та оновлення методів боротьби з загрозами. Соціальна інженерія та фішингові атаки, спрямовані на співробітників організації, можуть призвести до компрометації інформації, адже вони часто базуються на обмані та маніпуляції. Вразливості в програмному забезпеченні та операційних системах можуть бути використані зловмисниками для атак на інформаційні системи. Внутрішні загрози від інсайдерів, які можуть зловживати своїм доступом до конфіденційної інформації, також становлять значний ризик для організації.

SWOT-аналіз дозволив виявити сильні та слабкі сторони існуючої системи захисту інформації, а також визначити можливості для її покращення та потенційні загрози. Сильні сторони, такі як високий рівень мережевої безпеки, впроваджені політики безпеки, системи резервного копіювання та використання шифрування, забезпечують надійний захист інформації. Однак, слабкі сторони, такі як недостатнє автоматичне оновлення ПЗ, обмеженість фінансування, відсутність централізованого моніторингу та недостатня кількість кваліфікованих кадрів, потребують уваги та вдосконалення. Можливості для покращення включають впровадження нових технологій, збільшення фінансування, підвищення кваліфікації співробітників та співпрацю з зовнішніми фахівцями. Загрози, такі як зростання кількості кібератак, соціальна інженерія, вразливості в ПЗ та внутрішні загрози від інсайдерів, потребують постійного моніторингу та адаптації заходів захисту для мінімізації ризиків.

Виходячи з проведеного SWOT-аналізу, компанія може значно покращити свою систему захисту інформації через ряд конкретних заходів. По-перше, необхідно впровадити автоматичне оновлення програмного забезпечення та патчів, щоб забезпечити своєчасне усунення вразливостей. Це дозволить мінімізувати ризик експлуатації вразливих місць зловмисниками.

По-друге, варто збільшити фінансування на придбання сучасних інструментів та технологій захисту інформації. Інвестування в нові системи, такі як SIEM (Security Information and Event Management), дозволить централізовано моніторити та аналізувати мережеву активність, що значно підвищить здатність до виявлення та реагування на загрози в реальному часі.

Підвищення кваліфікації співробітників через спеціалізовані тренінги та сертифікаційні програми дозволить покращити їх обізнаність та навички у сфері кібербезпеки. Це допоможе зменшити ризики, пов'язані з людським фактором, такими як фішингові атаки та соціальна інженерія.

Для більшої безпеки варто також розглянути співпрацю з зовнішніми фахівцями та консультантами у сфері кібербезпеки. Вони можуть надати свіжий погляд на існуючі проблеми та запропонувати нові рішення для покращення системи захисту.

Загалом, реалізація цих рекомендацій дозволить значно зміцнити поточну систему захисту інформації в ТОВ "Перша депозитарна установа", підвищити її ефективність та забезпечити надійний захист від сучасних кіберзагроз.

РОЗДІЛ 3

РОЗРОБКА ЗАХОДІВ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ

3.1. Оптимізація процесів управління захистом інформації.

Для ефективної оптимізації процесів управління захистом інформації в ТОВ "Перша Депозитарна Установа" необхідно спочатку провести детальний аналіз існуючих практик. Цей аналіз дозволить виявити слабкі місця та вразливості, а також визначити пріоритетні області для покращення.

В даний час ТОВ "Перша Депозитарна Установа" використовує комплексний підхід до управління інформаційною безпекою, включаючи фізичні, технічні та адміністративні заходи. Основні компоненти системи захисту включають використання мережевих екранів (firewalls), систем виявлення та запобігання вторгненням (IDS/IPS), антивірусного програмного забезпечення, а також регулярне оновлення програмного забезпечення для усунення відомих вразливостей. Крім того, організація впроваджує політики контролю доступу, які регламентують права доступу співробітників до інформаційних ресурсів.

