

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

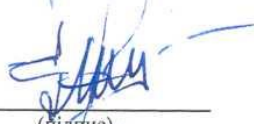
ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: Система інформаційної безпеки підприємства від кіберзагроз

Здобувача вищої освіти другого (магістерського) рівня,
II курсу, групи КМІ-23-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології в економіці»

Науковий керівник 
(підпис) Варіна Олега Олеговича

Науковий керівник 
(підпис) Філоненко Михайло
Миколайович, к.е.н.,
доцент

Керівник освітньо-
професійної програми 
(підпис) Горбовий Артур Юліанович,
д.т.н, професор

Допущено до захисту за рішенням кафедри протокол від «10» січня 2025 №11

Завідувач кафедри 
(підпис) Філоненко Михайло
Миколайович, к.ф.-м.н.,
доцент

Ірпінь – 2025

Реєстрація № 5

27.01.2025

(дата)



(підпис відповідальної особи)

Результати перевірки

до захисту

(до захисту, на доопрацювання)

27.01.2025

(дата)



(підпис)

Результат захисту

3 (задовільно)

(оцінка)

06.02.2025

(дата)



(підпис)

Голова комісії:



(підпис)

В.М. Франчук

(ініціали, прізвище)

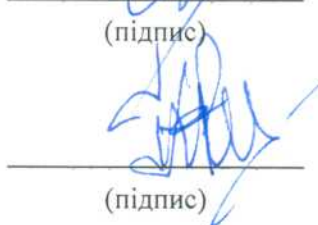
Члени комісії:



(підпис)

А.Ю. Горбовий

(ініціали, прізвище)



(підпис)

М.М. Філоненко

(ініціали, прізвище)



(підпис)

І.Д. Погореловська

(ініціали, прізвище)

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст кваліфікаційної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	18		06.02.2025 Франчук В.М. Горбовий А.Ю. Філоненко М.М. Погорсловська І.Д. Суховерхівка Л.П.
2. Дотримання вимог щодо оформлення	від 0 до 10	7		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	3		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	32		

Оцінювання кваліфікаційної роботи науковим керівником - 34 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

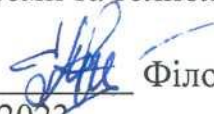
Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підписи)
66	D	3 (задовільно)	06.02.2025	Франчук В.М. Горбовий А.Ю. Філоненко М.М. Погорсловська І.Д. Суховерхівка Л.П.

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	3 (задовільно)
50-59	E	
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 122 «Комп'ютерні науки»
Освітня програма: «Інформаційні управляючі системи та технології в економіці»

Затверджую

Завідувач кафедри  Філоненко М. М.

«23» грудня 2023

**Завдання на кваліфікаційну роботу
здобувачу вищої освіти**

Варіну Олегу Олеговичу

(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи
«Система інформаційної безпеки підприємства від кіберзагроз»
Затверджена наказом ректора від «20» грудня 2023 р. № 1701
2. Строк здачі закінченої роботи: «7» січня 2025р.
3. Мета роботи: «Проектування найбільш ефективної системи захисту інформації»
Об'єкт дослідження: Огляд існуючих стандартів безпеки інформації.
Предмет дослідження: Моделі захисту інформації
4. Вихідні дані до роботи: Підбір та обґрунтування методів захисту інформації.
5. Перелік графічного матеріалу: Структурні схеми системи, діаграми потоків даних та макети інтерфейсу користувача.
6. Зміст випускної кваліфікаційної (дипломної) роботи (перелік питань за кожним розділом):
Розділ 1: ПРИНЦИПИ безпеки інформації
 - 1.1. Поняття безпеки інформації
 - 1.2. Огляд існуючих стандартів безпеки інформації
 - 1.3. Аналіз сучасного використання сонячних батарей в розумних будинках*Розділ 2: МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ*
 - 2.1. Вразливості інформації
 - 2.2. Протоколи захисту інформації
 - 2.3. Моделі, засновані на правилах та сигнатурах
 - 2.3.1. Моделі, засновані на правилах та сигнатурах
 - 2.3.2. Моделі, що ґрунтується на аномаліях
 - 2.3.3. Модель із використанням методів машинного навчання*Розділ 3: Проектування системи інформаційної безпеки підприємства на базі моделей безпеки*

- 3.2. Підбір та обґрунтування методів захисту інформації
 3.3. Підбір та обґрунтування інструментів захисту інформації
 3.4. Проектування найбільш ефективної системи захисту інформації
 7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури ДР	До 16.11.2023 р.	16.11. 2025 р.
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26.03. 2024 р.	26.03. 2025 р.
3	II розділ (аналіз експериментальної частини про і методики досліджень)	20. 06.2024 р.	20. 06. 2025 р.
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	15.10.2024 р.	15. 10. 2025 р.
5	Висновки	20.11.2024 р.	20. 11. 2025 р.
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	20.01.2025 р.	20. 01. 2025 р.
7	Отримання відгуку керівника	25.01.2025 р.	25. 01. 2025 р.
8	Отримання зовнішньої рецензії	27.01.2025р.	27. 01. 2025 р.

Дата видачі завдання «23» грудня 2023 р.

Керівник дипломної роботи


 (підпис) Філоненко М. М.

Керівник освітньо-професійної програми


 (підпис) Горбовий А. Ю.

Завдання до виконання отримав здобувач вищої освіти


 (підпис) Варін О. О.

АНОТАЦІЯ

Дипломна робота присвячена аналізу, розробці та впровадженню систем інформаційної безпеки на підприємствах з урахуванням сучасних кіберзагроз. У роботі розглянуто основні принципи забезпечення інформаційної безпеки, методи захисту даних, протоколи безпеки та моделі, засновані на правилах, аномаліях і машинному навчанні. Визначено ключові ризики та загрози, включаючи шкідливе програмне забезпечення, DDoS-атаки, фішинг, соціальну інженерію, а також внутрішні фактори, такі як помилки співробітників чи порушення політик.

У роботі також аналізуються міжнародні стандарти (ISO/IEC 27001, NIST, GDPR) та інструменти кіберзахисту, які забезпечують конфіденційність, цілісність та доступність інформаційних ресурсів. Особливу увагу приділено впровадженню адаптивних моделей безпеки, що базуються на машинному навчанні, для автоматичного виявлення та нейтралізації кіберзагроз.

Результати дослідження можуть бути використані для вдосконалення систем управління інформаційною безпекою підприємств, підвищення їх стійкості до кіберзагроз та ефективного управління ризиками.

КЛЮЧОВІ СЛОВА: Інформаційна безпека, Кіберзагроз, Конфіденційність, Цілісність даних, Доступність інформації, Захист від DDoS-атак, Фішинг, Машинне навчання, ISO/IEC 27001, Захист даних.

ABSTRACT

The thesis is dedicated to the analysis, development, and implementation of information security systems for enterprises, considering modern cyber threats. The study examines the key principles of information security, data protection methods, security protocols, and models based on rules, anomalies, and machine learning. The main risks and threats are identified, including malware, DDoS attacks, phishing, social engineering, and internal factors such as employee errors or policy violations.

The work also analyzes international standards (ISO/IEC 27001, NIST, GDPR) and cybersecurity tools that ensure the confidentiality, integrity, and availability of information resources. Special attention is given to the implementation of adaptive security models based on machine learning for the automatic detection and neutralization of cyber threats.

The results of the study can be applied to improve enterprise information security management systems, enhance their resilience to cyber threats, and effectively manage risks.

KEYWORDS: Information Security, Cyber Threats, Confidentiality Data Integrity, Information Availability, Protection Against DDoS Attacks, Phishing, Machine Learning, ISO/IEC 27001, Data Protection.

ВСТУП	3
РОЗДІЛ 1. ПРИНЦИПИ БЕЗПЕКИ ІНФОРМАЦІЇ	5
1.1. Поняття безпеки інформації	5
1.2. Огляд існуючих стандартів безпеки інформації	8
1.3. Постановка задачі	12
2. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ	15
2.1. Вразливості інформації	15
2.2. Протоколи захисту інформації	21
2.3. Моделі захисту інформації	25
2.3.1 Моделі, засновані на правилах та сигнатурах	27
2.3.2 Моделі, що ґрунтується на аномаліях	28
2.3.3 Модель із використанням методів машинного навчання	29
3. ПРОЕКТУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІДПРИЄМСТВА НА БАЗІ МОДЕЛЕЙ БЕЗПЕКИ	33
3.1. Підбір та обґрунтування методів захисту інформації	33
3.2. Підбір та обґрунтування інструментів захисту інформації	37
3.3. Проектування найбільш ефективної системи захисту інформації ..	49
ВИСНОВКИ	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	58

ВСТУП

В умовах розвитку комп'ютерних і інформаційно-телекомунікаційних технологій знаходження кордону приватних та публічних інтересів стає з кожним разом все більше скрутним, особливо в світлі нещодавно прийнятих законодавчих заходів протидії тероризму і забезпечення суспільної безпеки. Тим часом криза виступає не лише знаряддям розхитування системи, що склалася, цінностей, в яких перебуває суспільство і людина, а й переломним моментом в осмисленні того величезного значення, яке несе в собі недоторканність приватного життя для розвитку правосвідомості людини.

Забезпечення інформаційної безпеки є одним з центральних ланок в зовнішній політиці будь-якої держави, все це, безумовно, пов'язано з глобальною інформаційною революцією. Одночасний розвиток двох сфер - з однієї сторони постійне зростання обсягу інформації і її ролі в життя кожного, з іншої сторони, постійний процес розвитку і вдосконалення технологій накопичення та поширення інформації. Тому надійна робота інформаційних ресурсів, систем управління та зв'язку має виняткове значення для обороноздатності країни, для стійкого розвитку економіки і соціальної сфери, для того щоб забезпечити суверенітет держави.

Безперечно, ні одна сфера життя на сучасному етапі розвитку людства не може функціонувати без розвиненої інформаційної структури. Саме тому національний інформаційний ресурс став на сьогоднішній момент одним із ключових факторів, що впливають на всі сфери, а основним з них є економіка, так як зростання будь-якого держави, залежить від економічного складника, держава зацікавлена в ретельному регулюванні цієї сфери.

Державі особливо в умовах війни необхідно приділити увагу і направити всі свої зусилля у бік запобігання діям, спрямованим на виникнення і введення інформаційних воєн, які дестабілізують систему національної безпеки. Для того,

щоб суспільство продовжувало розвиватися і стрімко прогресувало, державі необхідно забезпечити кібербезпеку.

Мета цієї роботи полягає в тому, щоб вивчити теоретичні основи, що визначають місце та роль інформаційної безпеки, визначити проблеми в ході здійснення аналізу загроз, визначити шляхи вирішення виявлених проблем.

У відповідно з зазначеною метою були поставлені наступні завдання:

- вивчити основи інформаційної безпеки в сучасних умовах;
- система інформаційної безпеки підприємств від кіберзагроз

Об'єктом дослідження є система інформаційної безпеки підприємств.

Предметом дослідження є механізми, методи та засоби забезпечення інформаційної безпеки підприємств від кіберзагроз.

У ході роботи застосовувалися такі методи дослідження як загальнонаукові, в зокрема, в даному випадку можна виділити наступні методи: аналіз, синтез, дедукція, індукція, системний та функціональний підходи, а також приватно-наукові методи, основними з яких були формально-юридичний, порівняльно-правовий і соціологічний.

Сфера інформаційної безпеки є новим напрямом в області забезпечення національної безпеки держави, а саме поняття національної безпеки не є класичним для вітчизняної юриспруденції. Вказана обставина зумовлює необхідність проведення відповідних досліджень, необхідність яких обумовлена в числі іншого і необхідністю оновлення і доповнення існуючої юридичної термінології, впровадженні нових дефініцій в юридичний дискурс.

Теоретична і практична значимість випускний кваліфікаційної роботи полягає в тому, що основні положення та висновки дослідження можуть бути використані в подальших наукових дослідженнях, а також в правотворчій діяльності по вдосконаленню чинного законодавства, спрямованою на усунення виявлених в роботі проблем.

РОЗДІЛ 1. ПРИНЦИПИ БЕЗПЕКИ ІНФОРМАЦІЇ

1.1. Поняття безпеки інформації

Безпека інформації на підприємстві — це система заходів і процесів, спрямованих на захист інформаційних ресурсів підприємства від різноманітних загроз. Це включає захист даних від несанкціонованого доступу, зміни, пошкодження або знищення, а також забезпечення їх конфіденційності, цілісності та доступності.

Основні аспекти безпеки інформації на підприємстві:

Конфіденційність — забезпечення того, щоб лише авторизовані особи мали доступ до певної інформації.

