ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ WEB-РЕСУРСІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Володимир ГЛОТОВ

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
ГЛОТОВ Володимир
(ПРІЗВИЩЕ, Ім'я)

Керівник: БОРСУКОВСЬКИЙ Юрій
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: ТУРОВСЬКИЙ Олександр
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Глотову Володимиру Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія захисту Web-ресурсів в інформаційній системі організації»
керівник кваліфікаційної роботи: БОРСУКОВСЬКИЙ Юрій, к.т.н., доцент,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія управління контролем доступу до мережі;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж.
2. Методи та засоби управління мережевим доступом організацій.

3. Розроблення варіанта технології управління доступом до мережі організації.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності проблеми управління привілеями в інформаційній системі організації	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності контролю доступу до мережі на основі застосування політик пристроїв і користувачів корпоративних мереж	27.10. 2023р.	
4.	Методи та засоби управління мережевим доступом організацій	03.11.2023 р.	
5.	Розроблення варіанта технології управління доступом до мережі організації	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Володимир ГЛОТОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Глотов В.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту Web-ресурсів в інформаційній системі організації».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ГЛОТОВ Володимир*** обрав тему роботи, метою якої було дослідити зміст технології контролю доступу до мережі організацій. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ГЛОТОВ Володимир*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ГЛОТОВА Володимира*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***ГЛОТОВ Володимир***. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Глотова Володимира
на тему: «Технологія захисту Web-ресурсів в інформаційній системі організації».

Актуальність:

Метою кожної організації є контроль доступу користувачів до корпоративної мережі, Отримання доступу до мережі організації, може призвести до руйнації активів, репутації організації. Тому організації зосереджують свою увагу на впровадження технологій контролю доступу користувачів до корпоративної мережі. Залежність від інформаційних технологій вимагає вдосконалення систем безпеки для запобігання серйозним наслідкам кібератак та витоків конфіденційної інформації. Розробка та впровадження ефективних засобів захисту Web-ресурсів стає необхідністю для забезпечення стійкої та надійної роботи інформаційних систем. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми забезпечення контролю доступу до мережі організації.
2. Досліджено методи та засоби управління мережевим доступом організацій.
3. Запропоновано варіант технології управління доступом до мережі організації
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні групи користувачів проводового та безпроводового доступу.
2. Запропонований варіант варіант технології управління доступом до мережі організації доцільно було б показати на прикладі конкретного підприємства.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ГЛОТОВ Володимир** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:		Олександр ТУРОВСЬКИЙ
д.т.н., професор	*підпис*	*Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Сучасний швидкозмінний характер технологій та поширення інформаційних технологій породжують неабиякі виклики для забезпечення безпеки Web-ресурсів в інформаційних системах організацій. З урахуванням постійно зростаючого обсягу цифрової інформації, необхідно вдосконалювати технології захисту для забезпечення конфіденційності, цілісності та доступності даних. Магістерська робота присвячена розгляданню та вирішенню цих завдань шляхом розробки ефективних технологій захисту, орієнтованих на вимоги інформаційної безпеки. Робота спрямована на поєднання теоретичних аспектів кібербезпеки з практичними рішеннями для створення стійких та надійних Web-ресурсів в інформаційних системах організацій.

Мета дослідження: Метою магістерської роботи є розробка та вдосконалення технологічних засобів захисту Web-ресурсів у інформаційній системі організації з метою забезпечення конфіденційності, цілісності та доступності інформації.

Предмет дослідження: Об'єктом дослідження є методи, техніки та технології захисту Web-ресурсів, включаючи застосування шифрування, ідентифікації та автентифікації, виявлення та вирішення загроз безпеки.

Об'єкт дослідження: Об'єктом дослідження є інформаційна система організації, що включає в себе веб-додатки, бази даних та інші компоненти, піддаючись ризикам в сфері кібербезпеки.

Наукова новизна: Робота розглядає інтегрований підхід до захисту Web-ресурсів, враховуючи останні тенденції в галузі кібербезпеки. Особлива увага приділяється розробці ефективних методів виявлення та протидії новітнім загрозам.

Практична значущість: Результати дослідження можуть бути використані організаціями для підвищення рівня безпеки їхніх інформаційних систем. Розроблені технологічні рішення та рекомендації допоможуть забезпечити стійкість Web-ресурсів до сучасних кіберзагроз.

Ключові слова: захист інформації, кібербезпека, Web-ресурси, інформаційна система, шифрування, ідентифікація, автентифікація, загрози безпеки.

ABSTRACT

The dynamic nature of technology and the widespread use of information technologies pose considerable challenges for securing web resources within organizational information systems. Given the ever-increasing volume of digital information, there is a pressing need to enhance protective technologies to ensure the confidentiality, integrity, and availability of data. This master's thesis is dedicated to examining and addressing these challenges by developing effective protection technologies aligned with the requirements of information security. The study aims to integrate theoretical aspects of cybersecurity with practical solutions to create resilient and reliable web resources within organizational information systems.

Research Objective: The primary objective of this master's thesis is the development and improvement of technological tools for safeguarding web resources within an organizational information system, with the goal of ensuring the confidentiality, integrity, and availability of information.

Research Subject: The research focuses on methods, techniques, and technologies for protecting web resources, including the application of encryption, identification, authentication, and the detection and resolution of security threats.

Research Object: The object of the study is the information system of an organization, encompassing web applications, databases, and other components, susceptible to risks in the realm of cybersecurity.

Scientific Novelty: The thesis explores an integrated approach to securing web resources, taking into account the latest trends in the field of cybersecurity. Special attention is given to the development of effective methods for detecting and mitigating emerging threats.

Practical Significance: The findings of this research can be utilized by organizations to enhance the security levels of their information systems. The developed technological

solutions and recommendations will contribute to fortifying web resources against contemporary cyber threats.

Keywords: Information security, cybersecurity, web resources, information system, encryption, identification, authentication, security threats.

ЗМІСТ

ВСТУП

З появою та стрімким розвитком інформаційних технологій сучасний бізнес та організації стикаються з неспокійним завданням забезпечення безпеки своїх Web-ресурсів в умовах невпинної зміни технологій. Це вимагає від організацій вдосконалення технологічних рішень та прийняття комплексних заходів для забезпечення конфіденційності, цілісності та доступності інформації. Зокрема, захист Web-ресурсів стає ключовим аспектом інформаційної безпеки, оскільки саме через ці ресурси відбувається взаємодія між користувачами та інформаційною системою організації.

Однак, із зростанням обсягу цифрової інформації та розвитком сучасних кіберзагроз, традиційні методи захисту виявляються недостатньо ефективними, а тому необхідно постійно вдосконалювати стратегії та технічні засоби безпеки[1]. Ця магістерська робота присвячена ретельному розгляданню та вирішенню проблем безпеки Web-ресурсів в інформаційних системах організацій.

Актуальність дослідження – Нинішній момент є критичним, оскільки висока залежність від інформаційних технологій вимагає вдосконалення систем безпеки для запобігання серйозним наслідкам кібератак та витоків конфіденційної інформації. Розробка та впровадження ефективних засобів захисту Web-ресурсів стає необхідністю для забезпечення стійкої та надійної роботи інформаційних систем.

Мета та Завдання Дослідження – Метою цієї магістерської роботи є розробка та вдосконалення технологічних засобів захисту Web-ресурсів в інформаційній системі організації. Для досягнення цієї мети визначено такі завдання:

1. **Аналіз сучасних загроз безпеці:** Вивчення та аналіз сучасних кіберзагроз для визначення основних викликів, якими стикаються Web-ресурси.
2. **Розробка технологічних засобів захисту:** Розробка нових або вдосконалення існуючих технологічних засобів для ефективного захисту Web-ресурсів в інформаційній системі.
3. **Інтеграція теоретичних та практичних аспектів кібербезпеки:** Поєднання теоретичних знань та практичних рішень для створення комплексної стратегії захисту, яка враховує останні тенденції в галузі.

Очікувані Результати – Від цього дослідження очікується розробка інноваційних методів та засобів захисту, які підвищать рівень безпеки Web-ресурсів організацій та сприятимуть розвитку більш стійких інформаційних систем.

Ця робота стане важливим внеском у сферу кібербезпеки, сприяючи подальшому розвитку та вдосконаленню заходів захисту інформаційних ресурсів організацій.

РОЗДІЛ 1. ТЕОРЕТИЧНИЙ АНАЛІЗ ПРОБЛЕМНОЇ ГАЛУЗІ

1.1. Поняття інформаційної безпеки в організації

Інформаційна безпека в сучасному світі стає визначальним аспектом для стабільної та ефективної діяльності організацій, особливо в умовах зростаючого впливу технологій та інтернет-середовища. Пошкодження, втрата або неправомірний доступ до інформації може призвести до серйозних наслідків для діяльності підприємства[15]. Таким чином, розуміння і практична реалізація поняття інформаційної безпеки є стратегічно важливим завданням для будь-якої сучасної організації.

Основні аспекти інформаційної безпеки

Інформаційна безпека є невід'ємною складовою сучасної стратегії управління ризиками та забезпечення стійкості діяльності організацій в умовах постійно зростаючих загроз інформаційної безпеки. Вона включає в себе комплекс заходів та стратегій, спрямованих на забезпечення трьох основних аспектів: конфіденційності, цілісності та доступності інформації.

Конфіденційність є одним із ключових принципів інформаційної безпеки і передбачає збереження інформації в таємниці та відсутність несанкціонованого доступу до неї. Це означає застосування різноманітних методів шифрування, контролю доступу та інших технологічних засобів для запобігання несанкціонованому розголошенню чутливої інформації. Визначення рівнів доступу, обмеження прав користувачів та аудиторія дій є ключовими аспектами забезпечення конфіденційності[2].

Цілісність інформації означає гарантування точності, повноти та невід'ємності даних. Заходи, спрямовані на забезпечення цілісності, включають в себе системи контролю версій, механізми виявлення та запобігання змінам без належного санкціонування, а також процедури аудиту для моніторингу та фіксації змін в інформації.

Доступність визначає готовність інформації для використання у потрібний момент. Це включає в себе заходи, спрямовані на запобігання відмовам у роботі систем, відновлення обслуговування після інцидентів, а також регулярні тести та моніторинг для забезпечення оптимальної продуктивності та готовності до збоїв[16].

Ефективна інформаційна безпека включає в себе гармонійне поєднання цих трьох аспектів. Забезпечуючи конфіденційність, цілісність та доступність інформації, організації можуть забезпечити не лише захист від потенційних загроз, але й оптимальне використання своїх інформаційних ресурсів для досягнення стратегічних та операційних цілей.

Ризики інформаційної безпеки в організації

Організації стикаються з різноманітними загрозами інформаційної безпеки, серед яких можна виділити кібератаки, витоки даних, внутрішні порушення безпеки, та інші. Розуміння цих ризиків є важливим етапом для визначення стратегій та технологій захисту.

Кібератаки

Кібератаки є однією з найбільш серйозних загроз для інформаційної безпеки організацій. Ці напади можуть включати в себе витік чутливої інформації, зруйнування даних, або блокування доступу до важливих ресурсів. Наприклад, атаки

на мережеві системи, віруси та зловмисне програмне забезпечення можуть викликати серйозні наслідки для бізнес-процесів.

Витоки даних

Витоки даних можуть виникнути як через кібератаки, так і через необачне внутрішнє поводження з інформацією. Втрата конфіденційної інформації може призвести до порушення довіри клієнтів, порушення регулятивних вимог та великої фінансової шкоди.

Внутрішні порушення безпеки

Навіть при наявності передових заходів зовнішньої оборони, внутрішні порушення безпеки можуть виникнути через недбале ставлення або недостатню освіту співробітників. Несанкціонований доступ до інформації, використання слабких паролів, або недбале поводження з електронними пристроями може стати причиною витоків даних або зловмисного використання інформації[17].

Соціальний інжиніринг

Атаки через соціальний інжиніринг використовують вплив на людей, щоб вони виконали дії, які можуть призвести до компрометації інформації. Фішинг, або використання соціальних мереж для отримання конфіденційної інформації, стає все більш поширеним і вимагає особливої уваги в рамках стратегій захисту.

Недостатня усвідомленість та освіта

Недостатня усвідомленість та освіта персоналу щодо засобів інформаційної безпеки може призвести до виникнення ризиків, які можна було б уникнути.

Неправильне використання паролів, відсутність оновлень програмного забезпечення та інші практики можуть стати джерелом загроз.

Розуміння різноманітних ризиків інформаційної безпеки є критично важливим для розробки комплексних стратегій та технологій захисту. Забезпечення інформаційної безпеки включає в себе ідентифікацію, аналіз та мінімізацію цих ризиків для забезпечення стійкості та надійності інформаційних систем організації.