Незважаючи на впровадження значної кількості заходів захисту, існують певні слабкі місця та вразливості, які потребують уваги. По-перше, системи управління патчами не завжди встигають оновлювати програмне забезпечення вчасно, що створює ризики експлуатації відомих вразливостей. По-друге, відсутність централізованого моніторингу мережевої активності може призводити до запізненої реакції на інциденти безпеки. По-третє, рівень обізнаності співробітників щодо політик безпеки не завжди є достатнім, що збільшує ризики, пов'язані з людським фактором, зокрема фішингом та соціальною інженерією.

Таким чином, проведення детального аналізу існуючих процесів управління захистом інформації в ТОВ "Перша Депозитарна Установа" дозволяє виявити

ключові слабкі місця та вразливості, а також визначити пріоритетні області для покращення. Оптимізація цих процесів є важливим кроком для підвищення ефективності системи захисту інформаційних ресурсів організації.

Для підвищення ефективності управління захистом інформації в ТОВ "Перша Депозитарна Установа" необхідно впроваджувати сучасні технології, що дозволяють автоматизувати процеси виявлення та реагування на загрози. Використання таких систем, як IDS/IPS, SIEM та EPP, може значно покращити рівень інформаційної безпеки в організації.

Використання автоматизованих систем (IDS/IPS, SIEM, EPP). Системи виявлення та запобігання вторгненням (IDS/IPS) дозволяють виявляти аномалії в мережевому трафіку та блокувати потенційні атаки в реальному часі. Ці системи забезпечують постійний моніторинг мережевої активності та автоматично реагують на підозрілі дії, що знижує ризик успішних атак. Інтеграція системи управління інформаційною безпекою (SIEM) дозволяє централізувати збір, аналіз та кореляцію журналів подій з різних джерел, що забезпечує повну картину стану безпеки в організації. Використання рішень для захисту кінцевих точок (EPP) забезпечує захист робочих станцій і серверів від шкідливого програмного забезпечення, включаючи віруси, трояни та руткіти.

Переваги автоматизації для швидкої реакції на загрози. Автоматизація процесів управління безпекою дозволяє значно скоротити час реакції на інциденти. Впровадження автоматизованих систем знижує навантаження на ІТ-персонал, оскільки багато завдань виконуються без участі людини. Наприклад, системи IDS/IPS автоматично блокують підозрілий трафік, а SIEM-системи автоматично корелюють події та генерують оповіщення про потенційні загрози. Це дозволяє швидко реагувати на інциденти та мінімізувати їх вплив на організацію. Крім того, автоматизація процесів забезпечує більш точне виявлення загроз завдяки використанню алгоритмів машинного навчання та аналізу великих обсягів даних.

Інтеграція новітніх технологій у існуючі процеси. Для досягнення максимального ефекту від впровадження нових технологій необхідно інтегрувати їх у існуючі процеси управління захистом інформації. В ТОВ "Перша Депозитарна

Установа" це може включати перегляд та оновлення політик безпеки, розробку нових процедур реагування на інциденти та навчання співробітників роботі з новими системами. Важливо забезпечити безшовну інтеграцію нових технологій, щоб вони доповнювали існуючі заходи безпеки, а не створювали додаткові складнощі. Наприклад, інтеграція SIEM-системи з існуючими джерелами журналів подій та системами управління дозволяє забезпечити централізоване управління безпекою та підвищити ефективність реагування на інциденти.

Таким чином, впровадження сучасних технологій в ТОВ "Перша Депозитарна Установа" дозволяє значно підвищити рівень захисту інформації. Використання автоматизованих систем IDS/IPS, SIEM та EPP забезпечує швидке та точне виявлення загроз, автоматичне реагування на інциденти та зниження навантаження на ІТ-персонал. Інтеграція новітніх технологій у існуючі процеси дозволяє забезпечити комплексний підхід до управління інформаційною безпекою та підвищити стійкість організації до сучасних кіберзагроз.

3.2. Розробка рекомендацій щодо вдосконалення захисту інформації на основі системного аналізу.