Цілісність — гарантування, що інформація не буде змінена або пошкоджена без дозволу під час зберігання, обробки або передачі.

Доступність — забезпечення того, щоб інформація була доступною і використовуваною для авторизованих користувачів у потрібний час.

Аутентифікація та авторизація — процеси перевірки особистості користувачів і надання їм прав доступу до інформаційних систем.

Ідентифікація загроз і ризиків — це важливий крок для визначення потенційних небезпек, які можуть виникнути через людський фактор, технічні збої або кіберзагрози.

Контроль за доступом і моніторинг — встановлення процедур та інструментів для контролю доступу до інформації, а також моніторинг використання систем для виявлення будь-яких аномалій або загроз.

Захист від шкідливих програм і вірусів — використання антивірусних програм і інших заходів для захисту від шкідливих програм.

Забезпечення безпеки інфраструктури — включає в себе захист серверів, баз даних, мережевих підключень та інших складових ІТ-інфраструктури.

Планування реагування на інциденти — розробка та впровадження плану на випадок інцидентів безпеки, таких як витік даних або атака на інформаційну систему.

Таким чином, безпека інформації на підприємстві — це комплексна задача, що вимагає системного підходу та уваги до різних аспектів, включаючи технологічні, організаційні та людські фактори.

Загрози безпеки інформації на підприємстві можуть бути дуже різноманітними і виходити як з внутрішніх, так і з зовнішніх джерел. Вони можуть мати різний рівень складності та серйозності, але всі вони можуть впливати на конфіденційність, цілісність і доступність інформації. Ось основні типи загроз:

1. Шкідливі програми (Malware)

- Віруси, черв'яки, трояни — ці програми можуть заразити інформаційні системи, змінювати або пошкоджувати дані, викрадати інформацію або спричиняти відмову в обслуговуванні.

- Шпигунські програми (Spyware) — призначені для стеження за користувачами, збору конфіденційних даних без їхнього відома.

2. Фізичний доступ до інформації

- Неавторизований доступ — наприклад, стороння особа може отримати фізичний доступ до комп'ютерів, серверів або іншої інформаційної інфраструктури компанії.

- Втрати або крадіжка пристроїв — крадіжка ноутбуків, смартфонів або USB-накопичувачів з важливою інформацією може призвести до витоку даних.

3. Кіберзагрози

- Фішинг (Phishing) — атакуючі намагаються обманом змусити користувачів розкрити конфіденційну інформацію, наприклад, логіни, паролі або банківські реквізити.

- DDoS-атаки (Distributed Denial of Service) — масовані атаки на сервери чи мережу підприємства з метою їх відключення, що призводить до недоступності послуг.

- SQL-ін'єкції — використання уразливостей у веб-додатках для втручання в бази даних та викрадення або зміни даних.

4. Внутрішні загрози

- Невірні або несанкціоновані дії співробітників — порушення політик безпеки, навмисні або ненавмисні дії, які можуть призвести до витоку даних, втрати інформації або серйозних помилок.

- Соціальна інженерія — маніпулювання співробітниками з метою отримання доступу до конфіденційної інформації чи систем.

5. Загрози на рівні мережі

- Прослуховування (Sniffing) — перехоплення даних, що передаються через мережу, наприклад, бездротові з'єднання чи незахищені канали.

- Атаки типу «Man-in-the-Middle» (MitM) — атаки, де зловмисник перехоплює та змінює комунікації між двома сторонами без їх відома.

6. Природні і техногенні катастрофи

- Пожежі, затоплення, землетруси — можуть пошкодити або знищити інформаційні системи та дані.

- Проблеми з електроживленням — короточасні або довготривалі відключення електроенергії можуть призвести до втрати даних або порушення роботи систем.

7. Загрози, пов'язані з обробкою та зберіганням даних

- Неналежне зберігання даних — відсутність належного захисту на носіях інформації може призвести до її втрати або крадіжки.

- Неправильне знищення даних — незнищення інформації належним чином може призвести до її витоку або відновлення (наприклад, за допомогою спеціалізованих інструментів).

8. Зовнішні загрози

- Атаки конкурентів — зловмисні дії з боку інших компаній або осіб, спрямовані на витягування конфіденційної інформації, що може використовуватися для конкуренції.

- Шахрайство та крадіжки — зловмисники можуть використовувати різні методи для викрадення грошей або даних підприємства.

9. Людський фактор

- Невміння або ігнорування політик безпеки — співробітники можуть не дотримуватись встановлених правил безпеки або навіть свідомо їх порушувати.

- Помилки користувачів — помилкові дії, такі як відкриття заражених файлів або натискання на фішингові посилання, можуть стати причиною серйозних проблем.

Ці загрози можуть мати різний вплив на діяльність підприємства, тому важливо запроваджувати заходи з управління ризиками та постійно вдосконалювати стратегії безпеки для запобігання їх реалізації.

1.2. Огляд існуючих стандартів безпеки інформації

Існує кілька міжнародних та національних стандартів і методологій, які допомагають підприємствам забезпечити безпеку інформації. Ці стандарти описують кращі практики, вимоги до організації безпеки та рекомендації з управління інформаційними ризиками. Ось основні з них:

1. ISO/IEC 27001:2013 — Міжнародний стандарт системи управління безпекою інформації (ISMS)

Один із найпоширеніших стандартів для управління безпекою інформації. Він встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління безпекою інформації на підприємстві.

Ключові аспекти:

Управління ризиками безпеки інформації.

Визначення та реалізація політик безпеки.

Розробка планів реагування на інциденти.

Постійний моніторинг і удосконалення системи.

Оцінка та аудит рівня безпеки.

Ціль: Зниження ризиків і забезпечення конфіденційності, цілісності та доступності інформації.

2. ISO/IEC 27002:2013 — Керівництво з практик безпеки інформації

Допоміжний стандарт, який містить детальні рекомендації з реалізації практик безпеки, викладених в ISO/IEC 27001. Він не є вимогливим, але дає чітке керівництво щодо заходів і політик, які можна впровадити для забезпечення безпеки.

Ключові аспекти:

Управління доступом.

Захист активів підприємства.

Оцінка ризиків та керування ними.

Управління інцидентами безпеки.

Впровадження політик безпеки.

3. NIST SP 800-53 — Рекомендації з безпеки інформаційних систем (Національний інститут стандартів і технологій США)

Набір рекомендацій, що застосовуються переважно в державних установах США, але також може бути використаний в приватних організаціях. Цей стандарт

визначає технічні та організаційні заходи для забезпечення безпеки інформаційних систем.

Ключові аспекти:

Рекомендації щодо управління доступом, захисту даних, реагування на інциденти та інші аспекти безпеки.

Категоризація рівнів безпеки залежно від важливості інформації.

Застосування контролів для мінімізації ризиків. [8]

4. PCI DSS — Стандарт безпеки даних платіжних карток (Payment Card Industry Data Security Standard)

Стандарт для захисту інформації, що стосується платіжних карток. Він встановлює вимоги щодо зберігання, обробки і передачі даних карток.

Ключові аспекти:

Захист даних карток.

Впровадження систем моніторингу безпеки.

Оцінка і контроль доступу до платіжної інформації.

Захист від несанкціонованих транзакцій та доступу.

5. COBIT 5 — Фреймворк для управління та управління ІТ (Control Objectives for Information and Related Technologies)

Методологія, що допомагає організаціям забезпечити ефективне управління ІТ-ресурсами та забезпечити безпеку інформації. COBIT надає інструменти для управління ризиками, аудиту та контролю ІТ-інфраструктури.

Ключові аспекти:

Управління ІТ-ризиками та відповідністю.

Забезпечення цілісності та доступності даних.

Оцінка та контроль систем ІТ-безпеки.

6. GDPR — Загальний регламент про захист даних (General Data Protection Regulation)

Європейський стандарт, який визначає правила обробки особистих даних осіб у межах Європейського Союзу (і для компаній, які взаємодіють з користувачами в ЄС). Хоча цей регламент не є стандартом безпеки інформації в класичному розумінні, він має суворі вимоги щодо захисту особистих даних.

Ключові аспекти:

Збір та обробка особистих даних тільки за згодою користувача.

Забезпечення прав користувачів щодо їхніх даних.

Визначення і усунення ризиків для особистих даних.

Звітність про порушення безпеки даних.

7. ITIL (IT Infrastructure Library) — Фреймворк для управління IT-послугами
Міжнародний стандарт для управління IT-послугами, який включає в себе компоненти для забезпечення безпеки інформації та управління ризиками в рамках IT-операцій.

Ключові аспекти:

Оцінка і управління ризиками в IT-середовищі.

Використання інструментів і процесів для забезпечення безпеки послуг.

Постійне вдосконалення процесів безпеки.

8. ISO/IEC 22301:2019 — Стандарт системи управління безперервністю бізнесу

Цей стандарт фокусується на забезпеченні безперервності бізнесу в разі різноманітних загроз, включаючи кіберзагрози та технічні проблеми.

Ключові аспекти:

Планування та підготовка до відновлення після інцидентів.

Управління ризиками та мінімізація наслідків для бізнесу.

Реалізація планів на випадок непередбачених ситуацій.

9. ISO/IEC 27018:2019 — Захист особистих даних в хмарних обчисленнях

Стандарт, що описує кращі практики щодо захисту персональних даних у середовищі хмарних обчислень.

Ключові аспекти:

Захист даних в хмарних сервісах.

Збереження конфіденційності персональних даних.

Виконання вимог щодо доступу та збереження інформації.

Ці стандарти допомагають підприємствам створити структуровану і ефективну систему безпеки інформації, що здатна знизити ризики і гарантувати захист даних. Вибір конкретного стандарту залежить від потреб підприємства, виду діяльності, галузі та юрисдикції, в якій воно функціонує.

1.3. Постановка задачі

Мета: Забезпечити захист інформаційних активів підприємства від різноманітних загроз, зокрема кіберзагроз, внутрішніх і зовнішніх атак, а також природних і техногенних катастроф.

Завдання:

Забезпечення конфіденційності, цілісності та доступності інформації.

Виявлення та усунення потенційних загроз і вразливостей інформаційних систем.

Створення системи управління ризиками, пов'язаними з інформацією.

Впровадження політик і процедур для моніторингу, контролю та реагування на інциденти безпеки.

Підготовка співробітників до правильного поводження з інформацією та системами безпеки.

Здійснення регулярного аудиту безпеки та оцінки ефективності вжитих заходів.

2. Ідентифікація інформаційних активів

Для формулювання конкретних заходів необхідно визначити:

Які дані і ресурси є найважливішими для підприємства (наприклад, клієнтські бази, фінансова інформація, технології, інтелектуальна власність).

Які системи, програми та інфраструктурні компоненти забезпечують обробку, зберігання та передачу цієї інформації.

3. Оцінка ризиків та загроз

Необхідно провести детальний аналіз ризиків, зокрема:

Визначення потенційних загроз (кібератаки, втрати даних, людський фактор, природні катастрофи).

Оцінка ймовірності виникнення цих загроз і потенційних наслідків.

Розробка матриці ризиків і вибір пріоритетних заходів для їх зменшення.

4. Розробка політики безпеки інформації

На основі оцінки ризиків та необхідних заходів розробляється політика безпеки, яка може включати:

Політика доступу до інформаційних систем: визначення, хто має доступ до яких ресурсів, на яких умовах.

Політика захисту даних: методи шифрування, резервне копіювання та зберігання даних.

Політика управління інцидентами: порядок дій у разі виявлення інцидентів безпеки.

Політика навчання співробітників: регулярні тренінги та інструктажі з питань безпеки.

5. Вибір і впровадження засобів захисту

Після формулювання політики безпеки необхідно визначити, які технології та інструменти будуть використані для її реалізації:

Технічні засоби захисту: системи виявлення вторгнень (IDS/IPS), антивірусні програми, брандмауери, системи резервного копіювання, шифрування даних.

Організаційні заходи: контроль доступу, моніторинг мережі та інформаційних систем, створення планів відновлення після інцидентів.

6. Моніторинг та аудит

Для забезпечення ефективності заходів безпеки необхідно:

Створити систему постійного моніторингу інформаційних систем для виявлення аномалій або порушень.

Проводити регулярні аудити безпеки для оцінки ефективності існуючих заходів.

Впровадити процеси для коригування і покращення системи захисту на основі результатів моніторингу та аудиту.

7. Планування реагування на інциденти та відновлення після катастроф

Важливо мати чіткий план дій на випадок інцидентів безпеки або технічних збоїв:

Розробка сценаріїв реагування на різні види інцидентів (фізичні катастрофи, кіберзагрози, людські помилки).