Вплив інформаційної безпеки на бізнес-процеси

Захист довіри стейкхолдерів

Ефективна інформаційна безпека відіграє ключову роль у забезпеченні довіри стейкхолдерів до організації. Клієнти, партнери та інші зацікавлені сторони вимагають впевненості в тому, що їхні дані і інформація обробляються та зберігаються в безпечному середовищі[3]. Посилення заходів інформаційної безпеки сприяє підвищенню довіри, що в свою чергу може позитивно впливати на репутацію та конкурентоспроможність організації.

Збільшення ефективності бізнес-процесів

Інформаційна безпека служить фундаментом для безперебійності та ефективності бізнес-процесів. Захист від кіберзагроз, витоків даних та інших інцидентів дозволяє організації уникнути перерв у роботі та забезпечити неперервну доступність необхідної інформації. Це збільшує продуктивність та швидкість реакції на зміни в бізнес-середовищі.

Зниження витрат на подолання наслідків інцидентів

Інциденти інформаційної безпеки можуть призвести до серйозних фінансових втрат та інших негативних наслідків. Забезпечення адекватного рівня інформаційної безпеки допомагає зменшити ризик виникнення інцидентів, а в разі їхнього виникнення — забезпечити ефективне їхнє управління та подолання[18]. Це може включати в себе витрати на відновлення послуг, розслідування та відшкодування, які можна уникнути за наявності надійних систем захисту.

Забезпечення відповідності регуляторним вимогам

Багато галузей встановлюють строгі регуляторні вимоги щодо збереження та обробки інформації. Забезпечення відповідності цим вимогам через заходи інформаційної безпеки дозволяє уникнути штрафів та інших негативних наслідків, пов'язаних з порушенням законодавства.

Залучення інвестицій та клієнтів

Організації, що активно піклуються про свою інформаційну безпеку, можуть бути більш привабливими для інвесторів та клієнтів[19]. Захищена інформація стає додатковим аргументом у сприйнятті організації як надійного та відповідального партнера.

Стандарти та підходи до інформаційної безпеки

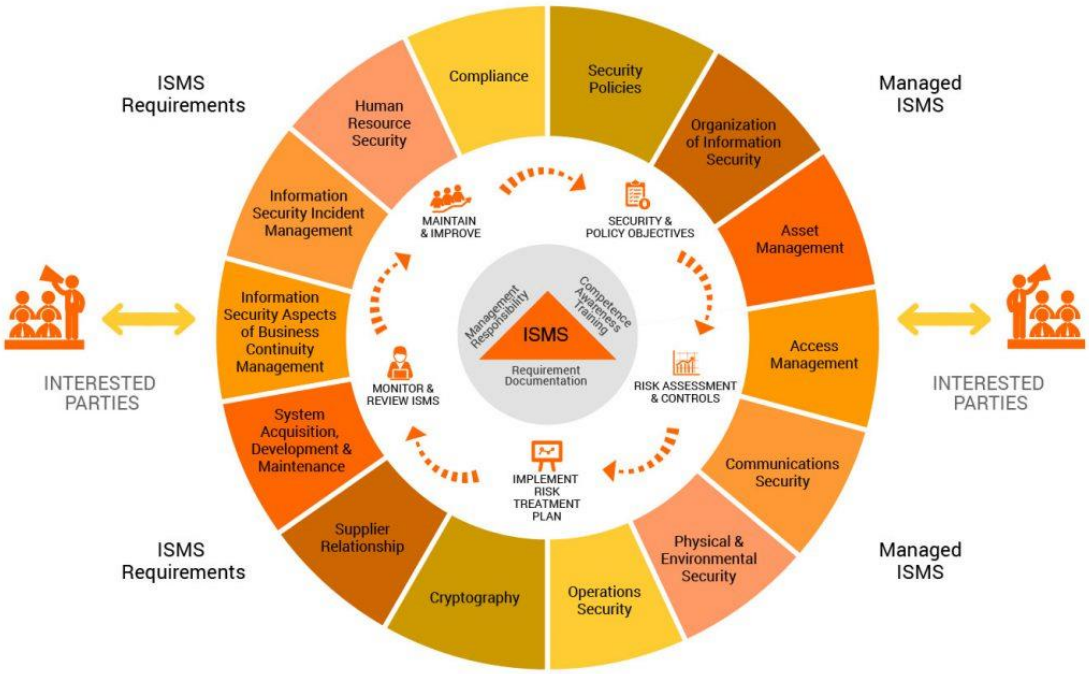

Рис.1.1 – Стандарт ISO/IEC 27001

ISO/IEC 27001 є одним з найвизнаніших стандартів у галузі інформаційної безпеки. Він встановлює системний підхід до управління інформаційною безпекою, включаючи в себе усі аспекти відзначені у триаді конфіденційності, цілісності та доступності[4]. Стандарт визначає вимоги до встановлення, впровадження, управління та покращення системи управління інформаційною безпекою.

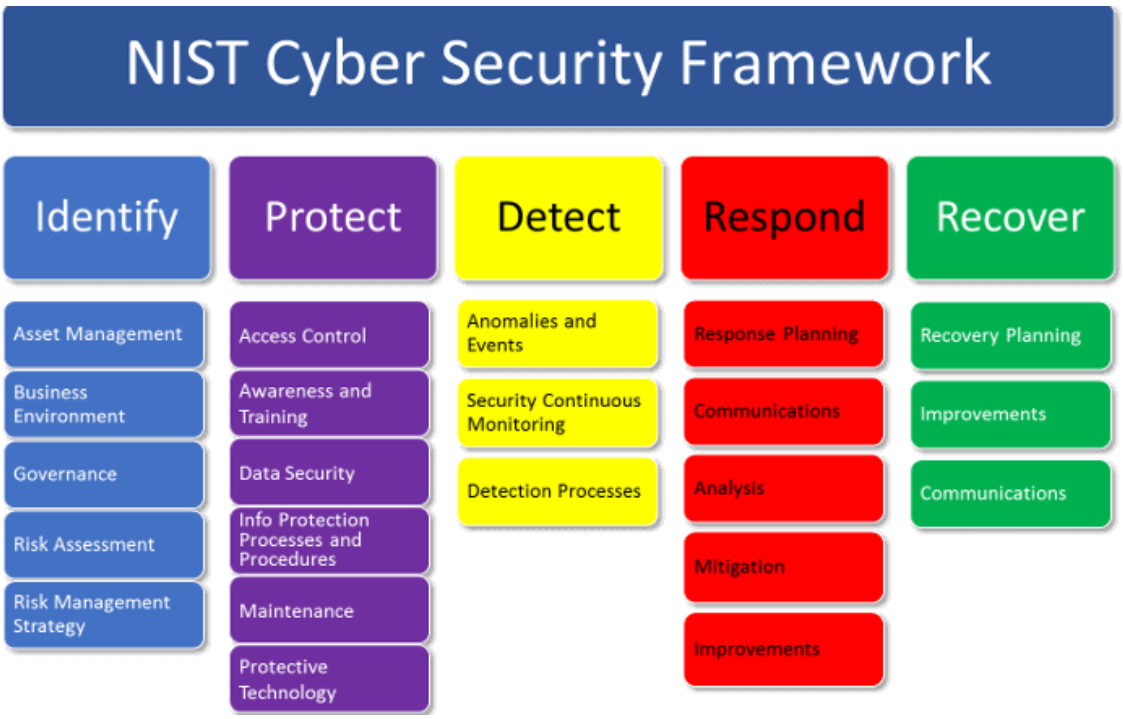

Рис. 1.2 – Nist

Розроблений Національним Інститутом Стандартів та Технологій (NIST) Cybersecurity Framework є іншим впливовим стандартом. Він пропонує систему керування ризиками та заходів забезпечення інформаційної безпеки, що дозволяє організаціям ефективно адаптуватися до зростаючих загроз.

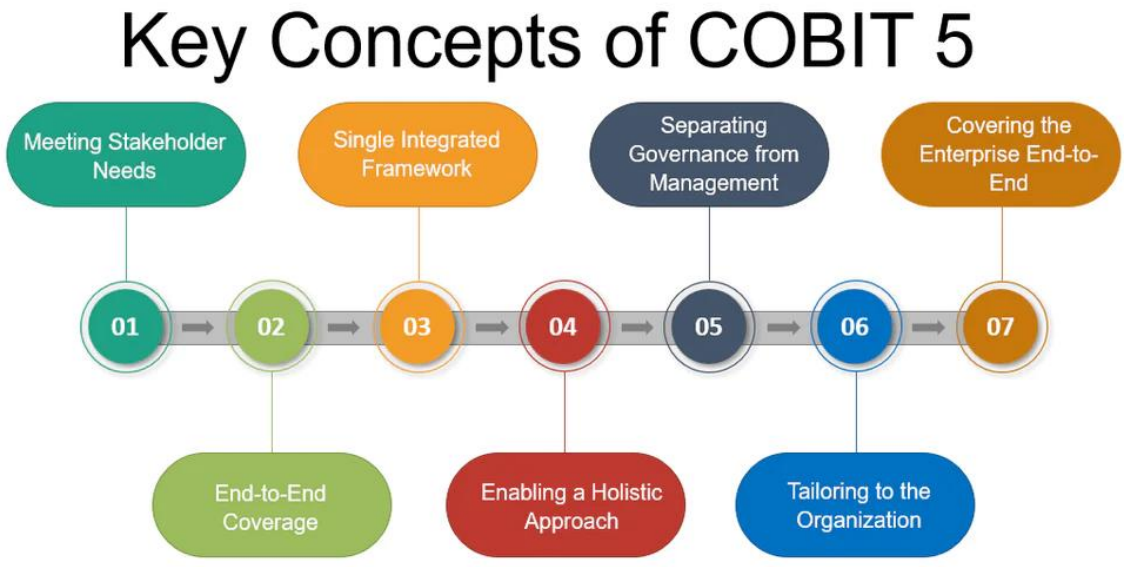

Рис.1.3 – Cobit 5

COBIT - це фреймворк для управління та контролю інформаційними технологіями. Він надає комплексний набір контрольних об'єктів та практик для досягнення бізнес-цілей через ефективне використання інформаційних технологій.

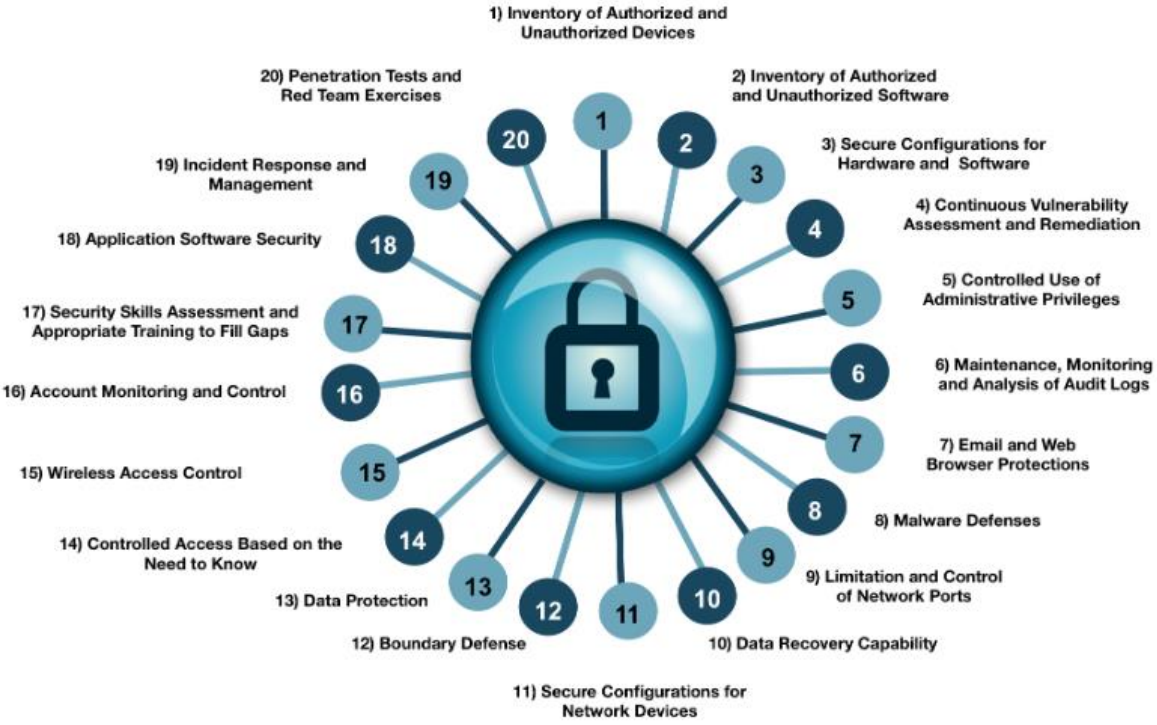

Рис.1.4 – Стандарт CIS

Стандарт Critical Security Controls, розроблений Центром Кібербезпеки (CIS), визначає 20 конкретних заходів безпеки, які є ефективними для запобігання найбільш поширеним атакам та загрозам.