Для забезпечення високого рівня інформаційної безпеки в ТОВ "Перша Депозитарна Установа" необхідно вдосконалити багаторівневий підхід до захисту інформації. Це включає впровадження сучасних рішень на рівні мережі, кінцевих точок, а також захисту даних і додатків.

Захист на рівні мережі є одним із ключових елементів багаторівневого підходу. Використання мережевих екранів (firewalls) дозволяє контролювати вхідний та вихідний трафік, забезпечуючи захист від несанкціонованого доступу та зовнішніх загроз. Інтеграція систем виявлення та запобігання вторгненням (IDS/IPS) дозволяє автоматично виявляти аномалії в мережевому трафіку та

блокувати потенційні атаки в реальному часі. Це забезпечує додатковий рівень захисту, мінімізуючи ризик успішних атак [25].

Захист кінцевих точок включає впровадження антивірусного програмного забезпечення та засобів шифрування. Антивірусне програмне забезпечення забезпечує захист робочих станцій і серверів від шкідливого програмного забезпечення, включаючи віруси, трояни та руткіти. [26] Використання засобів шифрування забезпечує захист даних на кінцевих точках, запобігаючи несанкціонованому доступу до конфіденційної інформації у разі втрати або крадіжки пристрою. Крім того, шифрування дисків і файлів допомагає захистити дані від внутрішніх загроз.

Захист даних і додатків є критично важливим для забезпечення конфіденційності та цілісності інформації. Використання шифрування для захисту даних під час їх передачі та зберігання забезпечує високий рівень безпеки. Політики контролю доступу дозволяють регламентувати права доступу до конфіденційної інформації, запобігаючи несанкціонованому доступу [27]. Це включає використання ролей та привілеїв для обмеження доступу до важливих даних лише авторизованим користувачам.

Таблиця 3.1 – Пропозиції щодо вдосконалення багаторівневого підходу до захисту інформації

Рівень захисту	Заходи	Опис
Захист на рівні мережі	Використання мережевих екранів (firewalls)	Контроль вхідного та вихідного трафіку, захист від несанкціонованого доступу та зовнішніх загроз.
	Інтеграція систем виявлення та запобігання вторгненням (IDS/IPS)	Виявлення аномалій у мережевому трафіку, автоматичне блокування потенційних атак у реальному часі.
Захист кінцевих точок	Впровадження антивірусного програмного забезпечення	Захист робочих станцій і серверів від шкідливого програмного забезпечення.

Продовження табл. 3.1

	Використання засобів шифрування	Захист даних на кінцевих точках, шифрування дисків і файлів.
Захист даних і додатків	Використання шифрування для захисту даних під час передачі та зберігання	Забезпечення конфіденційності та цілісності інформації.
	Політики контролю доступу	Регламентація прав доступу до конфіденційної інформації, обмеження доступу лише авторизованим користувачам.

Джерело: розроблено автором.

Вдосконалення багаторівневого підходу до захисту інформації в ТОВ "Перша Депозитарна Установа" дозволить забезпечити більш надійний захист інформаційних ресурсів від різноманітних загроз. Використання сучасних технологій та інструментів, таких як мережеві екрани, IDS/IPS, антивірусне програмне забезпечення та засоби шифрування, значно підвищить рівень безпеки в організації. Крім того, впровадження політик контролю доступу дозволить забезпечити належний рівень конфіденційності та цілісності даних, запобігаючи несанкціонованому доступу до критично важливої інформації.

Оновлення політик і процедур безпеки є важливим кроком у забезпеченні ефективного захисту інформації в ТОВ "Перша Депозитарна Установа". Враховуючи результати системного аналізу, необхідно розробити нові політики, забезпечити їх відповідність сучасним стандартам та регламентам, а також комунікувати їх до всіх співробітників організації.