Наявність засобів для відновлення даних і відновлення нормальної роботи підприємства після інцидентів.

Проведення тренувань і тестування плану відновлення для підвищення готовності до надзвичайних ситуацій.

8. Навчання і підвищення обізнаності співробітників

Людський фактор є однією з основних загроз для інформаційної безпеки. Тому необхідно:

2. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Вразливості інформації

Вразливості інформації на підприємстві — це слабкі місця, які можуть бути використані зловмисниками або виникати внаслідок технічних чи організаційних недоліків і призводити до порушення конфіденційності, цілісності чи доступності інформації. Вразливості можуть мати різні форми і виникати на різних рівнях: технічному, організаційному, фізичному та людському. Ось основні типи вразливостей, з якими можуть стикатися підприємства:

1. Організаційні вразливості

Невизначеність політик безпеки: Відсутність чітких політик безпеки інформації або невиконання наявних може призвести до недотримання правил і процедур співробітниками.

Невиконання стандартів безпеки: Недотримання міжнародних стандартів безпеки (ISO/IEC 27001, GDPR тощо) підвищує ризики втрати або викрадення інформації.

Відсутність управління ризиками: Якщо не проводиться регулярна оцінка і управління ризиками для визначення ймовірності та наслідків загроз, підприємство може опинитися незахищеним від нових типів атак.

Невідповідність процесів безпеки вимогам законодавства: Відсутність чітких процедур щодо захисту персональних даних, дотримання вимог таких норм, як GDPR, може призвести до юридичних наслідків і порушення безпеки.

3. Фізичні вразливості

Незахищений доступ до інфраструктури: Відсутність фізичної охорони на об'єктах, де зберігаються важливі сервери, комп'ютери чи інші пристрої, може призвести до крадіжки або пошкодження інформації.

Крадіжка або втрата пристроїв: Крадіжка ноутбуків, мобільних телефонів, USB-накопичувачів, що містять важливу інформацію, є однією з основних фізичних загроз.

Ненадійне зберігання інформаційних носіїв: Невірно організоване зберігання носіїв даних, таких як жорсткі диски, може призвести до втрати або викрадення конфіденційної інформації.

4. Людські вразливості

Невміле поводження з інформацією: Співробітники можуть випадково передавати конфіденційну інформацію або використовувати ненадійні канали комунікації (наприклад, відкривати підозрілі електронні листи).

Інсайдерські загрози: Співробітники або підрядники, які мають доступ до важливої інформації, можуть використовувати свої повноваження для крадіжки або знищення даних.

Невміння реагувати на кіберзагрози: Недостатня підготовка співробітників щодо безпеки, а також не знання правил кібергігієни (як уникати фішингових атак, створювати складні паролі тощо), підвищує вразливість підприємства до кіберзагроз.

Соціальна інженерія: Використання маніпуляцій для того, щоб співробітники підприємства добровільно надали важливу інформацію або доступ до систем. Наприклад, через фішинг або підставні дзвінки.

5. Вразливості, пов'язані з управлінням доступом

Неналежний контроль доступу: Надання співробітникам доступу до інформаційних ресурсів, які не відповідають їхнім ролям або повноваженням.

Слабкі паролі: Використання легких для вгадування паролів або однакових паролів для різних систем може стати основною вразливістю, яку зловмисники можуть використати для несанкціонованого доступу.

Відсутність двофакторної аутентифікації: Неактивоване додаткове захист (як-от двофакторна аутентифікація) на важливих системах збільшує ризик зловмисного доступу.

6. Вразливості, пов'язані з обробкою та зберіганням даних

Неналежне шифрування: Відсутність шифрування даних, особливо при передачі або зберіганні важливої інформації, може призвести до витоку даних у разі несанкціонованого доступу.

Незадовільне знищення даних: Відсутність належних процедур для безпечного видалення або знищення старих даних може призвести до їх відновлення і використання.

7. Вразливості, пов'язані з поставками та партнерами

Незахищені зовнішні з'єднання: Підключення до сторонніх сервісів або постачальників без належної перевірки їх безпеки може створювати вразливості для підприємства.

Залежність від третіх осіб: Порушення безпеки в постачальників або партнерах може вплинути на безпеку підприємства через спільне використання інформаційних ресурсів.

1. Кіберзагрози (Загрози, пов'язані з комп'ютерними системами і мережами)

Атаки хакерів: Сюди відносяться зломи систем, втручання в роботу інформаційних систем через зовнішні джерела. Це можуть бути атаки через вразливості в програмному забезпеченні або мережах підприємства.

День нульової вразливості (Zero-day attack) — атаки, що використовують вразливості, які ще не були виявлені або не мають публічних виправлень.

Атаки типу «відмова в обслуговуванні» (DDoS) — перенавантаження серверів, що призводить до їх відмови або тимчасової недоступності.

Шкідливе програмне забезпечення (malware): Включає віруси, трояни, шифрувальне програмне забезпечення (ransomware), яке може пошкодити або

зашифрувати дані, викрасти конфіденційну інформацію, або зробити систему некоректною.

Віруси — програми, що поширюються між комп'ютерами і змінюють їх функціональність.

Трояни — програми, що маскуються під корисне програмне забезпечення, але в реальності виконують зловмисні дії.

Шифрувальники (ransomware) — програми, які шифрують дані підприємства та вимагають викуп для їх розшифрування.

Фішинг: Способи обману користувачів з метою отримання конфіденційної інформації (наприклад, логінів і паролів) через підроблені електронні листи або вебсайти.

Соціальна інженерія: Використання маніпуляцій для отримання доступу до систем або даних, через маніпулювання людьми (наприклад, обман співробітників підприємства для отримання паролів). [39]

2. Внутрішні загрози

Загрози з боку працівників: Працівники підприємства можуть навмисно або через неуважність спричиняти шкоду інформації. Це можуть бути:

Інсайдерські атаки — зловживання правами доступу до інформації для викрадення або пошкодження даних.

Помилки користувачів — випадкове або необережне поводження з інформацією, наприклад, випадкове видалення важливих файлів або відкриття шкідливих електронних листів.

Невідповідність політикам безпеки: Якщо працівники не дотримуються політик безпеки або не усвідомлюють важливість безпеки даних, це може створити вразливості та можливості для порушень.

Неавторизований доступ: Використання співробітниками слабких паролів або спільне використання облікових записів може привести до несанкціонованого доступу до важливої інформації.

3. Загрози, пов'язані з фізичним доступом

Фізична крадіжка або пошкодження обладнання: Крадіжка серверів, ноутбуків, мобільних пристроїв або зовнішніх носіїв, на яких зберігаються конфіденційні дані.

Невірно організоване зберігання інформації: Якщо інформація зберігається без належного фізичного захисту (наприклад, на непідключених до мережі носіях, у відкритих місцях), це може призвести до її втрати або викрадення.

Втрата носіїв інформації: Невірно організоване зберігання переносних пристроїв (USB-накопичувачів, жорстких дисків) може призвести до втрати інформації.

4. Загрози, пов'язані з управлінням даними

Втрати даних через несправності обладнання: Пошкодження жорстких дисків, серверів або інші технічні проблеми можуть призвести до втрати важливої інформації.

Невиконання процедур резервного копіювання: Якщо на підприємстві не реалізовано надійне резервне копіювання даних, то це створює ризик втрати інформації в разі інцидентів (наприклад, при кібератаках або аваріях).

Ненадійне зберігання даних: Дані можуть бути скомпрометовані або втрачені, якщо не застосовуються належні методи шифрування та захисту інформації.

5. Природні загрози

Природні катастрофи: Повені, землетруси, пожежі та інші природні катастрофи можуть знищити обладнання або пошкодити інформаційні системи, а також привести до втрати даних.

Відключення енергопостачання: Перебої з електроенергією можуть спричинити пошкодження серверів, зниження продуктивності або навіть втрату даних, якщо відсутнє належне джерело безперебійного живлення.

6. Загрози, пов'язані з партнерськими відносинами

Ненадійні постачальники та підрядники: Спільне використання інформації з партнерами може створити додаткові ризики, якщо ці партнери не мають належного рівня безпеки інформації. Атаки через слабкі ланки у ланцюзі постачання можуть призвести до витоку або втрати даних.

Недостатній контроль за доступом партнера до внутрішніх систем: Невідповідність стандартам безпеки у партнерів може збільшити ризики проникнення до інформаційних систем підприємства. [28]

7. Юридичні загрози

Недотримання законодавства: Порушення законів щодо захисту персональних даних, таких як GDPR в Європейському Союзі, може призвести до значних штрафів і юридичних наслідків для підприємства.

Невиконання контрактних зобов'язань з безпеки: Якщо підприємство не виконує обов'язки щодо безпеки інформації, встановлені у контрактах з партнерами або клієнтами, це може призвести до юридичних позовів та репутаційних втрат.

Основні наслідки загроз для підприємства:

Фінансові втрати — через штрафи, компенсації клієнтам, відновлення пошкоджених систем, втрату бізнесу.

Втрати репутації — порушення довіри клієнтів, партнерів та інших зацікавлених осіб.

Втрати даних — втрата важливої, конфіденційної інформації, яка може бути критичною для бізнесу.

Перерви в роботі — зупинка виробництва, збої в наданні послуг або втрата доступу до систем підприємства.

Юридичні наслідки — штрафи та санкції за порушення законодавства з захисту інформації.

Забезпечення інформаційної безпеки є важливою складовою для підприємств будь-якого масштабу, і розуміння загроз є основою для розробки заходів захисту та зменшення ризиків. [14]

2.2. Протоколи захисту інформації

Протоколи захисту інформації на підприємстві — це набір стандартів, принципів, процедур та технічних засобів, що використовуються для забезпечення безпеки інформаційних ресурсів підприємства. Вони визначають, як організувати доступ до інформації, як забезпечити її конфіденційність, цілісність та доступність, а також як реагувати на загрози та інциденти безпеки.

Ось основні протоколи захисту інформації на підприємстві:

1. Протоколи шифрування

Шифрування є одним із основних способів захисту інформації. За допомогою шифрування дані перетворюються в незрозумілий для сторонніх осіб формат, що забезпечує їх конфіденційність.

SSL/TLS (Secure Sockets Layer / Transport Layer Security): Протоколи, які використовуються для захисту передавання даних через інтернет. Вони шифрують з'єднання між клієнтом та сервером (наприклад, під час здійснення покупок в інтернет-магазині або під час авторизації на вебсайтах).

IPsec (Internet Protocol Security): Протокол для шифрування даних на рівні мережі, що забезпечує захищене передавання даних через IP-мережі (наприклад, віртуальні приватні мережі — VPN).

AES (Advanced Encryption Standard): Один із найпоширеніших алгоритмів симетричного шифрування для захисту файлів, баз даних, а також для передачі чутливої інформації.

RSA: Алгоритм асиметричного шифрування, що використовується для захисту передавання ключів шифрування або для електронного підпису. [19]

2. Протоколи автентифікації та авторизації

Ці протоколи забезпечують перевірку особи користувача та контроль доступу до систем і даних.

LDAP (Lightweight Directory Access Protocol): Протокол, що дозволяє здійснювати доступ до служб каталогів (наприклад, для управління обліковими записами користувачів).

Kerberos: Протокол автентифікації, що дозволяє безпечно здійснювати перевірку користувачів у комп'ютерних мережах, зокрема в операційних системах Microsoft Windows.

OAuth: Стандарт автентифікації, який дозволяє третім сторонам отримувати обмежений доступ до облікових записів користувачів без надання їм паролів (наприклад, для доступу до API).

SAML (Security Assertion Markup Language): Протокол, що дозволяє здійснювати одноразову автентифікацію (Single Sign-On — SSO) між різними системами.

3. Протоколи безпеки при передачі даних

Протоколи, які забезпечують безпечну передачу даних через мережі.

HTTPS (HyperText Transfer Protocol Secure): Розширення HTTP, яке забезпечує захищене передавання даних між клієнтом та сервером за допомогою SSL/TLS шифрування. Це забезпечує захист конфіденційної інформації, такої як логіни та паролі.

FTPS/SFTP (FTP Secure / Secure File Transfer Protocol): Протоколи для безпечної передачі файлів через мережу, які використовують шифрування для захисту даних під час їх передавання.

SSH (Secure Shell): Протокол для безпечного доступу до віддалених серверів та комп'ютерів через мережу. Використовується для командного рядка та для безпечної передачі файлів.