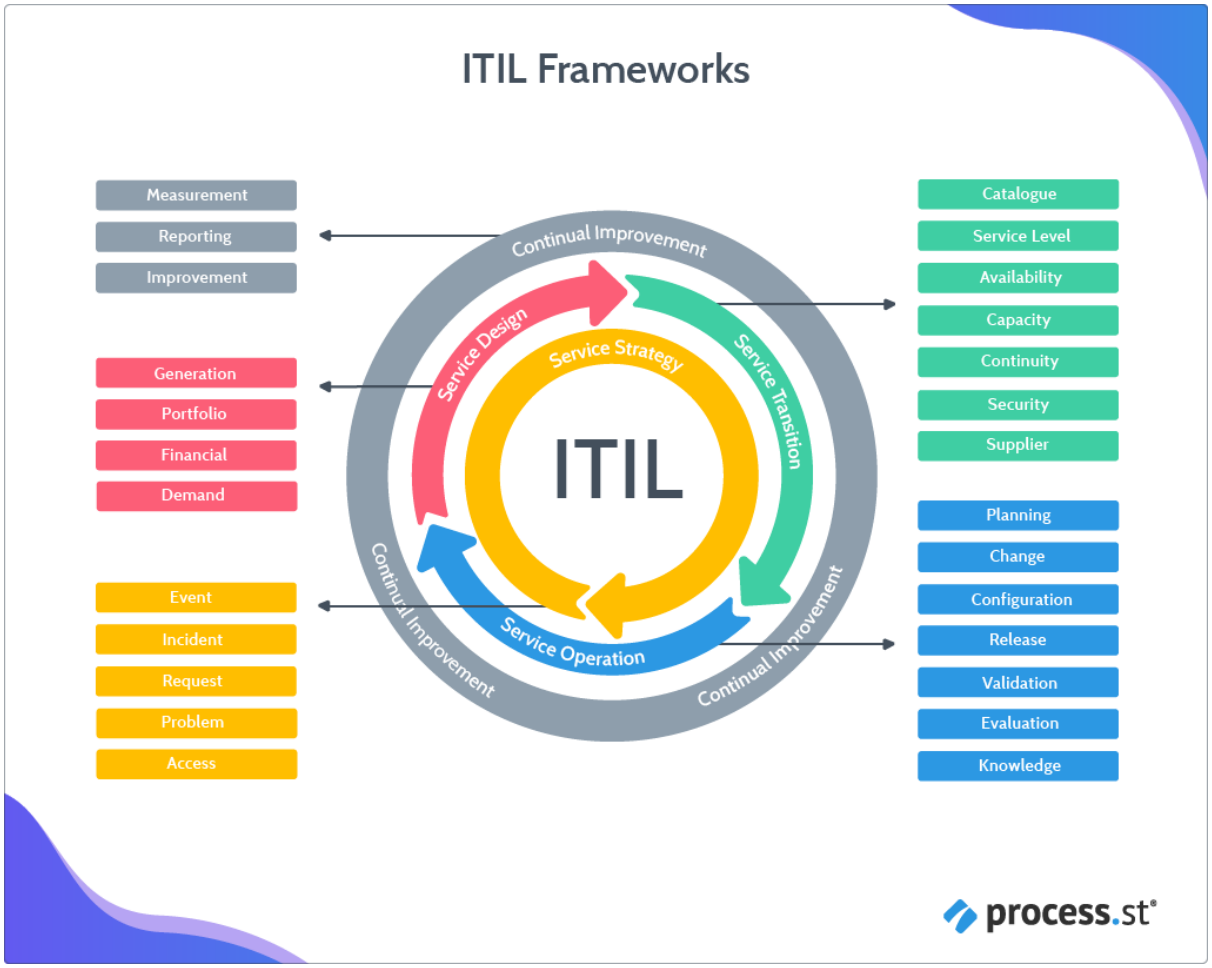

Рис.1.5 – ITIL

ITIL - це набір практик управління обслуговуванням, які включають аспекти безпеки інформації[21]. Він надає структурований підхід до впровадження та управління IT-сервісами, зокрема, з точки зору безпеки.

Часто організації використовують змішаний підхід, комбінуючи елементи різних стандартів та фреймворків відповідно до своїх потреб та конкретностей діяльності. Впровадження стандартів та підходів до інформаційної безпеки дозволяє організаціям створити системний та структурований підхід до захисту інформації. Вони допомагають ідентифікувати, оцінювати та управляти ризиками, а також розробляти та впроваджувати ефективні стратегії безпеки відповідно до визначених стандартів та рекомендацій.

Розуміння інформаційної безпеки в організації є важливою передумовою для розробки та впровадження ефективних стратегій та технічних рішень, спрямованих на захист від сучасних кіберзагроз та збереження цінної інформації для подальшого успішного функціонування організації.

1.2. Загрози та Вразливості у Веб-Середовищі

Загрози у Веб-Середовищі

Кібератаки та Віруси – Загрози цього типу включають в себе різноманітні кібератаки, такі як SQL-ін’єкції, кросс-сайт скриптинг та віруси, спрямовані на вразливості веб-додатків[5].Потенційний витік конфіденційної інформації, порушення цілісності даних, зниження доступності веб-ресурсів.

Фішинг – Атаки фішингу спрямовані на використання соціального інженірингу для отримання конфіденційної інформації, такої як паролі чи особисті дані. Несанкціонований доступ до акаунтів користувачів, ризик витоку конфіденційної інформації.

DDoS-атаки – Атаки з відмовою в обслуговуванні спрямовані на перевантаження веб-сервера запитами, щоб заблокувати доступ користувачів до ресурсу[22]. Зниження доступності веб-сайту, втрати бізнесу через призупинення онлайн-послуг.

Сесійні Атаки – Напад на ідентифікаційні дані сесій користувачів для отримання несанкціонованого доступу. Крадіжка аутентифікаційних даних, несанкціонований доступ до особистих акаунтів.

Вразливості у Веб-Середовищі

Недостатня Валідація та Санітарізація Даних – Введені дані не перевіряються або не очищаються на предмет вірусів, що може призвести до виконання шкідливого коду. Введення шкідливого коду, втрата конфіденційності та цілісності даних.

Неактуальне Віджет-Оновлення – Використання застарілих або неправильно налаштованих віджетів може створити вразливості для атак.*:* Можливість використання застарілих вразливостей для зловмисних цілей.

Несправжні Реєстраційні та Автентифікаційні Механізми – Використання слабких або неякісних механізмів реєстрації та автентифікації може стати причиною неправомірного доступу. Несанкціонований доступ до облікових записів користувачів.

Використання Небезпечних Функцій – Використання функцій, які можуть викликати вразливості, таких як віддалене виконання коду (Remote Code Execution). Зловмисне виконання коду, порушення цілісності системи.

Недостатня Шифрування Даних – Використання слабкого шифрування або його відсутність може призвести до проникнення в конфіденційну інформацію. Витік чутливої інформації, порушення конфіденційності.

Розуміння загроз та вразливостей у веб-середовищі є критично важливим для ефективного захисту інформаційних ресурсів. Впровадження заходів безпеки, таких як регулярне оновлення програмного забезпечення, валідація введених даних та використання сучасних методів аутентифікації, дозволяє зменшити ризик виникнення серйозних інцидентів та забезпечити стабільну безпеку веб-ресурсів.

1.3. Існуючі Методи та Технології Захисту Веб-ресурсів

Методи Шифрування Даних

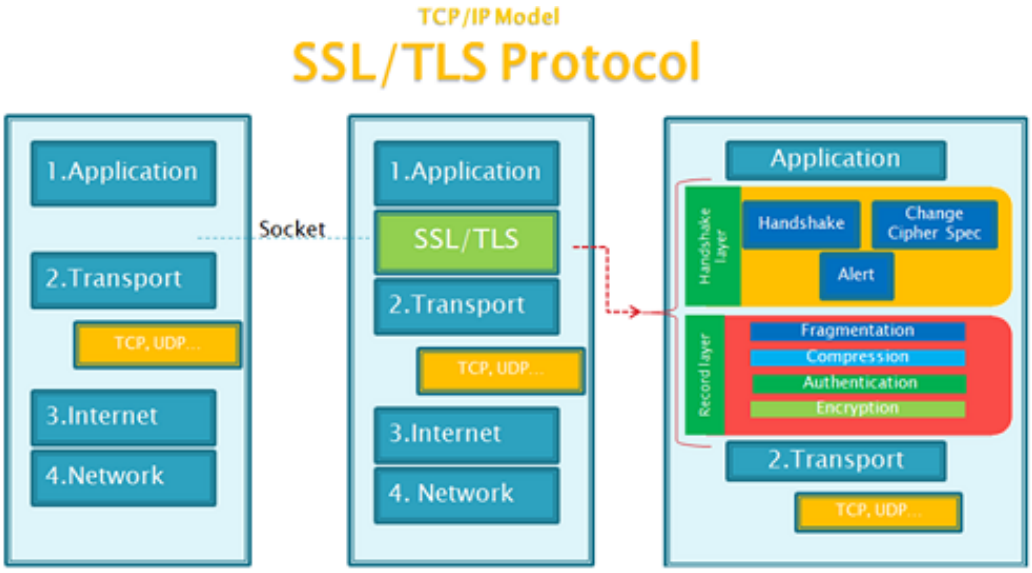

Рис.1.6 – Ssl та Tls протоколи

Secure Socket Layer (SSL) та Transport Layer Security (TLS) є криптографічними протоколами, використовуваними для забезпечення безпеки та конфіденційності під час передачі даних між веб-клієнтом та веб-сервером. SSL/TLS шифрують дані, що передаються між користувачем та сервером, ускладнюючи можливість прослуховування або перехоплення інформації третіми сторонами.

Наслідки:

- **Захищена Передача –** Забезпечення конфіденційності інформації під час передачі, оскільки дані шифруються та залишаються нерозкритими для неповноважених осіб.
- **Уникнення Прослуховування та Перехоплення –** Зменшення ризику прослуховування чи перехоплення даних під час їхньої передачі через мережу.

Шифрування на Рівні Додатків

Шифрування на рівні додатків є стратегією безпеки, яка використовує алгоритми шифрування для захисту конфіденційної інформації під час її зберігання та обробки в базах даних та інших системах[23]. Цей метод спрямований на створення

додаткового шару безпеки, який додається безпосередньо до функціоналу самого додатку.

Додатковий Шар Безпеки – Використання шифрування на рівні додатків дозволяє вбудовувати додаткові заходи безпеки безпосередньо в програмний код додатку. Забезпечення додаткового рівня захисту для конфіденційних даних, які обробляються та зберігаються додатком. Це зменшує ймовірність несанкціонованого доступу та витоку інформації.

Ускладнення Можливостей Зловживання – Шифрування на рівні додатків вносить додаткові бар'єри для зловживання чутливою інформацією користувачами або неправомірними суб'єктами. Зменшення ймовірності зловживання чутливою інформацією, оскільки доступ до даних стає більш обмеженим та контрольованим.

Шифрування на рівні додатків є ефективною стратегією для забезпечення безпеки конфіденційної інформації у веб-додатках та інших системах. Цей метод додає додатковий рівень захисту та сприяє ускладненню можливостей зловживання, забезпечуючи надійний захист чутливих даних.

Методи Виявлення та Захисту від Кібератак

Firewalls

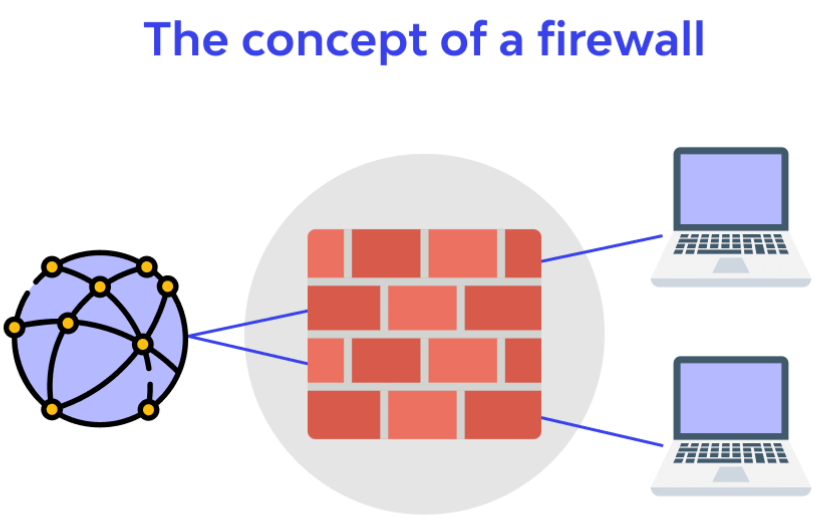

Рис.1.7 – Мережеві брандмауери

Мережеві брандмауери використовуються для контролю трафіку в мережі, фільтрації пакетів даних та запобігання несанкціонованого доступу до системи. Вони служать бар'єром між внутрішньою мережею та зовнішніми мережами, дозволяючи адміністраторам контролювати та моніторити мережевий трафік[6].