Для забезпечення високого рівня інформаційної безпеки слід розробити нові політики, які враховують сучасні вимоги та виклики. Ці політики повинні охоплювати всі аспекти захисту інформації [28], включаючи контроль доступу, управління ризиками, реагування на інциденти, використання шифрування, зберігання та передачу даних. Розроблені політики мають бути чіткими та доступними для розуміння всіма співробітниками. Вони повинні включати конкретні вимоги та інструкції, що допоможуть мінімізувати ризики та забезпечити належний рівень захисту інформаційних ресурсів.

Політики безпеки ТОВ "Перша Депозитарна Установа" повинні відповідати сучасним міжнародним стандартам і регламентам, таким як ISO/IEC 27001 та GDPR. Це дозволить організації не тільки забезпечити високий рівень захисту інформації, але й відповідати вимогам законодавства та регуляторів. Відповідність стандартам і регламентам допомагає забезпечити систематичний і структурований підхід до управління інформаційною безпекою. Для цього необхідно провести аудит існуючих політик і процедур, виявити невідповідності та внести необхідні зміни для досягнення відповідності встановленим вимогам.

Ефективність нових політик і процедур безпеки залежить від їх правильного впровадження та дотримання всіма співробітниками організації. Тому важливо забезпечити їхню комунікацію до всіх рівнів організації. Це можна зробити за допомогою регулярних тренінгів, семінарів, внутрішніх комунікаційних каналів та документів. Співробітники повинні розуміти важливість дотримання політик безпеки, а також знати свої обов'язки та відповідальність у цій сфері. Крім того, слід забезпечити зворотний зв'язок, щоб співробітники могли ставити питання та отримувати необхідні роз'яснення щодо нових вимог.

Оновлення політик і процедур безпеки в ТОВ "Перша Депозитарна Установа" є необхідним для забезпечення належного рівня інформаційної безпеки. Розробка чітких і доступних політик, їх відповідність сучасним стандартам та регламентам, а також ефективна комунікація до всіх співробітників сприяють створенню надійної системи захисту інформаційних ресурсів. Це дозволяє організації бути готовою до сучасних викликів і мінімізувати ризики, пов'язані з інформаційною безпекою.

Для підвищення ефективності захисту інформації в ТОВ "Перша Депозитарна Установа" необхідно розробити чіткий план впровадження запропонованих заходів, забезпечити моніторинг їх реалізації та оцінку ефективності, а також регулярно переглядати та оновлювати заходи захисту інформації.

Впровадження нових заходів з безпеки вимагає ретельного планування та визначення необхідних ресурсів. Першим етапом є формування робочої групи, яка

відповідатиме за реалізацію заходів. Ця група має включати фахівців з інформаційної безпеки, IT-персонал та представників керівництва. Другим етапом є розробка детального плану дій, що включає конкретні заходи, строки їх виконання та необхідні ресурси. Наприклад, для впровадження нових систем IDS/IPS необхідно визначити відповідальну особу, підготувати технічні вимоги, провести закупівлі та встановлення обладнання. Третій етап включає навчання персоналу роботі з новими системами та проведення тестування для перевірки їх працездатності.

Після впровадження нових заходів з безпеки важливо забезпечити постійний моніторинг їх реалізації та оцінку ефективності. Це дозволить вчасно виявляти проблеми та коригувати дії для досягнення поставлених цілей. Моніторинг включає регулярний збір даних про стан безпеки, аналіз журналів подій, проведення внутрішніх аудитів та тестування на проникнення. Оцінка ефективності може проводитися на основі ключових показників, таких як кількість виявлених вразливостей, час реакції на інциденти, рівень відповідності нормативам тощо. Результати оцінки повинні аналізуватися керівництвом організації для прийняття рішень щодо подальших дій.

Інформаційні загрози постійно еволюціонують [29], тому заходи з безпеки повинні бути динамічними та адаптуватися до нових викликів. Регулярний перегляд та оновлення заходів захисту інформації є необхідним для підтримання високого рівня безпеки. Це включає проведення періодичних аудитів, перегляд політик та процедур безпеки, впровадження нових технологій та засобів захисту. Наприклад, на основі результатів моніторингу та оцінки ефективності можуть бути прийняті рішення про необхідність оновлення програмного забезпечення, зміни конфігурацій мережевого обладнання або впровадження додаткових заходів захисту. Також важливо забезпечити постійне навчання співробітників новим методам захисту та підвищення їх обізнаності щодо сучасних загроз.