4. Протоколи для моніторингу та виявлення інцидентів

Ці протоколи використовуються для виявлення та реагування на інциденти безпеки в реальному часі.

SIEM (Security Information and Event Management): Протоколи та програмні засоби для збору, кореляції та аналізу логів безпеки з різних джерел (наприклад, сервери, мережеві пристрої, брандмауери), щоб виявити аномалії або загрози в мережі підприємства.

IDS/IPS (Intrusion Detection System / Intrusion Prevention System): Протоколи для виявлення та запобігання несанкціонованим вторгненням в інформаційні системи підприємства.

5. Протоколи для захисту від атак

Протоколи, що допомагають захистити системи та мережі підприємства від атак.

WPA2/WPA3 (Wi-Fi Protected Access): Протоколи для захисту бездротових мереж, що використовуються для шифрування трафіку та забезпечення безпеки на рівні Wi-Fi.

DDoS Protection Protocols: Протоколи та інструменти для захисту від атак типу «відмова в обслуговуванні» (DDoS). Вони можуть включати спеціалізовані брандмауери, проксі-сервери або сервери для фільтрації трафіку. [6]

6. Протоколи для резервного копіювання та відновлення

Протоколи для забезпечення відновлення інформації у разі її втрати або пошкодження.

Rsync: Протокол і утиліта для синхронізації файлів і резервного копіювання даних між комп'ютерами або серверами.

Cloud Backup Protocols: Протоколи для резервного копіювання даних у хмарні сервіси, що використовують шифрування і аутентифікацію для забезпечення безпеки інформації в процесі її зберігання в хмарі.

7. Протоколи для захисту кінцевих точок (endpoint security)

Протоколи для захисту пристроїв, які підключені до мережі підприємства (ноутбуки, мобільні пристрої, сервери).

Endpoint Detection and Response (EDR): Технології та протоколи, що використовуються для виявлення та реагування на загрози на кінцевих точках, таких як комп'ютери та мобільні пристрої.

Mobile Device Management (MDM): Протоколи і системи для управління мобільними пристроями співробітників, що включають налаштування безпеки, шифрування даних і віддалене блокування пристроїв у разі втрати.

8. Протоколи для управління доступом

Протоколи, які визначають, як забезпечити правильний доступ до інформаційних систем підприємства.

RBAC (Role-Based Access Control): Протокол, який визначає доступ до ресурсів на основі ролі користувача. Кожному користувачу надаються права доступу, що відповідають його професійним обов'язкам.

ABAC (Attribute-Based Access Control): Протокол, що забезпечує доступ до ресурсів на основі атрибутів користувача (наприклад, локація, час доступу, інші параметри).

MFA (Multi-Factor Authentication): Протокол, який вимагає підтвердження особи користувача за допомогою кількох факторів (наприклад, пароль і код з мобільного додатку).

9. Протоколи для захисту конфіденційності даних

Ці протоколи сприяють захисту особистої інформації і даних клієнтів.

GDPR (General Data Protection Regulation): Європейський протокол для захисту персональних даних користувачів. Підприємства повинні забезпечити конфіденційність даних та їх захист, а також мати механізми для управління доступом і видаленням персональної інформації.

HIPAA (Health Insurance Portability and Accountability Act): Протокол захисту конфіденційної інформації в галузі охорони здоров'я в США. Він регулює використання медичних даних і передбачає строгі вимоги до безпеки.

Протоколи захисту інформації на підприємстві є критично важливими для забезпечення конфіденційності, цілісності та доступності даних. Вони допомагають мінімізувати ризики від кіберзагроз, внутрішніх інцидентів і природних катастроф. Вибір і впровадження протоколів залежить від специфіки діяльності підприємства та вимог до безпеки. [22]

2.3. Моделі захисту інформації

Дослідники по всьому світу розробляють різні захисні методики для виявлення шкідливого трафіку та захисту від DDoS-атак.

Elastic Cloud Security System ECS2 надає складну захисну систему від шкідливого трафіку. ECS2 має антибот-таблиці та антивірусні рішення, вбудовані в систему захисту. Також у системі встановлені міжмережні екрани, що працюють у режимі реального часу. Мінусом використання такого підходу є час оновлення репутаційних таблиць та сигнатур вірусів. Несвоєчасне оновлення таблиць може призвести до пропуску шкідливого трафіку, що генерується з непомічених IP-

адрес. Тому мій підхід не базується на сигнатурах, списках шкідливих IP-адрес та інших методів, дані для яких необхідно постійно оновлювати.

У статті пропонується захисний метод, який використовує ресурси для виявлення шкідливого трафіку віртуальних машин. Метод був протестований на 108 сервісах, запущених різних віртуальних машинах. Методи у статті засновані на технології інтелектуального аналізу даних та запускаються як додатки на віртуальних машинах.

Мінусом цього рішення є розташування процесів захисту за клієнта. Багато клієнтів не хочуть бачити на своїх віртуальних машинах фонові сторонні процеси. Це не відповідає політикам безпеки багатьох компаній.

Стаття представляє новий метод виявлення аномалій у трафіку, що використовує аналіз потоків, заснований на алгоритмі K-mean. Навчання даних, що містять непідписані записи потоків, ділиться на кластери легітимного та шкідливого трафіку. Відповідні центроїди кластерів використовуються як патерни для ефективного виявлення аномалій в аналізованому потоці трафіку. Автори вказують, що застосування алгоритму окремо для різних сервісів (що використовують різні протоколи та номери портів) збільшує точність виявлення.

Автори пропонують алгоритм виявлення DDoS-атак, який використовує SSL/TLS протокол. Алгоритм заснований на фільтрації шуму даних і кластеризації для виявлення шкідливого трафіку. Моделі були навчені на даних, отриманих з реалістичного комп'ютерного середовища. Автори роблять висновок, що запропонована модель дозволяє виявляти всі шкідливі потоки з дуже малою кількістю помилкових спрацьовувань.

Використання методів детектування DDoS-атак на основі машинного навчання є досить популярним завданням серед дослідників. Один з методів детектування, описаний у роботі Keisuke Kato, з використанням алгоритму машинного навчання support vector Keisuke Kato машина з радіальним основним

функцією техніка з радіальним основним функцією (Gaussian) kernel на dataset from UCLA. Проте у роботі не розглядається можливість динамічної зміни трафіку.

У роботі Wafa Slaibi Alsharafat розглядається метод детектування на основі генерації класифікаторів з використанням генетичного алгоритму з набором даних KDD'99.

У роботі Bing Wang досліджуються особливості детектування

DDoS-атак у хмарних середовищах, де трафік відрізняється від звичайних мереж та існує можливість підвищення помилок першого та другого роду. Окрім виконання детектування атак у методі виконується перевірка на рівень упевненості моделі класифікації. При низькому рівні трафік відправляється на модуль глибокого аналізу, де виконується точніша перевірка. Якщо модуль визначить трафік як шкідливий, модель класифікації оновлюється з використанням отриманих даних про трафік. Цей підхід розглядає доповнення моделі новими сигнатурами атак. Зміна трафіку також може впливати на точність класифікації легітимних користувачів. Надання доступу легітимним користувачам часто є більш важливим завданням, внаслідок чого бажано зменшувати помилки другого роду.

2.3.1 Моделі, засновані на правилах та сигнатурах

Широко поширені системи, які використовують підписи для пошуку аномалій у трафіку. В принципі, такі системи безпеки аналізують поведінку атакуючого більш менш лінійно, порівнюючи потік трафіку зі зразками потоку, відомими як smurf, SYN або інші відомі типи атак. Такі рішення ефективні проти зловмисників, які використовують поширене програмне забезпечення та стандартні сценарії атаки, але вони не справлятимуться з будь-якими трюками, які

може зробити зловмисник. Крім того, у разі виявлення джерела шкідливого трафіку, система повністю заблокує його, хоча він може бути законним клієнтом, зараженим вірусом. У випадку OVS блокування внутрішньої віртуальної машини всього клієнта може викликати великі проблеми для клієнта, а потім для постачальника хмарних послуг, оскільки основною метою використання хмарних обчислювальних середовищ є наявність ресурсів та служб 24/7/365.

Виявлення за сигнатурами та правилами засноване на створенні наборів правил, що застосовуються до трафіку для виявлення шкідливої активності. Такі правила можуть бути написані на основі відомих фактів, таких як IP-адреси, зміст корисного навантаження трафіку, URL. Існує безліч доступних наборів правил і більшість програмного забезпечення поставляється з деякими стандартними правилами, але щоб протистояти новим загрозам, вони повинні регулярно оновлюватися.

2.3.2 Моделі, що ґрунтуються на аномаліях

Моделі, що ґрунтуються на аномаліях – це спосіб виявити незвичайну поведінку трафіку всередині мережі. Здатність IDS виявляти незвичайний трафік полягає в вимірах, попередніх розгортанні IDS. Ці тестові чи навчальні набори даних використовуються для імітації трафіку, який вважається легітимним у мережному оточенні. Ці виміри є основою уявлень у тому, як має виглядати «нормальний» трафік. Якщо трафік відхиляється від «нормального», система повідомляє про це відхилення. Навчальні набори даних також використовуються для імітації шкідливого трафіку, щоб система могла розпізнати шаблони відомих загроз і атак.

Це досить просто виконати для систем, у яких поведінка може бути визначена за допомогою простих математичних моделей, наприклад, систем, що характеризуються відомим середнім та стандартним відхиленням.

Для отримання характеристик із даних таких складних систем використовуються методи машинного навчання та інші методи інтелектуального аналізу даних. Також важливою особливістю завдань виявлення нетипової поведінки системи та виявлення аномалій є відсутність формального визначення аномалії. Зазвичай це поняття формалізуються під час досліджень залежно від обраного методу.

2.3.3 Модель із використанням методів машинного навчання

Наступний механізм захисту використовує машинне навчання. Він у автоматичному режимі виявляє аномалії трафіку та знаходить шкідливий трафік за допомогою навчених моделей.

Методи знаходження нетипової поведінки, аномалій, що базуються на моделях «нормальної» поведінки користувачів, обчислювальних вузлів, мереж, виявляють атаки як значне відхилення від цих моделей. Цей підхід автоматично виявляє аномалії трафіку та виявляє шкідливий трафік з використанням навчених моделей. Якщо виявлено аномалію, проводяться подальші дослідження трафіку. Якщо якась із характеристик потоків трафіку перевищує значення, отримане моделлю під час навчання, цей потік буде відкинутий. Перевагою цього є нелінійний аналіз трафіку, який дозволяє точно визначити право власності на трафік на зловмисне, і навіть здатність системи розпізнавати раніше невідомі атаки. Також ці системи можуть виявляти дії зловмисника, які важко описати сигнатурами. Підходи з використанням методів машинного навчання до проблеми виявлення вторгнень можна поділити на 2 класи:

- 1) виявлення неправильного використання (Misuse detection) - побудова прогностичної моделі на основі розмічених даних (Примірники позначені як «нормальні»): демонструють високу точність виявлення великої кількості відомих атак; не можуть виявити невідомі та нові атаки;

2) виявлення аномалій: система може виявляти нові атаки як відхилення від «нормальної» поведінки; можливий високий рівень помилкових «спрацьовувань», оскільки виявлене відхилення який завжди є реальне вторгнення.

Складність підходу полягає у процесі машинного навчання. Необхідно правильно виконати всі етапи машинного навчання задля досягнення ефективного захисту. Наведено аналіз традиційних підходів до вирішення завдань виявлення вторгнень у комп'ютерну систему та їх недоліки, зокрема, їх нездатність розпізнавати нові типи атак. У більшості випадків системи виявлення вторгнень шукають сигнатури або порушення трафіку на основі сформульованих правил або проведених вимірювань. Ці виміри припускають, що в мережі знаходиться легітимний трафік і якщо трафік не розпізнається як легітимний, система сповіщає про це. Ці порушення часто називаються шкідливим або підозрілим трафіком, але цей трафік може бути легітимним. Якщо система виявлення вторгнень налаштована блокувати трафік, вона стає системою запобігання вторгнень. Система запобігання працює майже так само, як і система виявлення, але замість повідомлення про підозрілий трафік вона блокує і відкидає трафік, позначаючи його як шкідливий.

Усі алгоритми виявлення аномалій створюють модель нормального паттерна даних, нормальної поведінки системи, а потім обчислюють «ступінь аномальності» певної точки даних (набору точок) з урахуванням відхилення від цього паттерна. Наприклад, модель даних може бути статистичної регресійної моделі або моделі близькості. Ці моделі мають різне тлумачення «нормальної поведінки» даних. Ступінь аномальності досліджуваної (нової) точки даних оцінюють обчисленням подібності точки даних та моделі. У деяких випадках модель може бути задана алгоритмічно. Наприклад, алгоритм виявлення викидів на основі методу найближчих сусідів моделює дані в термінах розподілу відстані

між k -сусідами. У цьому випадку викиди знаходяться на великій відстані від більшості даних.