- **Захист Мережі –** Зменшення ризику несанкціонованого доступу та захист внутрішніх ресурсів від потенційних атак з мережі.
- **Фільтрація Трафіку** – Забезпечення можливості фільтрації та блокування підозрілого та шкідливого трафіку.

Web Application Firewalls (WAF)

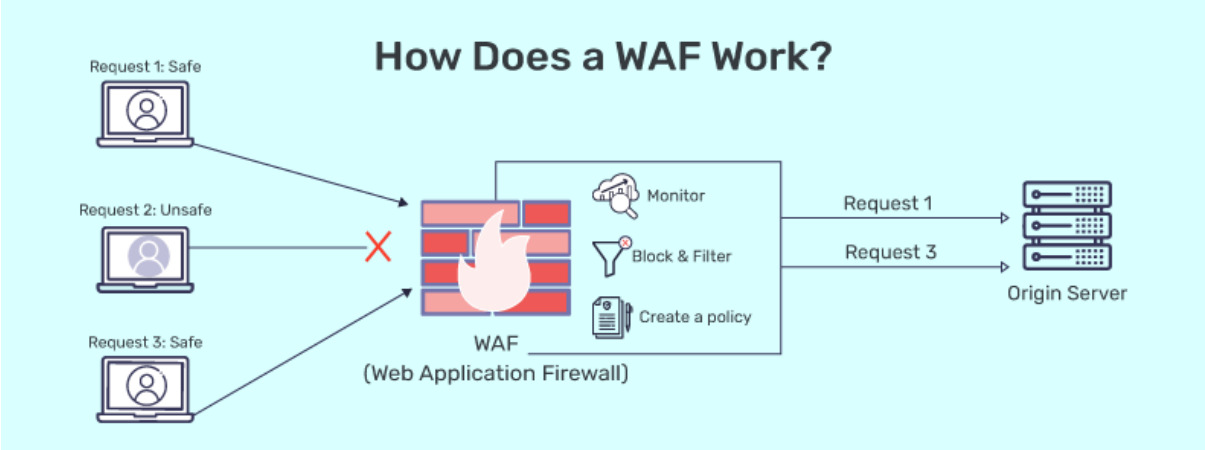

Рис.1.8 – WAF брандмауери

Web Application Firewalls (WAF) є спеціалізованими брандмауерами, спроектованими для захисту веб-додатків від різноманітних атак, таких як SQL-ін'єкції, кросс-сайт скриптинг та інші вразливості[24]. WAF виявляє та блокує потенційно шкідливий трафік, що спрямований на веб-додатки.

- **Зниження Ризику Кібератак на Веб-Додатки** – WAF допомагає ускладнити атакам на веб-додатки, виявляючи та блокуючи аномальний чи потенційно небезпечний трафік.
- **Захист Від Вразливостей** – Ефективний захист від різноманітних атак, спрямованих на вразливості веб-додатків.

Використання мережевих брандмауерів та Web Application Firewalls є важливими елементами стратегії кібербезпеки. Ці методи допомагають утримувати несанкціонованих користувачів і шкідливий трафік подалеку, забезпечуючи ефективний захист мережі та веб-додатків.

Методи Безпеки Систем Аутентифікації та Авторизації

Двофакторна аутентифікація є ефективною стратегією безпеки, використовуючи два різні етапи для підтвердження ідентифікації користувача.

Зазвичай це включає в себе введення пароля разом з одноразовим кодом, який надходить на мобільний пристрій. Цей додатковий етап аутентифікації збільшує безпеку системи та ускладнює завдання несанкціонованим особам, які намагаються отримати доступ до системи.

Ролева модель авторизації визначає та обмежує права доступу користувачів в залежності від їхньої ролі в системі. Кожній ролі призначаються конкретні привілеї та рівні доступу. Це сприяє мінімізації ризику несанкціонованого доступу та зловживання правами, а також ефективному управлінню правами користувачів[7].

Використання систем моніторингу є важливою частиною стратегії кібербезпеки. Ці системи постійно відстежують трафік, події та поведінку, дозволяючи вчасно виявляти потенційні кіберзагрози та вживати відповідних заходів безпеки.

Регулярні аудити безпеки є важливою складовою безпекової стратегії. Під час аудитів виконується перевірка та аналіз системи для виявлення вразливостей та неправомірного використання. Це допомагає утримувати високий рівень безпеки та уникнення повторення інцидентів.

Ці методи взаємодіють для створення комплексного заходу безпеки, забезпечуючи ефективний захист від різноманітних кіберзагроз та забезпечуючи стійкість систем до потенційних атак.

Існуючі методи та технології захисту веб-ресурсів надають комплексний підхід до забезпечення конфіденційності, цілісності та доступності даних[25]. Їх використання сприяє створенню надійних та стійких веб-систем, зменшуючи ризики кіберзагроз та забезпечуючи безпеку для користувачів та організацій.

1.4. Порівняльний аналіз методів і технологій

У даному розділі проводиться порівняльний аналіз різних методів і технологій, використовуваних для захисту Web-ресурсів в інформаційних системах організацій.

Методи Шифрування Даних – Порівняльний аналіз SSL/TLS протоколів та шифрування на рівні додатків дозволяє визначити ефективність та придатність кожного методу в забезпеченні конфіденційності інформації. Серед переваг можна виділити надійність передачі та додатковий рівень безпеки для зберігання даних.

Методи Виявлення та Захисту від Кібератак – Порівняльний аналіз firewalls та Web Application Firewalls допомагає визначити їхню здатність контролювати трафік та запобігати атакам на різних рівнях мережі. Оцінка ефективності цих методів визначає рівень захисту веб-додатків та загальної мережі[8].

Методи Безпеки Систем Аутентифікації та Авторизації – Порівняння двофакторної аутентифікації та рольової моделі авторизації дозволяє визначити оптимальний спосіб ідентифікації користувачів та контролю доступу. Застосування обох методів може забезпечити високий рівень безпеки в різних аспектах інформаційної системи.

Моніторинг та Аудит Безпеки: Порівняння систем моніторингу та аудиту безпеки визначає їхню здатність вчасно виявляти та реагувати на потенційні загрози. Оптимальне поєднання цих методів може гарантувати стійкість системи до різноманітних кіберзагроз.

Таблиця 1.1 – Порівняння методів та технологій

Аспекти Захисту	**SSL/TLS протоколи**	**Шифрування на рівні додатків**	**Firewalls**	**Web Application Firewalls (WAF)**	**Двофакторна Аутентифікація**	**Ролева Модель Авторизації**	**Системи Моніторингу Захисту Інформації**	**Аудит Безпеки**
Ефективність	Висока	Висока	Висока	Висока	Висока	Висока	Висока	Висока
Конфіденційність	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена

Аспекти Захисту	SSL/TLS протоколи	Шифрування на рівні додатків	Firewalls	Web Application Firewalls (WAF)	Двофакторна Аутентифікація	Ролева Модель Авторизації	Системи Моніторингу Захисту Інформації	Аудит Безпеки
Цілісність	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена
Доступність	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена	Забезпечена
Запобігання Атакам	Так	Так	Так	Так	Так	Так	Так	Так
Моніторинг та Реагування	Частково забезпечено	Частково забезпечено	Частково	Частково	Так	Частково	Так	Так

Висновки з порівняльного аналізу

Проведений аналіз методів і технологій захисту Web-ресурсів в інформаційних системах організацій дозволяє робити наступні висновки:

1. **Ефективність та Забезпеченість**
   - Усі розглянуті методи та технології демонструють високий рівень ефективності та забезпеченість конфіденційності, цілісності та доступності інформації.
2. **Запобігання Атакам та Моніторинг**
   - Методи шифрування даних, двофакторна аутентифікація та системи моніторингу забезпечують високий рівень захисту та реагування на потенційні загрози.
3. **Рольова Модель Авторизації та Аудит Безпеки**

- Рольова модель авторизації та аудит безпеки є ефективними засобами для контролю доступу та підтримки безпеки на високому рівні.

При виборі методів та технологій для захисту Web-ресурсів, оптимальним підходом є комплексне використання різних засобів для досягнення високого рівня інформаційної безпеки. Забезпечення конфіденційності, цілісності та доступності інформації вимагає інтеграції різноманітних технічних та організаційних заходів, а також постійного моніторингу та адаптації до зростаючих кіберзагроз.

Висновки до розділу

Перший розділ визначає ключові поняття, методи та технології, які становлять основу для подальших досліджень та розробки системи захисту Web-ресурсів в інформаційних системах організацій.

Визначено, що інформаційна безпека є комплексним заходом для захисту конфіденційності, цілісності та доступності інформації. Забезпечення цих аспектів є важливим завданням для забезпечення надійності та безпеки веб-ресурсів.

Визначено різноманітні загрози, з якими стикаються веб-середовища, включаючи кібератаки, витоки даних та внутрішні порушення безпеки. Розуміння цих ризиків є ключовим для розробки ефективних методів захисту.

Проведено детальний аналіз методів шифрування, методів виявлення та захисту від кібератак, аутентифікації та авторизації, а також стандартів та підходів до інформаційної безпеки. Визначено їхню ефективність та придатність для використання в організаційних інформаційних системах.

Порівняльний аналіз відобразив високу ефективність різних методів і технологій захисту, а також підкреслив необхідність комплексного підходу до захисту веб-ресурсів. Визначено, що оптимальна система захисту має використовувати комбінацію різних засобів для максимальної ефективності.

Розділ створив теоретичну базу для подальших досліджень та розробки технологічних рішень у сфері захисту Web-ресурсів в інформаційних системах організацій. Розуміння ключових концепцій і методів є важливим кроком у створенні надійних та ефективних систем інформаційної безпеки.

РОЗДІЛ 2. ОБГРУНТУВАННЯ МЕТОДІВ ДОСЛІДЖЕННЯ

2.1. Вибір методів дослідження

Аналіз Літературних Джерел

Для реалізації дослідження щодо технологій захисту Web-ресурсів в інформаційних системах організацій обрано метод аналізу літературних джерел[9]. Цей підхід передбачає систематичне оглядання та аналіз наукових публікацій, підручників, технічної літератури та інших джерел для отримання глибокого розуміння теми дослідження.

Широкий Обсяг Інформації – Літературні джерела містять різноманітні підходи, концепції та технології щодо захисту Web-ресурсів. Аналіз цих джерел дозволить охопити широкий спектр інформації.

Систематизація Знань – Метод дозволяє систематизувати існуючі знання, виокремити ключові поняття та тенденції, що сприятиме створенню концептуальної бази для подальших досліджень.

Визначення Ключових Аспектів – Аналіз літературних джерел допоможе визначити ключові аспекти технологій захисту Web-ресурсів, на які слід звернути увагу в рамках подальших етапів дослідження.

Актуальність та Новизна – Спостереження за останніми публікаціями дозволить визначити актуальні та нові тенденції в галузі кібербезпеки та захисту інформації.

Метод Критичного Аналізу – Цей метод включає критичний підхід до оцінки надійності та об'єктивності джерел, що гарантує високу якість інформації.

Аналіз літературних джерел сприятиме глибокому розумінню сучасних технологій захисту Web-ресурсів та визначенню напрямків подальших досліджень у цій області.

Емпіричні Дослідження

Один із ключових методів, що використовується в рамках даного дослідження - це емпіричні дослідження, включаючи практичне тестування технологічних рішень. Цей метод дозволяє здобути об'єктивні дані про реальні можливості та придатність різних технологій захисту Web-ресурсів.

Оцінка Реальної Ефективності – Емпіричні дослідження надають можливість перевірити технології в реальних умовах та визначити їхню ефективність під час різних сценаріїв використання.

Перевірка Придатності – Практичне тестування технологій дозволить визначити, наскільки вони придатні до застосування в конкретних умовах організації.

Виявлення Недоліків та Переваг – Емпіричні дослідження дозволяють ідентифікувати як потенційні недоліки, так і переваги технологічних рішень, що є важливою інформацією для подальшого вибору та вдосконалення заходів захисту.

Адаптація до Конкретних Сценаріїв – Емпіричні дослідження дозволяють адаптувати технології до конкретних потреб та сценаріїв використання організації.

Можливість Контролю – Практичне тестування дозволяє здійснювати контроль над умовами експерименту, забезпечуючи точність та достовірність результатів.

Емпіричні дослідження нададуть конкретні дані та висновки про ефективність вибраних технологій, а також допоможуть визначити їхню придатність до використання в реальних умовах інформаційної системи організації.