Таким чином, план впровадження заходів та оцінка ефективності є ключовими елементами вдосконалення системи захисту інформації в ТОВ "Перша Депозитарна Установа". Чітко визначені етапи, відповідні ресурси, постійний

моніторинг та регулярний перегляд заходів забезпечують належний рівень захисту інформаційних ресурсів, сприяючи підвищенню стійкості організації до сучасних кіберзагроз.

Дерево рішень є ефективним інструментом для аналізу та прийняття рішень у складних ситуаціях [22]. Воно являє собою графічну модель, яка відображає всі можливі варіанти рішень і їх наслідки, дозволяючи систематично підходити до вибору оптимальних заходів. Для ТОВ "Перша Депозитарна Установа" розробка дерева рішень допоможе визначити найбільш ефективні заходи з покращення захисту інформації, враховуючи наявні ресурси та потенційні ризики.

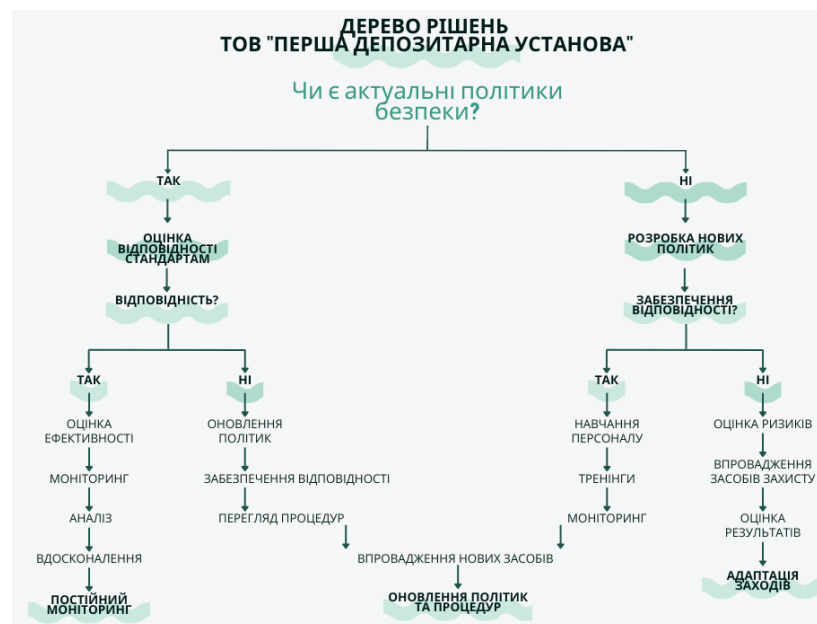


Рисунок 3.1 – Дерево рішень для ТОВ "Перша депозитарна установа"

Джерело: розроблено автором.

Можемо побачити як послідовно та систематично приймати рішення щодо оптимізації захисту інформації в ТОВ "Перша Депозитарна Установа". Процес починається з оцінки поточних політик безпеки, щоб визначити їх актуальність. Якщо політики є актуальними, проводиться їх оцінка відповідності сучасним стандартам і регламентам. Якщо політики відповідають стандартам, наступним кроком є оцінка їх ефективності. У випадку, якщо політики не відповідають стандартам, необхідно провести їх оновлення.

Оцінка ефективності політик включає моніторинг їх дотримання та аналіз результатів. Це дозволяє виявити, наскільки політики сприяють досягненню цілей

інформаційної безпеки. Якщо політики є ефективними, проводиться постійний моніторинг їх дотримання. Якщо ж політики виявляються неефективними, необхідно їх переглянути та вдосконалити, що включає впровадження нових засобів захисту [18].