Вибір моделі даних є важливим завданням. Некоректно обрана модель даних може бути причиною незадовільних результатів алгоритму. Наприклад, модель лінійної регресії може давати результати низької якості, якщо дані, на яких побудована ця модель, кластеризовані випадковим чином. Завданням класифікації в машинному навчанні є завдання присвоєння невідомого об'єкта одному з наперед визначених класів на основі його формалізованих характеристик. Кожен з об'єктів цього завдання представляється як вектора значень у просторі розмірності N , причому кожен розмір є опис однієї ознаки об'єкта.

Для класифікації кожного об'єкта тестової вибірки необхідно послідовно виконати такі операції:

1. Обчислити евклідову відстань до кожного з об'єктів навчальної вибірки.
2. Відібрати k об'єктів навчальної вибірки з мінімальною відстанню до об'єкта, що класифікується.
3. Клас класифікованого об'єкта – це клас, якого належить більшість з k найближчих сусідів.

Аналіз аномалій у сценаріях, у яких є попередні приклади нетипового поведінки, називають виявлення аномалій на розмічених даних чи виявлення аномалій з учителем. Мітки аномальних ділянок попередніх даних використовують для навчання моделей виявляти аномалії певного типу.

Аналіз аномалій на розмічених даних є специфічним (складнішим) випадком завдання класифікації. Характерною рисою є значна незбалансованість наявності міток нормальної та аномальної поведінки. Нормальні дані зазвичай легко зібрати і тому вони є в наборі даних у великій кількості. З іншого боку, випадки аномалій, викидів дуже розріджені. У класичних роботах по машинному навчанню ця проблема відома як виявлення класів з низькою частотністю (Rare Class Detection).

Дисбаланс міток (позитивно-негативних, нормальних – аномальних) часто призводить до проблеми перенавчання (over-training, overfitting). Крім того, відомо кілька варіацій проблем класифікації відповідно до рівня повноти розмітки:

1. Обмежена кількість позитивних прикладів, тоді як «Нормальні» приклади можуть містити деяку невідому пропорцію аномалій. Цей випадок відомий як класифікація на позитивно-нерозмічених даних (Positive-Unlabeled Classification). У тому випадку, коли нерозмічена навчальна вибірка не повною мірою відображає тестову вибірку, доцільно відкинути з навчальної вибірки нерозмічені дані та розглядати це завдання як проблему класифікації одного класу (oneclass problem).

2. У навчальній вибірці є лише деякі види аномалій, які можуть зустрітись в тестовій вибірці. Наприклад, у вибірці, на якій навчається модель виявлення вторгнень у комп'ютерну мережу, є аномалії у вигляді певного роду атак. Однак у робочому режимі система повинна реагувати і на нові види атак, які раніше не зустрічалися.

Метод опорних векторів (Support Vector Machine, SVM) є одним із найпотужніших методів машинного навчання. Хоча він розроблявся в основному для завдань класифікації, його модифікації успішно використовуються у задачах виявлення аномалій.

Метод опорних векторів дискримінаційного класифікатора: він «проводить» межу між кластерами даних.

3. ПРОЕКТУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІДПРИЄМСТВА НА БАЗІ МОДЕЛЕЙ БЕЗПЕКИ

3.1. Підбір та обґрунтування методів захисту інформації

Підбір та обґрунтування методів захисту інформації на підприємстві — це важливий етап у забезпеченні інформаційної безпеки. Вибір методів залежить від специфіки діяльності підприємства, типу інформації, яку обробляють, рівня загроз, а також ресурсів, доступних для реалізації цих методів. Розглянемо основні методи захисту та обґрунтування їх вибору.

1. Шифрування даних

Метод: Використання криптографії для захисту конфіденційності та цілісності даних. Шифрування є основним методом для захисту інформації при її зберіганні (на дисках, у базах даних) та передачі (через мережі).

Шифрування забезпечує захист даних від несанкціонованого доступу як при зберіганні, так і при передаванні через мережу.

Для захисту важливої або конфіденційної інформації (наприклад, фінансових даних, персональних даних клієнтів) шифрування є обов'язковим, особливо в умовах сучасних загроз (хакерських атак, перехоплення даних).

AES або RSA (для асиметричного шифрування) є найбільш поширеними та надійними методами шифрування для корпоративних даних.

2. Автентифікація та авторизація

Метод: Використання різних механізмів для підтвердження особи користувача та визначення рівня доступу до інформаційних систем.

Для зменшення ризику несанкціонованого доступу до систем підприємства необхідно впроваджувати багатофакторну автентифікацію (MFA), яка перевіряє особу користувача за кількома ознаками (пароль, код з мобільного додатку, біометричні дані).

Встановлення ролевого доступу (RBAC) або атрибутивного доступу (ABAC) дозволяє чітко визначити, які права має кожен користувач в залежності від його ролі або атрибутів, що обмежує можливості для зловживань.

Це забезпечує високий рівень контролю та безпеки, знижує ймовірність внутрішніх загроз та покращує загальний захист інформаційних систем.

3. Інтегровані системи моніторингу та реагування (SIEM)

Метод: Використання систем для моніторингу інформаційної безпеки, виявлення аномалій та реагування на інциденти.

SIEM системи дозволяють збирати логи з різних джерел (сервери, мережеві пристрої, додатки) і здійснювати їх аналіз для виявлення потенційних загроз, таких як спроби несанкціонованого доступу, вторгнень або шкідливого програмного забезпечення.

Вони надають можливість своєчасно реагувати на інциденти безпеки і мінімізувати наслідки, що дозволяє знизити ризики для підприємства від зовнішніх та внутрішніх атак.

Цей метод особливо важливий для підприємств, що працюють з великими обсягами чутливої інформації або мають високу критичність для безперервності бізнес-процесів.

4. Антивірусне та антивандальне програмне забезпечення

Метод: Використання антивірусних програм для захисту від шкідливого програмного забезпечення, вірусів, троянів, шпигунських програм тощо.

Антивірусне ПЗ є необхідним елементом базового рівня захисту для всіх кінцевих пристроїв (персональних комп'ютерів, мобільних пристроїв, серверів).

Ці програми допомагають виявляти, блокувати та видаляти шкідливі програми до того, як вони зможуть пошкодити інформацію або систему.

Неперервне оновлення баз сигнатур антивірусного ПЗ гарантує актуальність захисту від нових загроз.

5. Фізичний захист інформаційних ресурсів

Метод: Захист серверів, комп'ютерних систем, робочих місць, носіїв даних від фізичних загроз.

Фізичний захист включає обмеження доступу до серверних приміщень, установку відеоспостереження, контролю доступу (картки доступу, біометрія).

Це дозволяє запобігти несанкціонованому доступу до серверів і баз даних, викраденню носіїв інформації (наприклад, флеш-накопичувачів, жорстких дисків).

У випадку критичних даних (наприклад, фінансових документів або персональної інформації клієнтів) фізичний захист є необхідним доповненням до програмних методів безпеки.

6. Резервне копіювання та відновлення даних

Метод: Забезпечення регулярного резервного копіювання всіх важливих даних та розробка плану відновлення після аварій.

Резервне копіювання дає змогу відновити дані у разі їх втрати або пошкодження (наприклад, при атаках типу ransomware або технічних збоїв).

Важливо, щоб копії зберігались в безпечному місці (наприклад, у хмарному середовищі або на зашифрованих носіях).

Окрім цього, слід періодично тестувати відновлення даних, щоб впевнитися в ефективності процесу.

7. Підвищення обізнаності співробітників

Метод: Навчання співробітників основам інформаційної безпеки, інструктажі щодо запобігання фішингу, використання паролів і т.д.

Найбільша кількість інформаційних інцидентів відбувається через людські помилки або незнання. Наприклад, співробітники можуть випадково

завантажити шкідливе програмне забезпечення або відкрити підроблений електронний лист.

Постійне навчання співробітників та проведення тестів на знання політики безпеки знижує ймовірність виникнення подібних інцидентів.

Системи навчання та підвищення обізнаності є ефективним способом зменшення ризику від внутрішніх загроз.

8. Моніторинг та оцінка вразливостей

Метод: Регулярне тестування та оцінка вразливостей систем за допомогою спеціальних інструментів.

Підприємство повинно регулярно перевіряти свої інформаційні системи на наявність вразливостей, щоб вчасно виявити потенційні загрози до того, як зловмисники скористаються ними.

Для цього використовуються інструменти для сканування вразливостей (наприклад, Nessus, OpenVAS) і тестування на проникнення (penetration testing).

Регулярний моніторинг допомагає виявляти слабкі місця та своєчасно впроваджувати заходи для їх усунення.

Підбір методів захисту інформації має базуватися на системному підході, що враховує специфіку діяльності підприємства, типи даних, рівень загроз і доступні ресурси. Комбінація технологічних, організаційних і людських заходів забезпечує надійний захист від різноманітних загроз, а також дозволяє швидко реагувати на інциденти безпеки, зменшуючи ризики для бізнесу.

3.2. Підбір та обґрунтування інструментів захисту інформації

Вибір інструментів залежить від різних факторів, таких як тип інформації, що обробляється, рівень загроз, бюджет підприємства, масштаби діяльності та специфіка галузі. Ось основні категорії інструментів захисту інформації та їх обґрунтування.

1. Інструменти для шифрування даних

AES (Advanced Encryption Standard) — алгоритм симетричного шифрування для захисту даних.

RSA — алгоритм асиметричного шифрування для захисту даних при їх передачі.

BitLocker (для Windows) та FileVault (для MacOS) — інструменти для шифрування дисків, що зберігають конфіденційну інформацію.

OpenSSL — набір інструментів для криптографії, що дозволяє виконувати операції шифрування та дешифрування.

Шифрування даних є одним з основних методів захисту конфіденційності. Воно гарантує, що навіть у разі доступу до носіїв або перехоплення даних зломисниками, ті не зможуть отримати доступ до змісту інформації без наявності ключа дешифрування.

Використання таких інструментів важливе для зберігання та передачі чутливих даних (персональна інформація клієнтів, фінансові дані тощо).

2. Інструменти для управління доступом та автентифікацією

Active Directory (AD) — система для централізованого управління користувачами і доступом до корпоративних ресурсів.

Okta, Auth0, Microsoft Azure Active Directory — інструменти для управління ідентифікацією та доступом (Identity and Access Management — IAM).

Duo Security, Google Authenticator — рішення для багатофакторної автентифікації (MFA).

Інструменти управління доступом дозволяють визначити рівень доступу користувачів до різних інформаційних систем залежно від їх ролей у організації, що допомагає запобігти несанкціонованому доступу до ресурсів.

Многофакторна автентифікація (MFA) додає додатковий рівень захисту, мінімізуючи ризик компрометації облікових записів через викрадення паролів.

Для підприємств з високими вимогами до безпеки (наприклад, в фінансовому секторі) ці інструменти є обов'язковими для зниження ризику внутрішніх і зовнішніх загроз.

3. Антивірусні та антималварні інструменти

McAfee, Bitdefender — рішення для захисту від вірусів, троянів, шпигунського ПЗ і інших шкідливих програм.

CrowdStrike, Carbon Black — системи для виявлення та попередження вторгнень (EDR — Endpoint Detection and Response).

Malwarebytes — інструмент для виявлення і видалення шкідливих програм.

Антивірусне програмне забезпечення захищає кінцеві пристрої від широкого спектра шкідливих програм, таких як віруси, трояни, шпигунські програми, що можуть бути використані для викрадення або пошкодження даних.

Інструменти для виявлення та реагування на загрози (EDR) дозволяють моніторити діяльність на кінцевих точках (комп'ютери, сервери) і вчасно виявляти підозрілі активності, що можуть свідчити про атаку.

4. Системи моніторингу безпеки та управління подіями (SIEM)

Інструменти:

Splunk, IBM QRadar, ArcSight — інструменти для збору, кореляції та аналізу логів безпеки.

ELK Stack (Elasticsearch, Logstash, Kibana) — система збору і візуалізації даних для моніторингу та аналізу безпеки.

SIEM-системи дозволяють підприємствам отримувати цілісну картину про стан безпеки у реальному часі, аналізувати логи та виявляти аномалії, що можуть вказувати на спроби вторгнення або інші інциденти безпеки.