Кейс-стаді

Одним з важливих методів дослідження є вивчення кейс-стаді успішних реалізацій захисту Web-ресурсів у схожих організаціях. Цей метод дозволить

врахувати практичний досвід та здобуті висновки щодо оптимальних стратегій захисту і використовувати їх у контексті даного дослідження.

Практичний Досвід Успіху – Вивчення кейс-стаді успішних реалізацій дозволить отримати практичний досвід та інсайти з організацій, які вже здійснили успішну імплементацію заходів з захисту Web-ресурсів.

Адаптація Стратегій – Здобуття висновків з кейс-стаді дозволить адаптувати стратегії та технології захисту до конкретних умов і вимог інформаційної системи організації.

Зменшення Ризиків – Вивчення випадків успішної імплементації допоможе зменшити ризики та уникнути поширених помилок при впровадженні заходів з кібербезпеки.

Спільнота Практикуючих – Отримання відомостей з кейс-стаді сприятиме взаємодії з іншими організаціями та експертами в галузі, що може призвести до обміну кращими практиками.

Швидкі Результати – Вивчення кейсів дозволяє швидше використовувати успішні стратегії та технології, що може позитивно позначитися на швидкості впровадження заходів з захисту.

Вивчення кейс-стаді принесе конкретний практичний досвід та рекомендації для вдосконалення стратегій захисту Web-ресурсів в інформаційній системі організації.

Моделювання та Симуляції

Один із ключових методів, що використовується в даному дослідженні, - це математичне моделювання та симуляції[10]. Цей метод дозволить віртуально тестувати різні стратегії та сценарії захисту Web-ресурсів, що сприятиме визначенню оптимальних рішень та ефективних заходів кібербезпеки.

Віртуальне Тестування – Математичне моделювання та симуляції дозволяють віртуально тестувати заходи кібербезпеки без реального впровадження, що зменшує ризики та витрати.

Оптимізація Стратегій – Моделювання дозволяє провести оптимізацію стратегій та сценаріїв захисту, враховуючи різні умови та загрози.

Аналіз Ефективності – Використання математичних моделей дозволяє аналізувати ефективність заходів захисту в різних сценаріях та визначати їхню придатність.

Економія Часу та Ресурсів – Симуляції дають можливість швидко отримати результати та визначити оптимальні рішення без великих витрат часу та ресурсів.

Експерименти з Різними Сценаріями – Моделювання дозволяє провести експерименти з різними сценаріями кібератак та визначити, як ефективно заходи захисту протистоять різним загрозам.

Математичне моделювання та симуляції принесуть конкретні дані та висновки, що допоможуть визначити оптимальні стратегії та заходи захисту Web-ресурсів в інформаційній системі організації.

Збір та Аналіз Даних

Для отримання об'єктивних та науково підтверджених результатів щодо ефективності та придатності обраних методів захисту Web-ресурсів в інформаційній системі організації використовується систематичний збір та аналіз даних, включаючи статистичні методи.

Об'єктивні Результати – Систематичний збір даних дозволяє отримати об'єктивні результати, які можна науково аналізувати та порівнювати.

Широкий Обсяг Інформації – Збір різноманітних даних, таких як логи, метрики ефективності та інші, надає широкий обсяг інформації для комплексного аналізу.

Статистичні Методи – Використання статистичних методів дозволяє проводити об'єктивний аналіз та знаходити кореляції та тенденції у зібраних даних.

Інформаційна Підтримка Рішень – Науковий аналіз даних надає підстави для прийняття інформованих рішень щодо вибору та вдосконалення методів захисту.

Підтвердження Гіпотез – Збір та аналіз даних допомагає підтверджувати чи спростовувати гіпотези, що стосуються ефективності заходів кібербезпеки.

Систематичний збір та аналіз даних забезпечать об'єктивні результати, які визначать ефективність та придатність обраних методів захисту Web-ресурсів в інформаційній системі організації.

Системний Підхід

Врахування системного підходу до дослідження технологій захисту Web-ресурсів в інформаційній системі організації визначається необхідністю здійснення комплексного аналізу взаємодії та впливу різних компонентів системи захисту[11].

Комплексний Аналіз – Системний підхід дозволяє розглядати систему захисту як цілісну структуру, вивчаючи взаємозв'язки між її компонентами.

Взаємодія Компонентів – Аналіз впливу та взаємодії різних компонентів, таких як методи шифрування, системи аутентифікації та інші, дозволяє визначити їхню ефективність в контексті цілої системи.

Ідентифікація Зв'язків – Врахування системних зв'язків дозволяє виявити можливі ризики та прогалини в системі захисту.

Охоплення Всіх Аспектів – Системний підхід охоплює всі аспекти захисту, включаючи технічні, організаційні та людські фактори.

Цілісність Результатів – Аналіз системної взаємодії забезпечить цілісні результати, які враховують всі аспекти кібербезпеки.

Використання системного підходу дозволить отримати комплексний аналіз ефективності та взаємодії різних компонентів системи захисту Web-ресурсів в інформаційній системі організації.

Обрані методи дослідження спрямовані на створення комплексного та повного об'єктивного обґрунтування розроблених технологій захисту Web-ресурсів в інформаційних системах організацій.

2.2. Опис використовуваних інструментів

Інструменти Моніторингу та Аналізу

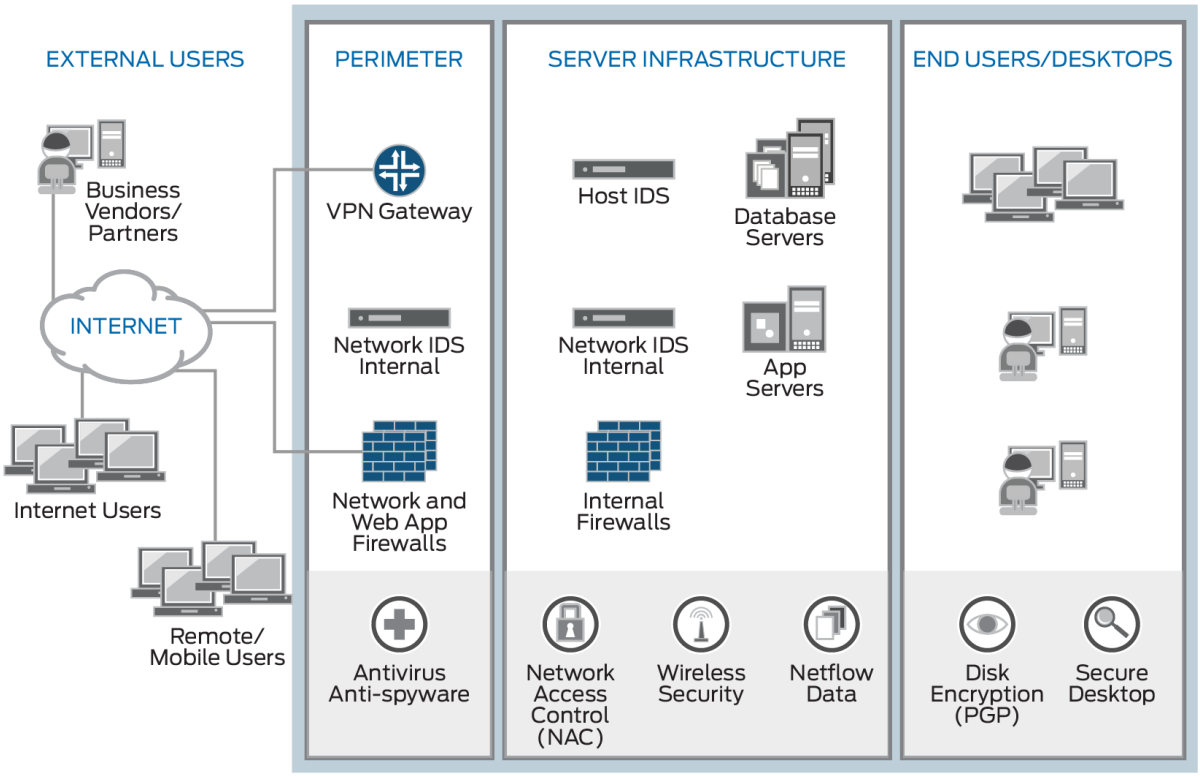

Рис.2.1 – SIEM інструменти

1. **Системи Моніторингу Захисту Інформації** виявляються важливим інструментом у дослідженні технологій захисту Web-ресурсів. SIEM використовується для комплексного збору, аналізу та інтерпретації журналів подій, що надходять з

різних джерел у системі[12]. Цей інструмент надає можливість оперативно виявляти аномалії у поведінці системи та ідентифікувати потенційні загрози безпеки. Аналіз журналів дозволяє стежити за діяльністю користувачів та ідентифікувати несподівані події, що можуть свідчити про можливі атаки чи порушення безпеки.

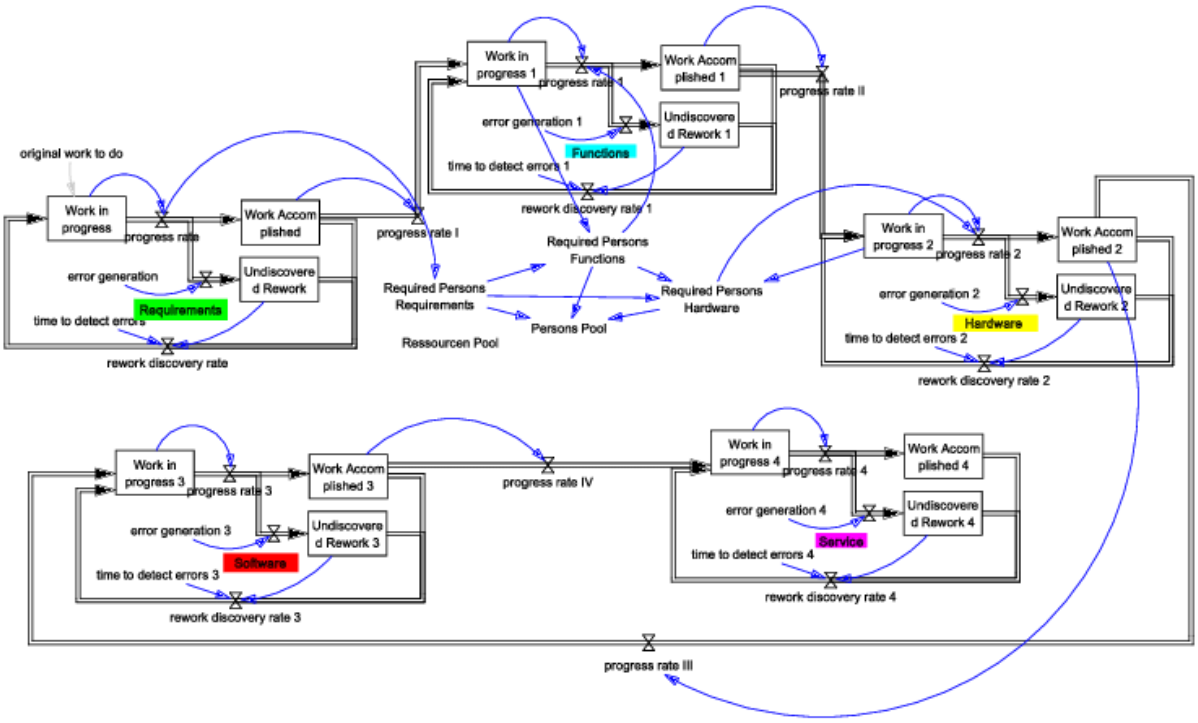

Рис.2.2 – Інструменти System Dynamics

2. **Інструменти Системного Аналізу** – Дослідження включає в себе використання інструментів системного аналізу, таких як MatLab чи System Dynamics. Ці інструменти використовуються для математичного моделювання та аналізу взаємодії елементів системи захисту. Вони дозволяють створювати складні математичні моделі, які охоплюють різноманітні аспекти безпеки Web-ресурсів. Це важливо для здійснення комплексного аналізу та визначення оптимальних стратегій захисту, орієнтованих на усунення виявлених аномалій та вдосконалення системи безпеки у цілому.

Інструменти Штучного Інтелекту та Кібераналітики

1. **Алгоритми Машинного Навчання** – В контексті дослідження технологій захисту Web-ресурсів, використання алгоритмів машинного навчання виявляється ключовим елементом. Ці алгоритми застосовуються для аналізу великого обсягу даних, що стосуються діяльності користувачів та системи безпеки[13]. Вони дозволяють виявляти складні патерни у поведінці користувачів, а також ідентифікувати надзвичайні події та аномалії, які можуть свідчити про потенційні загрози безпеці.