Якщо ж на початковому етапі було виявлено, що політики не є актуальними, необхідно розробити нові політики безпеки. Це включає забезпечення їх відповідності сучасним стандартам та регламентам. Далі слід провести навчання персоналу щодо нових політик, що допоможе підвищити їхню обізнаність та знизити ризики, пов'язані з людським фактором.

Навчання персоналу включає проведення регулярних тренінгів та семінарів, що дозволяє співробітникам краще розуміти політики та процедури безпеки. Після цього необхідно здійснити оцінку ризиків для визначення пріоритетних областей для впровадження заходів захисту. На основі цієї оцінки проводиться впровадження засобів захисту, таких як шифрування, антивірусне програмне забезпечення тощо.

Постійний моніторинг та оцінка результатів впроваджених заходів дозволяють виявити їх ефективність та необхідність у подальших коригуваннях. На основі результатів моніторингу проводиться адаптація заходів, що включає оновлення політик та процедур для забезпечення постійного підвищення рівня захисту інформації [30].

Розробка дерева рішень дозволяє ТОВ "Перша Депозитарна Установа" систематизувати процеси захисту інформації, забезпечити їх прозорість та ефективність. Це сприяє прийняттю обґрунтованих рішень та підвищує рівень інформаційної безпеки в організації.

ВИСНОВКИ

Проведене дослідження системного аналізу управління захистом інформації в комп'ютерних мережах та розроблені рекомендації дозволили визначити чіткі напрямки для підвищення ефективності управління захистом інформації в ТОВ "Перша Депозитарна Установа". Аналіз теоретичних засад і існуючих методологій системного аналізу забезпечив міцну основу для подальших практичних дій. Виявлені загрози та вразливості дозволили чітко визначити пріоритетні напрями для вдосконалення, що сприяло більш цілеспрямованому підходу до захисту інформації.

Оптимізація процесів управління, зокрема впровадження сучасних технологій і автоматизації, суттєво підвищить ефективність реагування на інциденти безпеки. Впровадження автоматизації знизить навантаження на ІТ-персонал, підвищить точність і швидкість виявлення загроз, що в свою чергу мінімізує потенційні збитки від можливих інцидентів.

Оновлення політик і процедур безпеки, їх відповідність міжнародним стандартам і регламентам забезпечать високий рівень захищеності інформаційних ресурсів, відповідність законодавчим вимогам і підвищення довіри з боку партнерів і клієнтів. Підвищення обізнаності та кваліфікації співробітників завдяки регулярним тренінгам і навчальним програмам значно знизить ризики, пов'язані з людським фактором.

Розробка і впровадження дерева рішень дозволить систематизувати підхід до управління захистом інформації, забезпечивши прозорість і послідовність у прийнятті рішень. Це сприятиме більш обґрунтованому підходу до впровадження заходів безпеки і підвищить загальну ефективність системи захисту інформації.

Крім того, використання методів системного аналізу, таких як SWOT-аналіз і дерево проблем, надало можливість всебічно оцінити поточний стан інформаційної безпеки в організації та виявити ключові слабкі місця. SWOT-аналіз допоміг ідентифікувати сильні і слабкі сторони, а також можливості і загрози, що

дозволило розробити більш цілеспрямовані і ефективні рекомендації. Дерево проблем забезпечило структурований підхід до виявлення кореневих причин проблем у захисті інформації, що сприяло розробці більш ефективних стратегій для їх усунення.