Вони дають змогу швидко реагувати на інциденти, автоматизувати процеси моніторингу та виявлення загроз, що особливо важливо для великих організацій з високим рівнем ризиків.

5. Інструменти резервного копіювання та відновлення даних

Veeam, Acronis, Commvault — рішення для резервного копіювання та відновлення даних.

Регулярне резервне копіювання даних є критичним для забезпечення відновлення інформації в разі її втрати або пошкодження (через атаки, технічні збої або природні катастрофи).

Використання хмарних рішень для резервного копіювання дозволяє забезпечити високу доступність та гнучкість, зберігаючи резервні копії в географічно віддалених місцях, що знижує ризик втрати даних через локальні інциденти.

6. Інструменти для захисту мережі та периметра

Firewall (брандмауери) — апаратні та програмні рішення для контролю доступу до мережі.

Cisco ASA, Palo Alto, Fortinet — брандмауери нового покоління (NGFW), які інтегрують функції аналізу трафіку, виявлення загроз і блокування шкідливих запитів.

VPN (Virtual Private Network) — для захисту трафіку при віддаленому доступі до корпоративних мереж.

OpenVPN, Cisco AnyConnect — інструменти для забезпечення захищеного з'єднання при віддаленому доступі.

Брандмауери дозволяють контролювати трафік між внутрішньою мережею підприємства та зовнішнім світом, блокуючи шкідливі запити та атаки.

Віртуальні приватні мережі (VPN) забезпечують захист даних під час передачі через незахищені мережі (наприклад, інтернет), що є критично важливим

для співробітників, які працюють віддалено або при використанні незахищених публічних мереж.

7. Інструменти для тестування безпеки та виявлення вразливостей

Nessus, OpenVAS — інструменти для сканування вразливостей.

Metasploit — платформа для тестування на проникнення.

Виявлення вразливостей та тестування систем на проникнення дозволяють виявити потенційні слабкі місця в інфраструктурі до того, як зловмисники їх використовують.

Регулярне тестування безпеки є важливою частиною стратегії з управління ризиками та забезпечення захисту від нових і розвиваючихся загроз.

8. Інструменти для управління політиками безпеки та конфігураціями

Puppet, Ansible, Chef — інструменти для автоматизації управління конфігураціями.

CIS-CAT — інструмент для оцінки відповідності до стандартів безпеки.

Автоматизація управління конфігураціями дозволяє забезпечити стабільність і відповідність систем до політик безпеки без людських помилок.

Це допомагає запобігти неправильному налаштуванню, яке може призвести до вразливостей або порушення стандартів безпеки.

Підбір інструментів захисту інформації на підприємстві має бути ґрунтовним і стратегічним. Вибір інструментів залежить від специфіки бізнесу, рівня загроз та технічних вимог до безпеки. Важливо враховувати інструменти для забезпечення конфіденційності, доступності та цілісності даних, а також для моніторингу безпеки, реагування на інциденти та управління доступом. Комбінація цих інструментів дозволить створити ефективну систему захисту інформації на підприємстві.

Обґрунтування та вибір прототипу SIEM системи

Далі розглянемо деякі SIEM системи, як приклад Security Capsule, HP ArcSight, MaxPatrol SIEM.

HP ArcSight

Даний продукт забезпечує збір, зберігання і обробку подій інформаційної безпеки, які можуть надходити з різних засобів захисту.

Основою продуктової лінійки ArcSight є комплекс HP ArcSight Security Intelligence, ядром в якому служить HP ArcSight Enterprise Security Manager, який сумісний величезною кількістю прикладних систем і пристроїв. Поставляється з декількома сотнями, заздалегідь встановленими шаблонами кореляції. Так само до складу може входити свій агент: FlexConnector, який сумісний з будь-яким типом додатків

HP ArcSight ESM є лідером на ринку за технічними можливостями і можливостям інтеграції з бізнес-додатками. Архітектура HP ArcSight ESM дозволяє розгорнути рішення навіть в територіально-розподіленій інформаційній системі з низькошвидкісними каналами зв'язку. HP ArcSight ESM поставляється як в програмному, так і програмно-апаратному вигляді, що вигідно відрізняє його від інших систем кореляції.

Для спрощення завдання зі збирання, зберігання та аналізу журналів аудиту може використовуватися продукт HP ArcSight Logger - готовий програмний або програмно-апаратний комплекс, який може збирати і аналізувати всі дані журналів аудиту організації, надаючи стислий і економічний репозиторій для зберігання логів.

Для більш простого і ефективного збору інформації про події безпеки в складі HP ArcSight ESM і HP ArcSight Logger можуть використовуватися програмні комплекси HP ArcSight Connectors. Необхідно відзначити, що HP ArcSight Connectors також можуть поставлятися у вигляді програмно-апаратних комплексів (HP ArcSight Connector Appliance).

Рішення HP ArcSight Security Intelligence включають в себе наступні продукти:

HP ArcSight Logger - забезпечує збір і фільтрацію подій;

HP ArcSight Threat Response - забезпечує миттєву реакцію на інциденти за допомогою аналізу інформації від HP ArcSight ESM, обчислення географії проблеми і прийняття відповідних дій;

HP ArcSight Configuration Management - дозволяє настроїти мережеве обладнання та налаштування безпеки;

HP ArcSight Fraud Detection - унікальне рішення для виявлення та запобігання шахрайству в області інтернет-банкінгу і банківських (пластикових) карт.

Використання системи моніторингу на основі HP ArcSight допомагає автоматизувати процес реакції на події, пов'язані з порушенням політик безпеки. Також застосування системи моніторингу підвищує ефективність вже встановлених засобів захисту інформації.

Сьогодні рішення від HP популярні в усьому світі серед фінансових організацій, державних структур і операторів зв'язку.

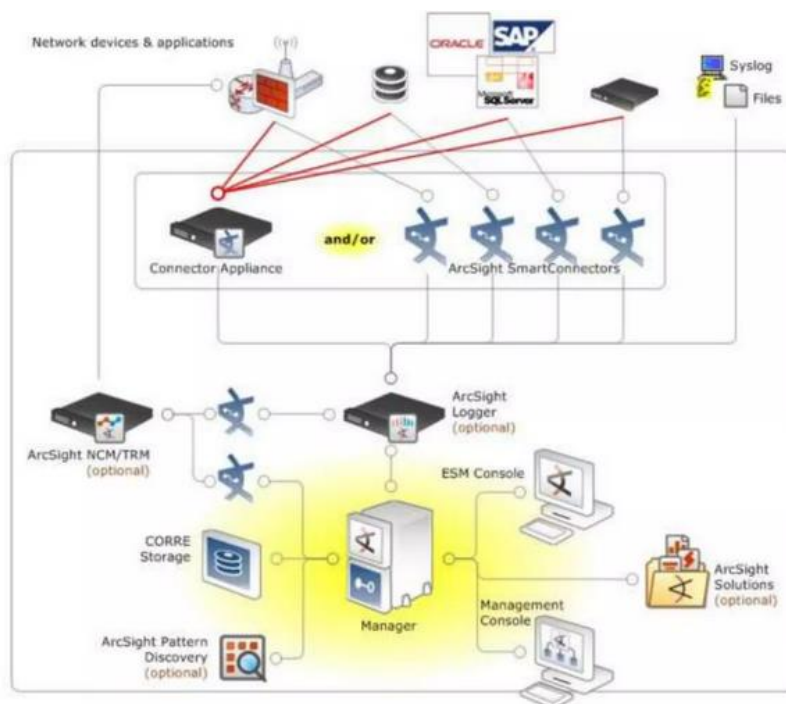


Рис.3.1. Архітектура HP Arcsight

HP Arcsight складається з наступних компонентів:

- ArcSight Manager - основний серверний компонент, «ядро» системи, що забезпечує кореляцію подій і їх обробку;
- ArcSight DB - база даних (на основі СУБД Oracle 11g), призначена для зберігання інформації;
- ArcSight Console - консоль для управління і роботою з системою, що представляє собою додаток, яке встановлюється на клієнтське робоче місце адміністратора або користувача системи;
- ArcSight Web - серверний компонент web-консолі для моніторингу та отримання звітності. Для доступу до інформації використовується будь-який сучасний web-браузер;
- ArcSightSmartConnectors-компоненти системи, забезпечують збір подій з джерел, їх попередню фільтрацію і агрегацію, а також передачу подій в ArcSight Manager. [7]

MAX PATROL 8

MaxPatrol 8 дозволяє отримувати оцінку стану захищеності всієї системи, а так само окремих підрозділів, додатків і вузлів. Механіка системних перевірок, контролю відповідності стандартам і тестування на проникнення, в купе з можливістю аналізу різних операційних систем, систем баз даних і веб-додатків, дають можливість забезпечувати постійний аудит безпеки на всіх рівнях інформаційної системи.

Ключові можливості

Ядром SIEM системи MaxPatrol 8 є професійний сканер вразливостей XSpider. Існуючі в ньому механізми контролю були доповнені за рахунок додавання компонентів системних перевірок і аналізу безпеки без даних. Поєднання в одному комплексі функцій системних і мережевих сканерів, а так само засобів оцінки стану захищеності систем управління баз даних та веб-додатків, дозволяють отримувати максимально реальну картину захищеності системи.

При наявності доступу до механізмів віддаленого управління вузлом модуль сканування може використовувати їх для глибокої перевірки безпеки операційної системи і додатків. Даний метод дозволяє з мінімальним використанням ресурсів отримати комплексну оцінку захищеності, а також провести аналіз параметрів, недоступних в режимі тесту на проникнення.

База знань включає в себе системні перевірки для більшості поширених операційних систем лінійок Windows, Linux і Unix, а також спеціалізованого обладнання, такого як маршрутизатори і комутатори Cisco IOS, міжмережеві екрани Cisco PIX і Cisco ASA.

В відміну від класичних системних сканерів, MaxPatrol 8 не вимагає розгортання програмних модулів на вузлах, що спрощує експлуатацію і знижує сукупну вартість володіння. Всі перевірки проводяться віддалено з використанням

вбудованих механізмів віддаленого адміністрування. За підтримки вузлом декількох протоколів (наприклад, Telnet і SSH) MaxPatrol 8 вибирає найбільш безпечний з них, що забезпечує захист чутливих даних при передачі по мережі.

Архітектура MaxPatrol:

- Безпека
- Захист даних

При передачі та зберіганні використовуються криптографічні методи захисту, що забезпечують конфіденційність і цілісність важливої інформації, такої як паролі користувачів, привілеї на доступ і т. Д. Передбачена можливість використання сертифікованих реалізацій вітчизняних криптографічних алгоритмів.

Захист трафіку забезпечується за допомогою цифрових сертифікатів і протоколу SSL / TLS, що є індустріальним стандартом, що забезпечує високу сумісність і захист даних.

Гнучка система розмежування прав доступу дає можливість здійснювати моніторинг інформаційної безпеки на різних рівнях ієрархії (наприклад, на рівні адміністраторів, менеджерів по ІТ та ІБ підрозділу, Директора з ІБ Компанії). Для кожного з користувачів системи можна задати список завдань, які він може виконувати в системі, а також дозволу на операції над конкретними об'єктами системи. Так, адміністратору Web-серверів можуть бути делеговані права на зміну профілю сканування, запуск і перегляд результатів завдання по оцінці захищеності керованих їм серверів, але заборонено змінювати список сканованих вузлів. У той же час розробник Web-додатків матиме можливість лише переглядати звіти за результатами сканування.

Дозволи можуть призначатися на рівні MaxPatrol 8 Server або MaxPatrol 8 Consolidator. Такий підхід дозволяє адаптувати систему розмежування доступу практично під будь-яку ієрархію управління системою ІБ.

Security Capsule

SIEM ссистема реєстрації подій безпеки ПАКАБ «Security Capsule» сертифікована ФСТЕК для захисту конфіденційної інформації, включаючи ІСПДн. Сертифікат ФСТЕК №2705 від 7 вересня 2012 року.

ПАКАБ SIEM «Security Capsule» призначений для реєстрації подій інформаційної безпеки і виконує наступні функції: реєстрація та облік подій інформаційної безпеки (ІБ) в інформаційно-обчислювальних системах і мережах, розмежування доступу користувачів до інформаційних ресурсів SIEM, контроль доступу SIEM, контроль цілісності файлів SIEM, кореляцію подій ІБ, реакцію на події ІБ.

На основі аналізу інформації, отриманої за допомогою SIEM «Security Capsule», адміністратор безпеки вживає заходів щодо забезпечення безпеки об'єктів інформаційно-обчислювальних систем і мереж.