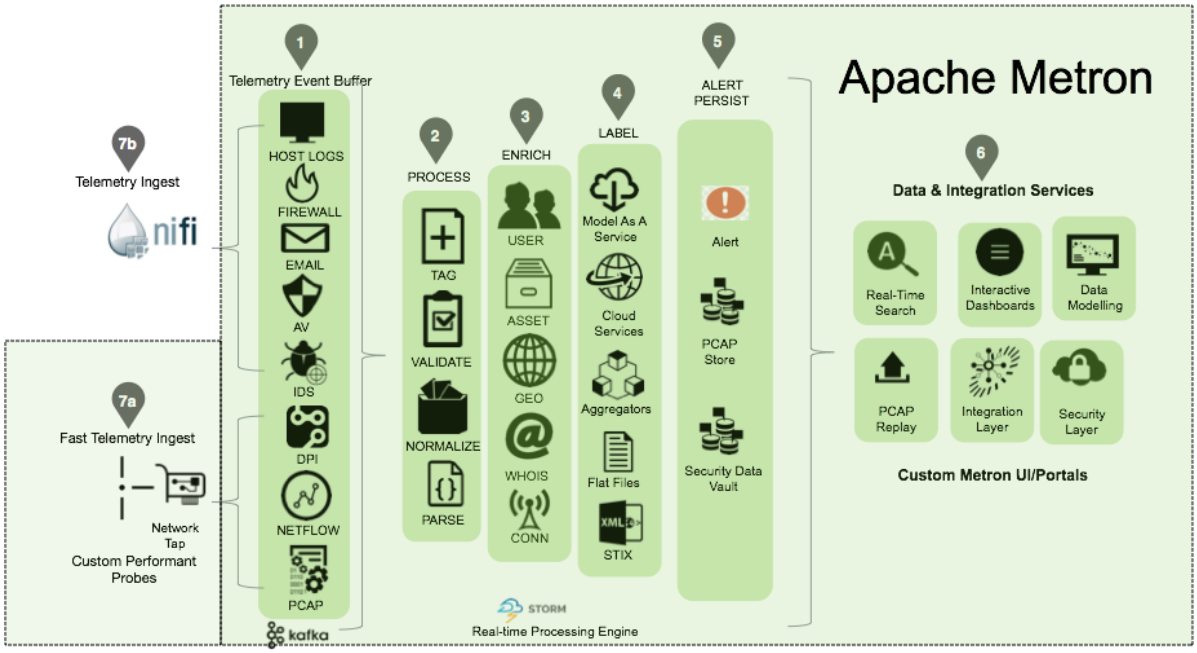

Рис.2.3 – Apache Metron

2. **Інструменти Кібераналітики** – Вивчення технологій захисту Web-ресурсів включає використання інструментів кібераналітики, таких як Apache Metron. Ці платформи розроблені для збору та аналізу даних, пов'язаних з кібербезпекою. Apache Metron, зокрема, надає засоби для виявлення потенційних загроз та реагування на них. Інтеграція таких інструментів дозволяє ефективно аналізувати дані щодо безпеки, реагувати на інциденти та вдосконалювати заходи захисту Web-ресурсів.

Інструменти Тестування Та Вразливостей

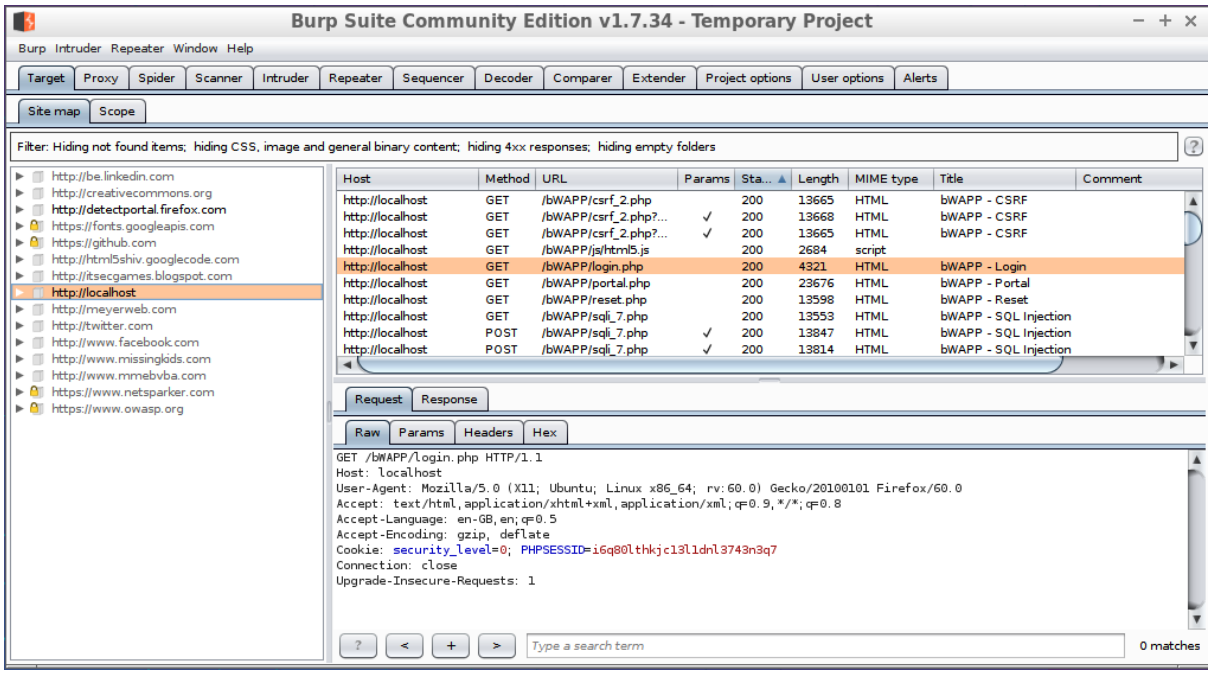

Рис.2.4 – Burp Suite

1. **Burp Suite –** Burp Suite є невід'ємним інструментом для виявлення та тестування вразливостей в веб-додатках. Цей набір інструментів дозволяє здійснювати аналіз безпеки коду та інфраструктури веб-сайту. За допомогою Burp Suite можна виявити та вивчити потенційні слабкі місця, які можуть бути використані для несанкціонованого доступу чи атак.

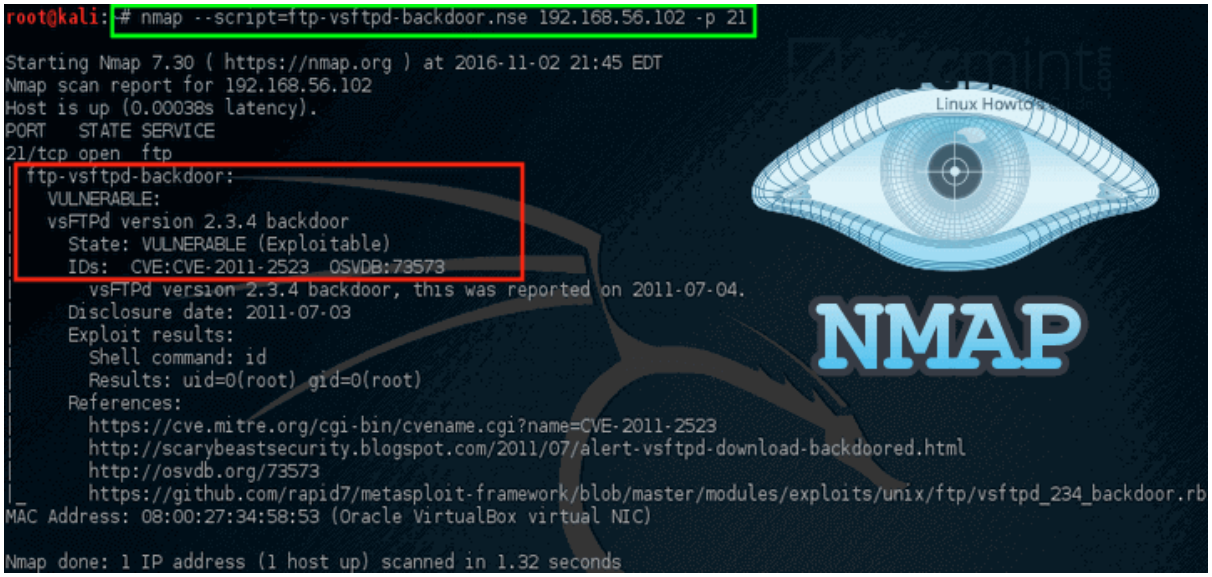

Рис.2.5 – NMAP

2. **Nmap** – Nmap є потужним інструментом для сканування мережі та виявлення відкритих портів та служб. Використання Nmap дозволяє ідентифікувати можливі точки входу для атак та оцінювати рівень доступності системи для потенційних загроз. Цей інструмент є незамінною складовою для аудиту безпеки та виявлення вразливостей в мережевих системах.

2.3. Визначення критеріїв оцінки ефективності технологій захисту

Для об'єктивної оцінки ефективності технологій захисту Web-ресурсів в інформаційній системі організації визначені ключові критерії, які враховують різні аспекти їхньої роботи[14]. Нижче наведено детальний опис критеріїв оцінки:

1. **Інтеграція з існуючими системами –** Оцінюється можливість технологій захисту ефективно інтегруватися з існуючими інформаційними системами організації. Цей критерій визначає, наскільки легко та безперервно нові заходи безпеки можуть бути впроваджені в існуючий інфраструктурний стек.

2. **Рівень надійності та стійкості –** Оцінка технологій включає аналіз їхньої стійкості до різних видів атак та здатність витримувати високе навантаження без втрати продуктивності. Також враховується швидкість виявлення та реагування на потенційні загрози.

3. **Вартість реалізації та утримання –** Критерій вартості оцінює ефективність технологій з точки зору витрат на їхню реалізацію, впровадження та подальше утримання. Враховуються як прямі витрати, так і можливі затрати на навчання персоналу та оновлення.

4. **Зручність у використанні та адмініструванні –** Оцінюється інтуїтивність інтерфейсу, наявність документації та підтримка з боку виробника. Цей критерій визначає, наскільки легко адміністраторам та іншому персоналу можна використовувати та налаштовувати дані технології.

5. **Відповідність стандартам безпеки –** Критерій включає в себе перевірку відповідності технологій визнаним стандартам безпеки, таким як ISO/IEC 27001, NIST Cybersecurity Framework тощо. Це забезпечує додаткову гарантію високого рівня безпеки.

6. **Інноваційність та майбутні перспективи –** Оцінка можливостей для майбутнього розвитку та оновлення технологій. Враховується, наскільки інноваційними є заходи безпеки та як вони можуть враховувати майбутні тренди у сфері кібербезпеки.

Ці критерії допомагають об'єктивно оцінити ефективність технологій захисту Web-ресурсів, враховуючи різноманітні аспекти їхнього впровадження та функціонування.

Висновки до розділу

У цьому розділі було детально розглянуто та обгрунтовано методи дослідження, які будуть використані для вивчення технологій захисту Web-ресурсів в інформаційній системі організації. Вибір цих методів був здійснений з урахуванням потреб дослідження та специфіки проблеми.

Обрані методи дозволять отримати різнобічне та об'єктивне розуміння ефективності технологій захисту. Теоретичний аналіз, літературний огляд, емпіричні дослідження та аналіз кейс-стаді нададуть повністю обґрунтовану основу для подальшого дослідження.

У розділі були визначені та описані інструменти, які будуть використані під час дослідження. Це включає системи моніторингу захисту інформації, інструменти системного аналізу, інструменти штучного інтелекту та кібераналітики, інструменти тестування та виявлення вразливостей. Використання цих інструментів дозволить отримати повний обсяг інформації про стан безпеки та ефективність застосовуваних технологій.

Визначені критерії надають об'єктивну основу для оцінки ефективності технологій захисту. Їхнє ретельне врахування дозволить здійснити комплексну оцінку та зробити обґрунтовані висновки щодо використання конкретних технологій в інформаційній системі організації.

Завдяки аналізу та обгрунтуванню обраних методів дослідження та визначенню критеріїв їх ефективності, розділ надає чіткий план для подальшого дослідження технологій захисту Web-ресурсів в інформаційній системі організації. Цей підхід забезпечить комплексне та об'єктивне розглядання питань кібербезпеки та сприятиме отриманню високоякісних результатів дослідження.

РОЗДІЛ 3. АНАЛІЗ ПОТОЧНОГО СТАНУ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЙ

3.1. Опис інформаційних систем

Аналіз інформаційних систем організацій є стратегічно важливим етапом для визначення їхньої поточної кібербезпеки та виявлення можливих недоліків. В даному розділі проведемо детальний огляд інформаційних систем, що використовуються в організаціях.

Фінансові Інформаційні Системи

Для детального аналізу фінансових інформаційних систем обрано платформу **SAP S/4HANA Finance**.