Підсумовуючи, можна стверджувати, що проведена робота визначила низку заходів та їх послідовність для підвищення рівня інформаційної безпеки в ТОВ "Перша Депозитарна Установа". Запропоновані заходи забезпечать стійкість організації до сучасних кіберзагроз, знизять ризики і підвищать ефективність управління інформаційними ресурсами. Ці рекомендації нададуть можливість створення безпечного інформаційного середовища в умовах постійно зростаючих загроз і вимог сучасного світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Янчук Т. В. ЗНАЧЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ. Акредитація освітніх програм економічного блоку в умовах війни. 2022. URL: <https://doi.org/10.36059/978-966-397-259-6-23>
2. Хамленко І. І. ФІЛОСОФІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ : thesis. 2013. URL: <http://er.nau.edu.ua/handle/NAU/10788> (дата звернення: 08.02.2024).
3. Самедова Л. Р. Ідентифікація поняття інформаційної безпеки в сучасних економічних умовах. Студентський вісник Національного університету водного господарства та природокористування. 2018. Вип. 1 (9). С. 131–133.
4. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ / А. Al-Ammouri та ін. Системи управління, навігації та зв'язку. Збірник наукових праць. 2024. Т. 1, № 75. С. 38–44. URL: <https://doi.org/10.26906/sunz.2024.1.038>
5. Василюк В. Об'єкти захисту інформації. Методи та засоби захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. Вип. 2 (13). С. 88–95.
6. Правові засади захисту інформації в Україні : thesis / А. Ю. Тверезовська та ін. 2015. URL: <http://essuir.sumdu.edu.ua/handle/123456789/41617> (дата звернення: 08.05.2024).
7. Кубрак О. В. Деякі аспекти інформаційної безпеки та інформаційної культури. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи. 2023. URL: <https://doi.org/10.32782/ppss.2023.1.63>
8. К. В. Захаренко К. В. МІЖНАРОДНИЙ ДОСВІД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки. 2019. С. 95–109. URL: <https://doi.org/10.34142/24130060.2019.17.1.09>

9. Degtyareva L., Miroshnykova M., Voloshko S. АНАЛІЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ. Системи управління, навігації та зв'язку. Збірник наукових праць. 2019. Т. 2, № 54. С. 78–82. URL: <https://doi.org/10.26906/sunz.2019.2.078>
10. Fadila V., Mutiah N., Sari R. P. Cyber Security Audit using CIS CSC, NIST CSF and COBIT 2019 Framework. CESS (Journal of Computer Engineering, System and Science). 2023. Vol. 8, no. 2. P. 271. URL: <https://doi.org/10.24114/cess.v8i2.43257>
11. Sulistyowati D., Handayani F., Suryanto Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV : International Journal on Informatics Visualization. 2020. Vol. 4, no. 4. P. 225. URL: <https://doi.org/10.30630/joiv.4.4.482>
12. Галаган О. Ю. Управління захистом інформації в контексті фінансово-економічної безпеки підприємства : thesis. 2018. URL: <https://er.knutd.edu.ua/handle/123456789/9997> (дата звернення: 09.05.2024).
13. Павленко Л. І. Шляхи комплексного визначення ефективності захисту інформації. Актуальні проблеми міжнародних відносин. 2006. Вип. 64, ч. 1. С. 97–102.
14. Палагнюк Д. М., Тищук Д. С., Березюк О. В. Принципи забезпечення інформаційної безпеки : thesis. 2018. URL: <http://ir.lib.vntu.edu.ua/handle/123456789/24491> (дата звернення: 09.05.2024).
15. Шемчук В. Принципи забезпечення інформаційної безпеки. Наукові записки Інституту законодавства Верховної Ради України. 2018. № 4. С. 50–56.
16. ПЕРША ДЕПОЗИТАРНА УСТАНОВА. *YouControl*. URL: <https://youcontrol.com.ua/>.
17. Ову Л., Owoo L. Розробка проекту комп'ютерної мережі для офісу компанії : bachelor's thesis. 2022. URL: <http://elartu.tntu.edu.ua/handle/lib/37228> (дата звернення: 10.05.2024).
18. Droniuk I. M., Fedevych O. Y. ПРОГРАМНИЙ КОМПЛЕКС МОНІТОРИНГУ ТА ПРОГНОЗУВАННЯ ТРАФІКУ ПОТОКУ В СЕГМЕНТІ