Реєстрація подій інформаційної безпеки реалізується шляхом ведення журналів реєстрації подій інформаційної безпеки:

- доступ користувача до додатка і завершення роботи;

- дозволені та недозволені дії користувачів по доступу до інформаційних ресурсів;

- повідомлення, одержувані від мережевих пристроїв;

- дії операторів на клієнтських робочих станціях такі як: встановлення доступу до робочої станції за допомогою USB-ключа eToken; звернення до зовнішніх USB-пристроїв, звернення до файлів на зовнішніх пристроях.

Склад модулів програми, у вигляді розроблених конекторів може встановлюватися і надаватися опціонально.

За погодженням із замовником перелік конекторів може бути розширений під конкретні потреби Замовника.

Перелік розроблених конекторів, що дозволяють накопичувати такі дані про події інформаційної безпеки:

- дані від мережевих пристроїв, що використовують протокол syslog
- дані в журналах СУБД,
- дані в системному журналі ОС сімейств Windows, Linux;
- дані при застосуванні знімних носіїв інформації типу eToken, USB, LPT, COM, IEEE 1394, ZlocK, Device Lock;
- дані, отримані від СЗІ від НСД, наприклад
- дані, отримані від антивірусних засобів,
- дані, отримані з Active Directory;
- дані реєстру ОС Windows;
- дані, отримані від IDM систем (Identity Management)
- дані, отримані від DLP систем (Data Leak Prevention)

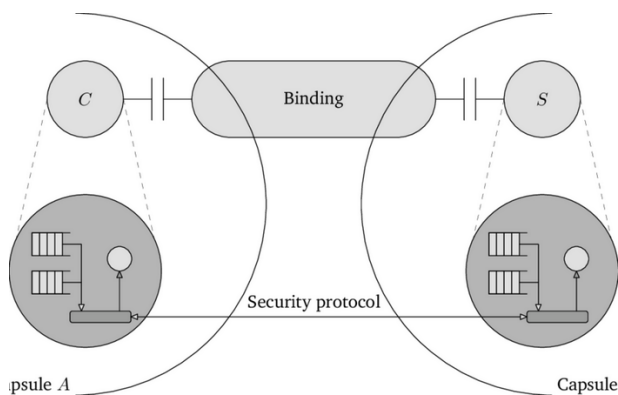


Рис. 3.2. Архітектура

ПАКАБ «Security Capsule» ґрунтується на клієнт-серверній технології для розподілених неоднорідних ІС, СПД, ЛВС і системи захисту конфіденційної інформації.

ПАКАБ «Security Capsule» має модульну архітектуру, що включає в себе:

- модуль серверної частини;

- модуль моніторингу і адміністрування;
- центральний модуль;
- клієнтські модулі;
- коннектори;
- модуль формування звітів.

Таблиця 3.1

Порівняння SIEM систем

	Security Capsule	HP ArcSight	MaxPatrol SIEM
Сертифікат щодо захисту конфіденційної інформації, включаючи ІСПДн	сертифікат від 07.09.2012 (На серійне виробництво) інспекційний контроль	Тільки у 5-й версії ESM. сертифікат від 06.05.2014 (200 примірників)	сертифікат від 31.12.2013
Сертифікат відповідності за рівнем контролю відсутності НДВ	Так	немає	Так
Принцип роботи	Syslog, Eventlog, SNMP, SQL, власний протокол	збір і наступний аналіз логів (в тому числі по Syslog і з мережевих пристроїв)	За допомогою протоколу віддаленого доступу відбувається підключення до системи, аутентифікація, авторизація, збір логів ElasticSearch,
СУБД	MySQL	Своя розробка CORR-E, Red HatEnterprise	MongoDB, MS,SQL

Платформа	OS Windows, OS Windows server, OS RedHat з версії 4.8, RedHat Enterprise Linux 6.X	Linux, версії 6.4 і 6.5, SUSE 11 SP3 (64 розрядна, Windows Server 2012	OC Windows XP \ 7 \ 8, OC Windows Server \ 2008 рік \ 2010 рік \ 2 012
Мова інтерфейсу	українська	українська або англійська	українська або англійська
Звіти	Так	Так	Так
Лог-Менеджмент	Так	Так	Так
Інцидент- менеджмент	Так	Так	да
Оповіщення про інциденти	Так	Так	Так
Можливість установки на сервер	Так	Так	Так
Програмно-апаратна реалізація	Так	Так	Так
Облік вразливостей ресурсів	Так	Так	Так
Управління ховищем даних	Так	Так	Так
Збір логів	Так	Так	Так
Кореляція	Так	Так	Так
Управління інцидентами	Так	Так	Так
Захист інформації про події безпеки	Так	Так	Так

3.3. Проектування найбільш ефективної системи захисту інформації

Політика інформаційної безпеки підприємства

1. Вступ

Політика інформаційної безпеки підприємства (далі — Політика) є основним документом, що визначає загальні принципи, правила та процедури для захисту інформаційних активів підприємства. Метою цієї політики є забезпечення конфіденційності, цілісності, доступності та відновлюваності інформації, а також мінімізація ризиків втрати чи компрометації даних.

2. Область застосування

Ця політика застосовується до всіх співробітників підприємства, підрядників, партнерів та постачальників, які мають доступ до інформаційних систем і ресурсів підприємства. Вона охоплює всі аспекти управління інформаційною безпекою, включаючи захист інформаційних систем, фізичний доступ, управління ризиками, моніторинг та реагування на інциденти.

3. Основні принципи інформаційної безпеки

3.1 Конфіденційність

Всі чутливі та конфіденційні дані підприємства повинні бути доступні тільки тим особам, яким вони необхідні для виконання своїх обов'язків. Це включає персональні дані клієнтів, фінансові звіти, стратегії компанії та іншу критичну інформацію.

3.2 Цілісність

Інформація повинна бути точною, повною і актуальною. Не допускаються будь-які несанкціоновані зміни, втручання або пошкодження даних.

3.3 Доступність

Інформація та інформаційні системи повинні бути доступні для авторизованих користувачів у будь-який час, коли це необхідно для виконання їхніх обов'язків.

3.4 Відновлюваність

У разі інцидентів або збоїв у системах, підприємство повинно мати чітко визначені процедури для відновлення даних і забезпечення безперебійної роботи.

4. Ролі та обов'язки

4.1 Вища керівна команда

Вища керівна команда підприємства несе загальну відповідальність за забезпечення інформаційної безпеки і затвердження цієї політики. Вона повинна забезпечити належні ресурси для впровадження і підтримки заходів безпеки.

4.2 Відповідальна особа за інформаційну безпеку (CISO)

CISO відповідає за розробку, впровадження та моніторинг політики інформаційної безпеки, а також за забезпечення належної роботи систем безпеки, їх постійне вдосконалення і реагування на інциденти.

4.3 Співробітники

Всі співробітники підприємства повинні дотримуватися вимог цієї політики, зокрема щодо захисту паролів, використання ресурсів, управління доступами та повідомлення про інциденти безпеки.

5. Управління доступом

5.1 Ролі та права доступу

Доступ до інформаційних систем та даних має надаватися на основі принципу "необхідності знати". Кожен співробітник повинен мати доступ лише до тих ресурсів, які необхідні для виконання його обов'язків.

5.2 Аутентифікація та авторизація

Використовуються багаторівневі механізми аутентифікації, зокрема багатофакторна автентифікація (MFA) для доступу до критичних систем та даних.

5.3 Перегляд прав доступу

Регулярно переглядається та оновлюється список користувачів з доступом до інформаційних ресурсів. При зміні ролі співробітника або його звільненні доступ до даних має бути негайно змінений або відкликаний.

6. Захист інформаційних систем

6.1 Шифрування даних

Всі чутливі дані, що зберігаються або передаються через мережу, повинні бути зашифровані із використанням сучасних стандартів шифрування, таких як AES-256 для зберігання даних і TLS/SSL для передачі.

6.2 Антивірусний захист

Усі кінцеві пристрої (персональні комп'ютери, ноутбуки, мобільні пристрої) повинні бути оснащені актуальними антивірусними програмами для виявлення і блокування шкідливого ПЗ.

6.3 Захист мережі

Використовуються сучасні брандмауери, системи виявлення та запобігання вторгнень (IDS/IPS), а також VPN для захищеного віддаленого доступу до корпоративних ресурсів.

6.4 Резервне копіювання та відновлення

Резервне копіювання критичних даних має здійснюватися регулярно, а також повинні бути визначені процедури для відновлення інформації у разі втрати або пошкодження.

7. Моніторинг та аудит

7.1 Моніторинг систем

Усі інформаційні системи підприємства підлягають постійному моніторингу для виявлення аномалій, підозрілих активностей або потенційних загроз. Для цього використовуються інструменти SIEM (наприклад, Splunk).

7.2 Аудит доступу

Регулярно проводиться аудит прав доступу і використання інформаційних систем, а також перевірка на відповідність політиці безпеки.

7.3 Повідомлення про інциденти

Співробітники зобов'язані негайно повідомляти про будь-які інциденти безпеки або підозрілі дії, що можуть загрожувати інформаційній безпеці підприємства.

8. Реагування на інциденти

8.1 План реагування на інциденти

У разі виявлення інцидентів безпеки повинна діяти розроблена процедура реагування, яка включає:

Виявлення та ізоляцію інциденту.

Аналіз та оцінку масштабу.

Усунення загрози та відновлення систем.

Документування інциденту та аналіз причин.

8.2 План відновлення після катастрофи

Має бути розроблений і підтримуваний план відновлення критичних інформаційних ресурсів і систем після серйозних інцидентів.

9. Навчання та підвищення обізнаності персоналу

Регулярні тренінги для співробітників щодо актуальних загроз (фішинг, соціальна інженерія, шкідливе ПЗ), а також навчання основам інформаційної безпеки (використання сильних паролів, безпечне використання пристроїв тощо).

10. Оцінка та вдосконалення політики

Ця політика підлягає регулярному перегляду та вдосконаленню для забезпечення відповідності сучасним вимогам безпеки та новим загрозам. Оцінка ефективності політики проводиться не менше одного разу на рік.

11. Порушення політики

Порушення цієї політики може призвести до дисциплінарних заходів, включаючи попередження, звільнення або інші санкції відповідно до трудового законодавства.

Ця політика є основою для створення безпечного інформаційного середовища на підприємстві та повинна бути чітко донесена до всіх співробітників для належного виконання.

На підставі розглянутих у попередніх розділах моделей загроз та можливого порушника та враховуючи вимоги до політики безпеки та параметрів КСЗІ можна запропонувати наступну структуру КСЗІ на підприємстві, сфера діяльності якого – надання адміністративних послуг. Компоненти КСЗІ показані на рис.3.2.

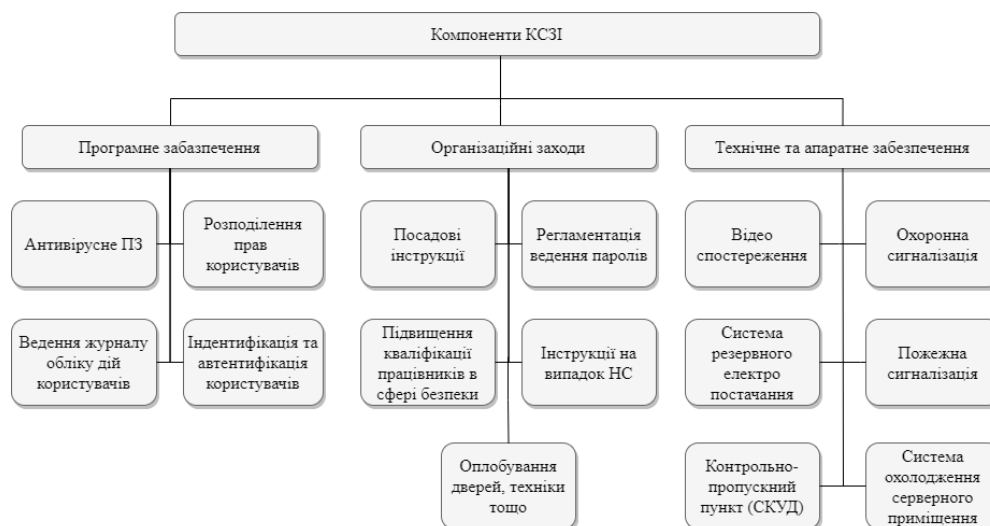


Рисунок 3.2 – Компоненти комплексної системи захисту інформації

Узагальнене представлення загроз та відповідних рішень наведено у табл. 3.2.