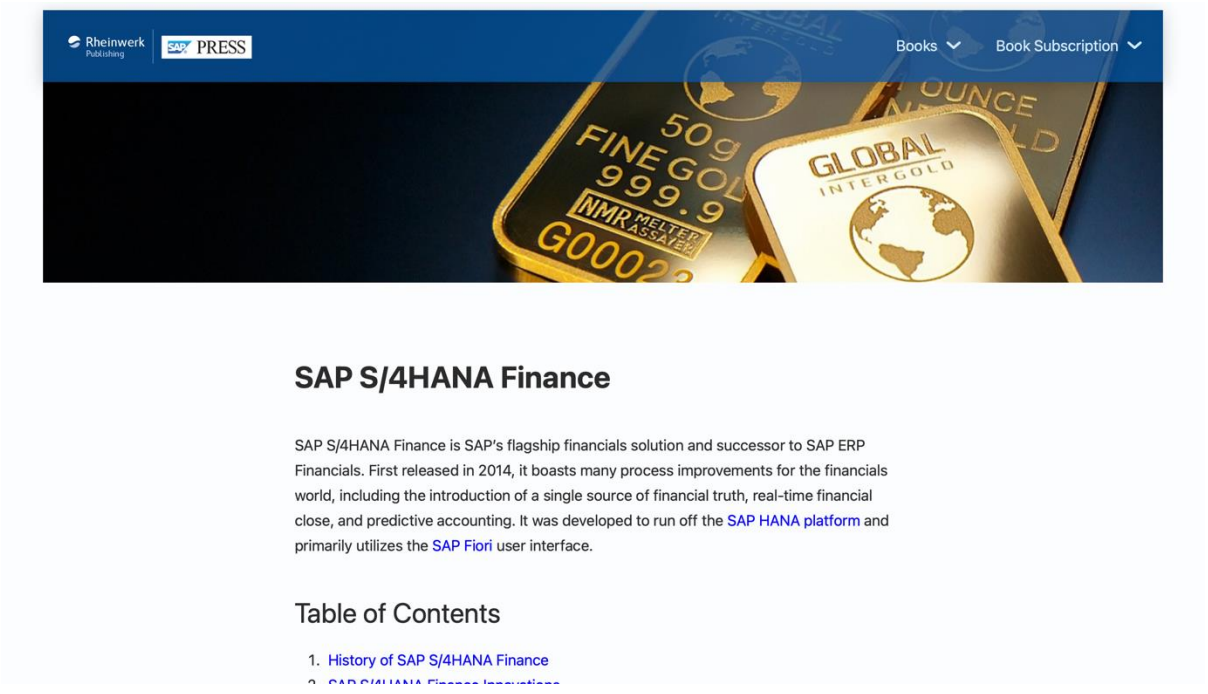

Рис.3.1 – Платформа Sap S

Вхідні дані аналізу поточного стану

Аналіз проводиться на основі інформації, що стосується функціональності та характеристик **SAP S/4HANA Finance**, отриманої з документації, офіційних джерел, та відгуків користувачів.

Елементи аналізу поточного стану

Організаційна структура

SAP S/4HANA Finance – Платформа розроблена для компаній різних галузей та розмірів.

Специфікації – Інтеграція з різними системами ентерпрайзу, забезпечення ефективного використання у великих корпораціях.

Можливості та процеси

Можливості – Аналітика в реальному часі, оптимізація фінансових процесів.

Процеси – Автоматизована обробка операцій, ефективна аналітика ключових показників.

Технології та інфраструктура

Інфраструктура – Хмарний та локальний варіанти розгортання.

Технології – Використання технології SAP HANA для обробки великого обсягу даних в реальному часі.

Політика (Policies)

Політика безпеки – Захист конфіденційної інформації, регулярні оновлення безпеки.

Архітектура бізнесу (Business Architecture)

Орієнтація на користувача – Інтуїтивний інтерфейс для фінансових аналітиків та керівників.

Проведений аналіз фінансової інформаційної системи SAP S/4HANA Finance показує, що платформа володіє широким спектром можливостей, зокрема аналітикою в реальному часі та ефективним управлінням фінансовими процесами. Однак вибір платформи повинен бути обдуманим та залежати від конкретних потреб організації.

ERP-Системи

Для детального аналізу ERP-систем обрано платформу **Microsoft Dynamics 365**.

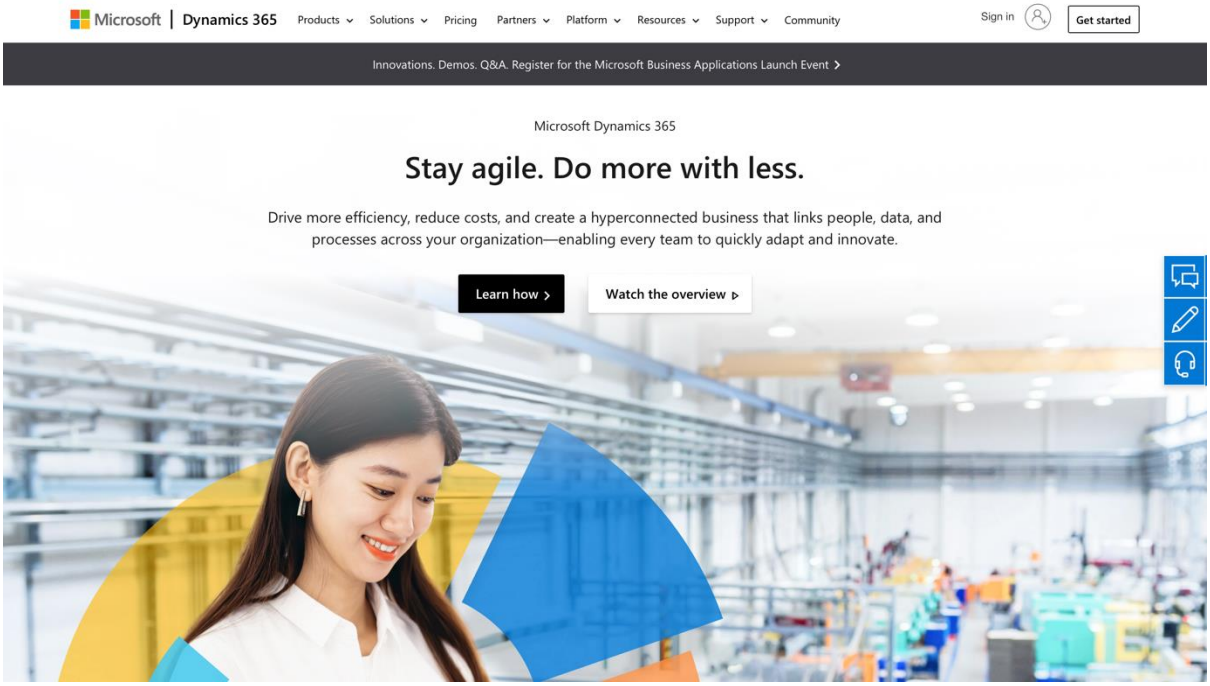

Рис.3.2 – Платформа Microsoft 365

Вхідні дані аналізу поточного стану

Аналіз проводиться на основі інформації, що стосується функціональності та характеристик **Microsoft Dynamics 365**, отриманої з документації, офіційних джерел, та відгуків користувачів.

Елементи аналізу поточного стану

Організаційна структура

Microsoft Dynamics 365 – ERP-платформа призначена для управління виробництвом, постачанням, та фінансами.

Специфікації – *І*нтеграція з іншими продуктами Microsoft та платформами сторонніх розробників.

Можливості та процеси

Можливості – Управління виробництвом та логістикою, аналітика для прийняття стратегічних рішень.

Процеси – Автоматизація операцій, управління відносинами з клієнтами, аналіз даних.

Технології та інфраструктура

Інфраструктура – Хмарний розгортання за допомогою Azure.

Технології – Використання технологій Microsoft для забезпечення ефективної роботи.

Політика (Policies)

Політика безпеки – Відповідає стандартам безпеки даних, регулярні оновлення безпеки.

Архітектура бізнесу (Business Architecture)

Орієнтація на користувача – Інтерактивний інтерфейс для користувачів різних рівнів.

Аналіз ERP-системи Microsoft Dynamics 365 свідчить про її широкий функціонал та можливості для управління виробництвом і фінансами. Організації мають змогу ефективно використовувати дану платформу, враховуючи їхні конкретні потреби та стратегії.

CRM-Системи

Для детального аналізу CRM-системи обрано платформу **Salesforce**.

Рис.3.3 – Платформа Salesforce

Вхідні дані аналізу поточного стану

Аналіз проводиться на основі інформації, що стосується функціональності та характеристик **Salesforce**, отриманої з документації, офіційних джерел, та відгуків користувачів.

Елементи аналізу поточного стану

Організаційна структура

Salesforce – CRM-платформа для управління відносинами з клієнтами та оптимізації продажів.

Специфікації – Інтеграція з електронною поштою, системами телефонії та системами зберігання контактів.

Можливості та процеси

Можливості – Автоматизація маркетингу, управління продажами та послугами.

Процеси – Взаємодія з клієнтами, відстеження продажів, аналіз даних.

Технології та інфраструктура

Інфраструктура – Хмарне розгортання за допомогою власних серверів Salesforce.

Технології – Використання технологій штучного інтелекту для аналізу даних.

Політика (Policies)

Політика безпеки – Високі стандарти безпеки та шифрування для захисту конфіденційної інформації.

Архітектура бізнесу (Business Architecture)

Орієнтація на клієнт – Інтерактивна CRM-платформа для взаємодії з клієнтами та покращення обслуговування.

Аналіз CRM-системи Salesforce підтверджує її ефективність у веденні відносин з клієнтами та оптимізації процесів продажів. Організації можуть використовувати Salesforce для вдосконалення комунікації з клієнтами та збільшення обсягу продажів.

HR-Системи

Для детального аналізу HR-системи обрано платформу **Workday**.

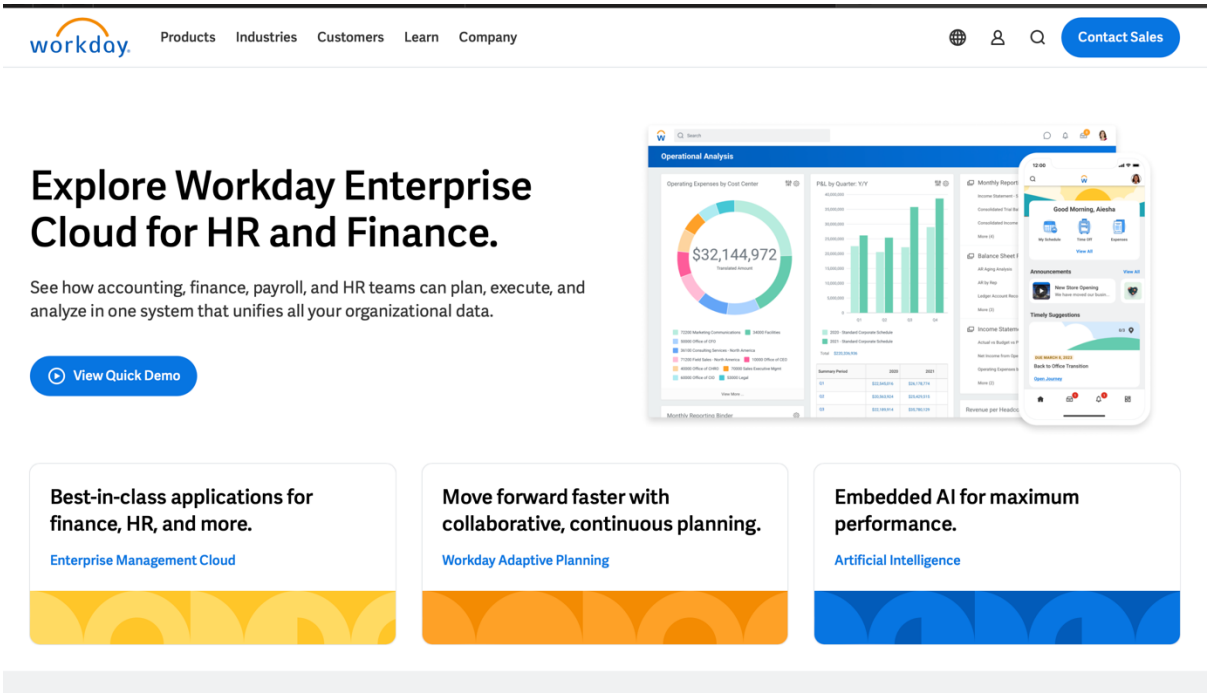

Рис.3.4 – Платформа Workday

Вхідні дані аналізу поточного стану

Аналіз проводиться на основі інформації, що стосується функціональності та характеристик **Workday**, отриманої з документації, офіційних джерел, та відгуків користувачів.

Елементи аналізу поточного стану

Організаційна структура

Workday – HR-платформа для управління персоналом та кадровим обліком.