КОМП'ЮТЕРНОЇ МЕРЕЖІ. *Scientific Bulletin of UNFU*. 2015. Т. 25, № 10. С. 295–301. URL: <https://doi.org/10.15421/40251045>

19. Дудикевич В. Б., Томашевський Б. П., Сергієнко Р. В. Протоколи і механізми безпеки інформації в комп'ютерних системах і мережах. *Ukrainian Information Security Research Journal*. 2009. Т. 11, № 2(43). URL: <https://doi.org/10.18372/2410-7840.11.4043>

20. Сергієнко Ю. С. Протоколи динамічної маршрутизації в корпоративних мережах : master's thesis. 2020. URL: <https://essuir.sumdu.edu.ua/handle/123456789/82256> (дата звернення: 10.05.2024).

21. Ухман А. М. Метод виявлення мережевих аномалій та потенційних загроз на прикладі комп'ютерної мережі ТНТУ : master's thesis. 2018. URL: <http://elartu.tntu.edu.ua/handle/lib/26979> (дата звернення: 17.05.2024).

22. Шугайло Я. Використання інструментів "дерево проблем" та "дерево рішень" в проєктній діяльності майбутніх фахівців з професійної освіти : thesis. 2021. URL: <https://er.knutd.edu.ua/handle/123456789/19123> (дата звернення: 15.05.2024).

23. Абламська В. ОСНОВНІ АСПЕКТИ КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ. *SPECIALIZED AND MULTIDISCIPLINARY SCIENTIFIC RESEARCHES*. 2020. URL: <https://doi.org/10.36074/11.12.2020.v2.21>

24. Kniazeva M., Baskin E. SWOT Analysis. 2455 Teller Road, Thousand Oaks California 91320 United States : SAGE Publications, Inc., 2023. URL: <https://doi.org/10.4135/9781071902943>

25. Солодовник М. С. ЗАСТОСУВАННЯ НЕЙРО-НЕЧІТКОГО ПІДХОДУ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ І ОПТИМАЛЬНОЇ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ. *Refrigeration Engineering and Technology*. 2014. Т. 50, № 1. URL: <https://doi.org/10.15673/0453-8307.1/2014.32663>

26. Samociuk D. Antivirus Evasion Methods in Modern Operating Systems. *Applied Sciences*. 2023. Vol. 13, no. 8. P. 5083. URL: <https://doi.org/10.3390/app13085083>

27. A systematic literature review for authorization and access control: definitions, strategies and models / A. K. Y. S. Mohamed et al. *International Journal of Web Information Systems*. 2022. URL: <https://doi.org/10.1108/ijwis-04-2022-0077>
28. Komatsu A., Takagi D., Takemura T. Human aspects of information security. *Information Management & Computer Security*. 2013. Vol. 21, no. 1. P. 5–15. URL: <https://doi.org/10.1108/09685221311314383>
29. Evolution of Malware Threats and Techniques: a Review / M. N. Alenezi et al. *International Journal of Communication Networks and Information Security (IJCNIS)*. 2022. Vol. 12, no. 3. URL: <https://doi.org/10.17762/ijcnis.v12i3.4723>
30. Alhogail A. Enhancing information security best practices sharing in virtual knowledge communities. *VINE Journal of Information and Knowledge Management Systems*. 2020. Ahead-of-print, ahead-of-print. URL: <https://doi.org/10.1108/vjikms-01-2020-0009>

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

ID перевірки:
1016334691

Дата перевірки:
08.06.2024 11:15:45 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2024 11:28:23 EEST

ID користувача:
100005746

Назва документа: Диплом_Долженков

Кількість сторінок: 51 Кількість слів: 10211 Кількість символів: 83507 Розмір файлу: 568.48 KB ID файлу: 1016135145

5.29% Схожість

Найбільша схожість: 0.39% з джерелом з Бібліотеки (ID файлу: 1003958057)

2.91% Джерела з Інтернету 288 Сторінка 53

4.62% Джерела з Бібліотеки 489 Сторінка 55

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0% Вилучень

Немає вилучених джерел