Таблиця 3.2

Узагальнене представлення загроз і рішень

	Загроза	Вразливість	Рішення
1	Пасивний моніторинг мережі	Конфіденційність	Криптографія, шифрування
2	Прослуховування та аналіз трафіку	Конфіденційність	Криптографія, шифрування
3	Атаки маршрутизації	Цілісність мережі, маршрутизація, доступність даних	Захищена маршрутизація, аутентифікація, керування ключами центр довіри
3.1	Підміна ідентифікатора	Механізми маршрутизації, агрегація даних	Захищена маршрутизація, захищене агрегування даних
3.2	Вибіркове видалення	Цілісність мережі, доступність даних	Захищена маршрутизація
3.3	Модифікація інформації про маршрутизацію	Таблиці маршрутизації	Захищена маршрутизація
3.4	Атаки типу "воронка"	Маршрутизація, цілісність мережі	Захищена маршрутизація
3.5	Атака через переповнення	Пропускна здатність каналів мережі, енергетичні та обчислювальні ресурси	Захищена маршрутизація
3.6	Атаки типу "червоточина"	Цілісність мережі, таблиці маршрутизації	Захищена маршрутизація

4	Відмова в обслуговуванні	Цілісність мережі, енергетичні та обчислювальні ресурси	Стійкість до відмов в обслуговуванні, зокрема механізм розширеного спектру
5	Захоплення вузла	Цілісність мережі, криптографічні ключі, конфіденційна інформація	Ідентифікація вторгнень
6	Несправність вузла або вихід його ладу	Цілісність мережі	Альтернативні маршрути, вбудована діагностика
7	Фальшування або копіювання вузла	Цілісність мережі, конфіденційна інформація	Ідентифікація вторгнень

Загальна модель призначена для відбору найбільш значущих загроз з повного переліку, який здійснюється в два етапи:

1. Відбір по пріоритету загроз.
2. Відбір за рівнем втрат від реалізації загроз.

Загальна модель загроз включає в себе наступні компоненти:

- об'єкт, на який спрямована загроза;
- компонент, що відображає привабливість реалізації загрози для порушника;
- матрицю потенційних втрат об'єкта захисту при реалізації загрози.

Інтегрована модель загроз призначена для опису можливих дій порушників і формування сценаріїв реалізації загроз. Наведемо приклад уявлення інтегрованої моделі у вигляді ієрархічної структури, що складається з моделей декількох рівнів.

У загальному вигляді інтегрована модель загроз включає в себе [19]:

- компонент, що описує комплексний рівень;
- компонент, що описує сценарний рівень;
- компонент, що описує дії порушника.

ВИСНОВКИ

В роботі розглянуто варіанти рішення важливого та актуального завдання аналізу вразливостей інформаційних систем та відповідних методів захисту.

При цьому отримано наступні результати.

Проблемами аналізу трафіку є обмеження методів вимірювання та виявлення, великий обсяг трафіку та подій, а також необхідність захисту персональних даних. Кожне мережеве середовище є унікальним, і просте співвідношення подій безпеки може працювати в невеликих і добре підтримуваних мережах. Такі середовища є рідкісними. Як правило, будь-яка мережа, що підключена до Інтернету, піддається щоденному мережевому скануванню, спаму, атак нульового дня, а також шкідливим користувачам мережі, які є прихованими у величезних обсягах трафіку в просторах Інтернету. Величезний обсяг трафіку може перешкоджати роботі засобів аналізу трафіку, змусити їх відмовитися від даних і погіршити їхні загальні можливості аналізу.

Наприклад, неправильно працююча система виявлення аномалій може створити таку велику кількість повідомлень, що команда безпеки перестане їх аналізувати. Не менш важливим є те, що чутливий характер даних, які передаються по мережі, вимагає, щоб аналіз трафіку ретельно враховував питання конфіденційності.

Детальна інформація про трафік необхідна для забезпечення постійної ситуаційної обізнаності про мережу. Така інформація може бути слідами пакетів, статистикою потоку або статистикою обсягу. Як правило, необхідно зробити компроміс між обчислювальною доцільністю та наданим рівнем інформації для ефективної обробки високошвидкісного трафіку у великих мережах.

Повні сліди пакетів, що традиційно використовуються аналізаторами трафіку, забезпечують найбільш детальну інформацію. Проте, масштабованість і можливість обробки постійного спостереження за трафіком і зберігання у

високошвидкісних мережах є проблемою внаслідок необхідності збереження конфіденційності та високих експлуатаційних витрат. Статистика потоків надає інформацію з заголовків Інтернет-протоколу (IP). Вони не містять інформації про корисне навантаження; однак, ми все ще знаємо, з точки зору інформаційної системи, хто спілкується з ким, коли і як довго, який протокол використовувався, а також, скільки даних було передано. Такий підхід значно зменшує обсяг даних, які необхідно обробити та зберегти. Статистика потоків надає інформацію навіть про зашифрований трафік, оскільки заголовки пакетів не шифруються.

Апаратне прискорення інструментів моніторингу використовується для того, щоб впоратися з високошвидкісним мережевим трафіком, особливо в середовищах, де потрібно гарантувати функціональність моніторингу навіть у найгірших випадках, таких як атаки відмови в обслуговуванні. Проте, будь-який апаратний або програмний прискорювальний механізм часто повинен використовувати оптимізовані версії операційної системи і засоби моніторингу.

Таким чином, аналіз потоків забезпечує масштабований підхід до моніторингу великих мереж. Однак необхідно проаналізувати дані про потоки, а не тільки зберігати їх для отримання даних, обробки інцидентів та проведення експертизи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A quantitative analysis of current security concerns and solutions for cloud computing / N. Gonzalez et al. // Journal of Cloud Computing: Advances, Systems and Applications. – 2022. – V. 1, №. 1. – P. 110-117.
2. A view of cloud computing / M. Armbrust [et al.] // Communications of the ACM. – 2020. – V. 53, №. 4. – C. 50-58.
3. About SecuCloud. URL: <https://secucloud.com/en/company/about-us>
4. Almorsy, M. Collaboration-based cloud computing security management framework /M. Almorsy, J. Grundy, A.S. Ibrahim // Cloud Computing (CLOUD), 2021 IEEE International Conference on, Washington, 4-9 July, 2021 y. – IEEE, 2021. – P. 364-371.
5. AlSharafat M. S. et al. Adaptive steady state genetic algorithm for scheduling university exams // Networking and Information Technology (ICNIT), 2010 International Conference on. – IEEE, 2020. – C. 70-74.
6. Bernstein, D. Cloud foundry aims to become the OpenStack of PaaS / D. Bernstein // IEEE Cloud Computing. – 2024. – V. 2, №. 1. – P. 57-60.
7. Bhardwaj, S. Cloud computing: A study of infrastructure as a service (IAAS) / S. Bhardwaj, L. Jain, S. Jain // International Journal of engineering and information Technology. – 2020. – V. 2, №. 1. – P. 60-63.
8. Carlin, A. Defence for Distributed Denial of Service Attacks in Cloud Computing / A. Carlin, M. Hammoudeh, O. Aldabbas // Procedia Computer Science. – 2023. – V. 73. – P. 490-497.
9. Cloud computing: the limits of public clouds for business applications / P. Hofmann, D. Woods // IEEE Internet Computing. – 2020. – V. 14, №. 6. – P. 90-93.
10. Cloud computing: the limits of public clouds for business applications / P. Hofmann, D. Woods // IEEE Internet Computing. – 2021. – V. 14, №. 6. – P. 90-93.

11. Deitel, H. An introduction to operating systems / H. Deitel. – Boston: Addison-Wesley publishing company, 2024. – 657 p.
12. Delimitrou C.; Kozyrakis C. Security Implications of Data Mining in Cloud Scheduling // IEEE Computer Architecture Letters. 2023. №PP. pp. 64-68.
13. Detecting DNS amplification attacks / G. Kambourakis [et al.] // International Workshop on Critical Information Infrastructures Security, Malaga, Spain, 3-5 October, 2021 y. – Springer Berlin Heidelberg, 2021. – P. 185-196.
14. Fierceitsecurity. 5 ways to stop a DDoS attack. [Электронный ресурс]. – Режим доступа: <http://www.fierceitsecurity.com/story/5-ways-stop-ddos-attack/2021-06-02>.
15. Garreta R., Moncecchi G. Learning scikit-learn. Machine Learning in Python. Birmingham: Packt, 2023. p. 118.
16. Gartner Inc. Special Report: Cybersecurity at the Speed of Digital Business [Электронный ресурс]. – Режим доступа: <https://www.gartner.com/doc/3426427>
17. Intelligent workload factoring for a hybrid cloud computing model / H. Zhang [et al.] // Proceedings of 2021 Congress on Services. c. Los Angeles, 6-10 July 2021 y. Los Alamitos.: IEEE computer society, 2021. – P. 701-708.
18. Kato K., Klyuev V. Large-scale network packet analysis for intelligent DDoS attack detection development // Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for. – IEEE, 2024. – C. 360-365.
19. Keller, E. The "Platform as a Service" Model for Networking / E. Keller, J. Rexford // Proceedings of INM WREN. Plumouth, 19-21 July, 2022 y. – Plumouth: Plumouth University, 2022. – P. 29-43.
20. Liu, L. Cloud service portal for mobile device management/ L.Liu, R. Moulic, D. Shea // e-Business Engineering (ICEBE), 2021 IEEE 7th International Conference on. – IEEE, 2021. – P. 474-478.

21. Mell, P. The NIST definition of cloud computing / P. Mell, T. Grance // Community cloud computing / A. Marinos, G. Briscoe // Lecture Notes in Computer Science. – 2022. – № 5931. – P. 472-484.
22. Microsoft office 365-cloud in business environment / A. Skendzic, B. Kovacic 2022 Proceedings of the 35th International Convention. c. Opatija, 21-25 May, 2022 y. – Rijeka: MIPRO, 2022. – P. 1434-1439.
23. Miller, M. Cloud computing: Web-based applications that change the way you work and collaborate online / M. Miller. – Pearson: Que publishing, 2022. – 29 p.
24. Munz, G., Li, S., Carle, G.: Traffic Anomaly Detection Using K-Means Clustering // Proceedings of GI/ITG Workshop MMBnet. 203. pp. 106-110.
25. Mutu, L. Improved SDN responsiveness to UDP flood attacks /L. Mutu, R. Saleh, A. Matrawy // Communications and Network Security (CNS), 2022 IEEE Conference on, San Francisco, 29-31 October, 2022 y. – IEEE, 2022. – P. 715-716.
26. Olszak, C. M. Business Intelligence in cloud / C. M. Olszak // Polish Journal of Management Studies. – 2024. – V. 10. – P. 115-125.
27. Performance analysis of high performance computing applications on the amazon web services cloud / Jackson K. R. [et al.] // Proceedings of 2021 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). – Indianapolis.: IEEE. – P. 159-168.
28. Pousty, S. Getting started with OpenShift / S. Pousty, K. Miller. – Sebastopol: O'Reilly Media, 2024. – 316 p.
29. Prasad, K. M. DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey / K.M. Prasad, A.R.M. Reddy, K.V. Rao // Global Journal of Computer Science and Technology. – 2024. – V. 14, №. 7. – P. 15-32.
30. Prechelt, L. An empirical comparison of seven programming languages / L. Prechelt // Computer. – 2020. – V. 33, №. 10. – P. 23-29.

31. Rittinghouse, J. W. Cloud computing: implementation, management, and security / J.W. Rittinghouse, J.F. Ransome. – Boca Raton: CRC press, 2022. – 97 p.
32. Sla-based resource allocation for software as a service provider (saas) in cloud computing environments / L. Wu [et al.] // Proceedings of 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), c. Newport Beach, 23-26 May, 2021. – Los Alamitos: IEEE computer society, 2021. – P. 195-204.
33. The flooding time synchronization protocol / M. Maroti [et al.] // Proceedings of the 2nd international conference on Embedded networked sensor systems, New York, 3-5 November, 2024 y. – ACM, 2024. – P. 39-49.
34. Tyde, F. Oracle Cloud Computing Strategy / F. Tyde // Program Executive, High Performance, Grid, Cloud Computing Oracle ASEAN. – 20229. – 52 p.
35. Wang B. et al. DDoS attack protection in the era of cloud computing and software-defined networking // Computer Networks. – 2021. – T. 81. – C. 308-319.
36. Wodczak, M. Resilience aspects of autonomic cooperative communications in context of cloud networking / M. Wodczak // Proceedings of First International Symposium on Network Cloud Computing and Applications (NCCA). c. Toulouse, 21-23 November, 2021 y. – Los Alamitos: IEEE computer society, 2021. – P. 107-113.