Специфікації – Забезпечення конфіденційності особистих даних працівників та їхніх фінансових інформацій.

Можливості та процеси

Можливості – Автоматизація обліку робочого часу, управління оплатою праці, аналітика по персоналу.

Процеси – Електронна звітність, адаптація нових працівників.

Технології та інфраструктура

Інфраструктура – Хмарне розгортання для забезпечення доступності даних з будь-якої точки світу.

Технології – Використання технологій штучного інтелекту для прогнозування потреб у персоналі.

Політика (Policies)

Політика безпеки – Високі стандарти безпеки для захисту особистих даних працівників.

Архітектура бізнесу (Business Architecture)

Орієнтація на персонал – Зосередженість на підтримці ефективної роботи та розвитку кожного працівника.

Аналіз HR-системи Workday підтверджує її здатність ефективно управляти персоналом та забезпечувати конфіденційність особистих даних працівників. Організації можуть використовувати Workday для автоматизації кадрового обліку та оптимізації робочих процесів.

Системи Аналізу Даних

Для детального аналізу систем аналізу даних обрано платформу **Tableau**.

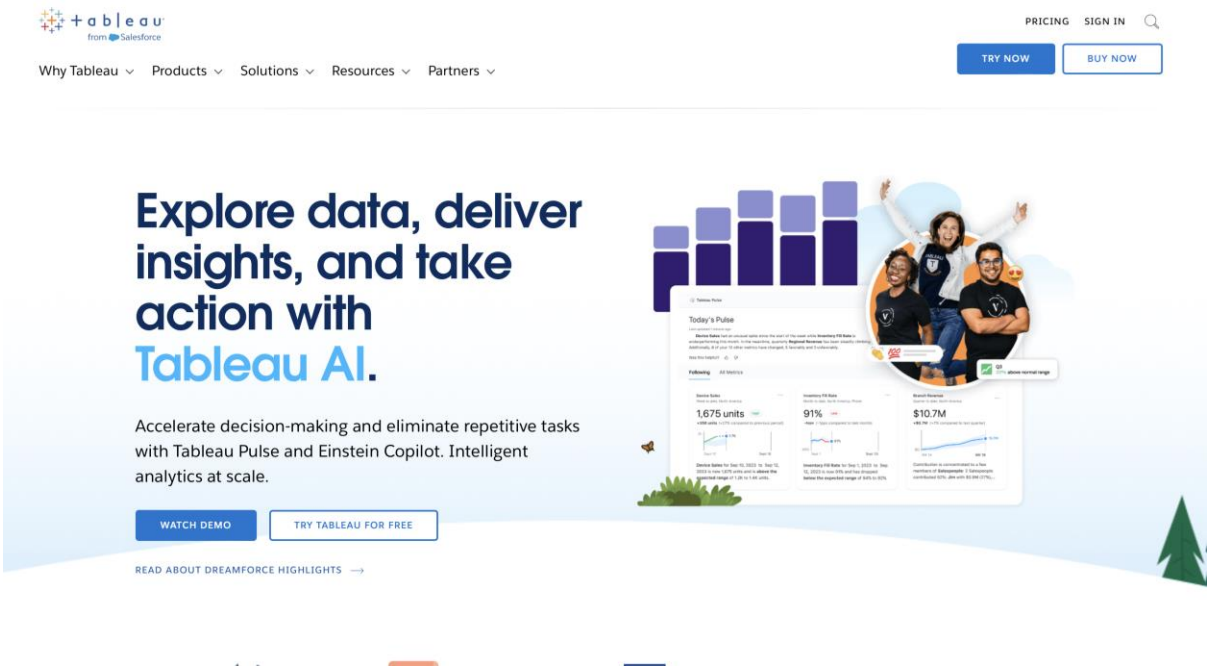

Рис.3.5 – Платформа Tableau

Вхідні дані аналізу поточного стану

Аналіз проводиться на основі інформації, що стосується функціональності та характеристик **Tableau**, отриманої з документації, офіційних джерел, та відгуків користувачів.

Елементи аналізу поточного стану

Організаційна структура

Tableau – Платформа для бізнес-аналітики та візуалізації даних.

Специфікації – нтеграція з різними джерелами даних, такими як бази даних, ексель-файли, веб-сервіси.

Можливості та процеси

Можливості – Візуалізація та аналіз великих обсягів даних, створення інтерактивних звітів та дашбордів.

Процеси – Збір, обробка, та аналіз даних для прийняття управлінських рішень.

Технології та інфраструктура

Інфраструктура – Хмарне та локальне розгортання для забезпечення доступу до аналітики в будь-який час.

Технології – Використання технологій машинного навчання для прогнозування та виявлення патернів.

Політика (Policies)

Політика безпеки – Високі стандарти безпеки для захисту конфіденційної інформації під час аналізу даних.

Архітектура бізнесу (Business Architecture)

Фокус на аналітиці – Спрямованість на підтримку прийняття рішень на основі аналізу даних.

Аналіз платформи аналізу даних Tableau підтверджує її здатність до великомасштабної візуалізації та аналізу даних з різних джерел. Організації можуть використовувати Tableau для вдосконалення своєї аналітичної діяльності та оптимізації процесу прийняття управлінських рішень.

Кожна з цих інформаційних систем має свої унікальні характеристики, але загальною є необхідність захисту від потенційних кіберзагроз. У подальших розділах буде проведений аналіз рівня кібербезпеки цих систем та розроблені пропозиції щодо поліпшення інформаційної безпеки організацій.

3.2. Виявлення вразливостей в веб-ресурсах організації

Уразливості веб-додатків виникають, коли розробники вставляють небезпечний код у веб-додаток. Це може траплятися як на етапі розробки, так і на етапі вдосконалення або виправлення виявлених раніше уразливостей. Недоліки часто класифікуються за ступенем критичності та їх поширеністю. Об'єктивною та найбільш популярною класифікацією уразливостей вважається OWASP Top 10. Рейтинг складається спеціалістами проекту OWASP і оновлюється кожні 3-4 роки.

OWASP Top 10

A1 Внедрення — Уразливості, пов'язані з впровадженням SQL, NoSQL, OS та LDAP. Виникають, коли неперевірені дані надсилаються інтерпретатору у складі команди чи запиту. Злоякісні дані можуть змусити інтерпретатор виконати непередбачувані команди або звернутися до даних без відповідної авторизації.

A2 Недоліки аутентифікації — Функції додатків, пов'язані з аутентифікацією та управлінням сесіями, часто некоректно реалізовуються, дозволяючи зловмисникам компрометувати паролі, ключі або сесійні токени, а також експлуатувати інші помилки реалізації для тимчасового або постійного перехоплення облікових записів користувачів.

A3 Розголошення конфіденційних даних — Багато веб-додатків та API мають слабкий захист критичних фінансових, медичних чи особистих даних. Зловмисники можуть викрасти або змінити ці дані, а потім вчинити шахрайські дії з кредитними

картками чи особистими даними. Конфіденційні дані потребують додаткових заходів захисту, наприклад, їх шифрування при зберіганні чи передачі, а також спеціальних заходів обережності при роботі з браузером.

A4 Внедрення зовнішніх сутностей XML — Старі або погано налаштовані XML-процесори обробляють посилання на зовнішні сутності всередині документів. Ці сутності можуть використовуватися для доступу до внутрішніх файлів через обробники URI файлів, спільні теки, сканування портів, віддалене виконання коду та відмову в обслуговуванні.

A5 Недоліки контролю доступу — Дії, дозволені аутентифікованим користувачам, часто некоректно контролюються. Зловмисники можуть скористатися цими недоліками та отримати несанкціонований доступ до облікових записів інших користувачів чи конфіденційної інформації, а також змінити користувацькі дані чи права доступу.

A6 Некоректна настройка параметрів безпеки — Некоректна настройка безпеки є поширеною помилкою. Це відбувається через використання стандартних параметрів безпеки, неповної або специфічної настройки, відкритого хмарного сховища, некоректних HTTP-заголовків та докладних повідомлень про помилки, що містять критичні дані. Всі операційні системи, фреймворки, бібліотеки та додатки повинні бути не лише налаштовані належним чином, а й своєчасно коригуватися та оновлюватися.

A7 Міжсайтове виконання сценаріїв — XSS виникає, коли додаток додає неперевірені дані на нову веб-сторінку без їх відповідної перевірки або перетворення, або коли він оновлює відкриту сторінку через API браузера, використовуючи надані користувачем дані, які містять HTML- чи JavaScript-код. За допомогою XSS зловмисники можуть виконувати сценарії в браузері жертви, дозволяючи їм перехоплювати сеанси користувачів, підмінювати сторінки сайту або перенаправляти користувачів на шкідливі сайти.

A8 Небезпечна десеріалізація — Небезпечна десеріалізація часто призводить до віддаленого виконання коду. Помилки десеріалізації, які не призводять до віддаленого виконання коду, можуть бути використані для атак із повторною відтворенням, впровадженням та підвищенням привілегій.

A9 Використання компонентів із відомими уразливостями — Компоненти, такі як бібліотеки, фреймворки та програмні модулі, запускаються з привілеями додатка. Експлуатація вразливого компонента може призвести до втрати даних чи перехоплення контролю над сервером. Використання додатками та API компонентів із відомими уразливостями може порушити захист додатка та мати серйозні наслідки.

A10 Недоліки логування та моніторингу — Недоліки логування та моніторингу, а також відсутність або неефективне використання системи реагування на інциденти, дозволяє зловмисникам розвивати атаку, приховувати свою присутність та проникати в інші системи, а також змінювати, вилучати чи знищувати дані. Звичайно вторгнення в систему зазвичай виявляють лише через 200 днів, і, як правило, це роблять сторонні дослідники, а не в межах внутрішніх перевірок чи моніторингу.

Розповсюджені уразливості

Для початку розглянемо типові уразливості, яким піддаються багато веб-додатків.

Ін'єкції

Як і відповідає, атаки класу "Ін'єкції" займають лідируючу позицію у рейтингу OWASP Top 10, зустрічаючись практично всюди і будучи дуже різноманітними у реалізації. Уразливості цього класу починаються з SQL-ін'єкцій в різних їх варіантах і закінчуються RCE — віддаленим виконанням коду.

```
SQLi: http://example.com/?id=1' union select 1,2,version(),4
RCE: http://example.com/search.php?q=;+cat+/etc/passwd
```

Рис.3.6 – Приклад ін’єкцій

XSS (Міжсайтовий скриптинг) — уразливість, яка наразі зустрічається рідше, ніж раніше, якщо вірити рейтингу OWASP Top 10, але, незважаючи на це, не стала менш небезпечною для веб-додатків і користувачів. Особливо для користувачів, оскільки атака XSS спрямована саме на них. Узагальнено, зловмисник внедрює скрипт в веб-додаток, який спрацьовує для кожного користувача, що відвідує шкідливу сторінку.

```
http://example.com/?search=<script>alert('xss')</script>
```

Рис.3.7 – Приклад xss

LFI/RFI

Уразливості даного класу дозволяють зловмисникам через браузер включати локальні та віддалені файли на сервері відповідно до веб-додатка. Ця вразливість присутня там, де відсутня коректна обробка вхідних даних, якою може маніпулювати зловмисник, інжектувати символи типу "path traversal" та включати інші файли з веб-сервера.

```
http://example.com/?search=/../../../../../../etc/passwd
```

Рис.3.8 – Приклад rfi уразливості

Атаки через JSON та XML

Веб-додатки та API, які обробляють запити у форматі JSON або XML, також піддаються атакам, оскільки ці формати мають свої недоліки.

JSON (JavaScript Object Notation) — це легкий формат обміну даними, використовуваний для комунікації між додатками. Він схожий на XML, але простіший та краще підходить для обробки за допомогою JavaScript. Багато веб-додатків

використовують цей формат для обміну даними між собою та серіалізації/десеріалізації даних. Деякі веб-додатки також використовують JSON для зберігання важливої інформації, наприклад, даних користувача. Зазвичай використовується в RESTful API та додатках AJAX.

JSON найчастіше асоціюється із API, проте часто використовується навіть у звичайних та добре відомих веб-додатках. Наприклад, редагування матеріалів у WordPress відбувається саме за допомогою відправки запитів у форматі JSON:

```
POST /index.php?rest_route=%2Fwp%2Fv2%2Fposts%2F12&_locale=user HTTP/1.1
Host: wordpress.example.com
...
%Другие заголовки%
...

{"id":12,"title":"test title","content":"test body","status":"publish"}
```

Рис.3.10 – Приклад JSON запиту

JSON Injection

Проста ін'єкція JSON на стороні сервера може бути виконана в PHP наступним чином:

Сервер зберігає користувацькі дані у вигляді рядка JSON, включаючи тип облікового запису; Ім'я користувача та пароль беруться безпосередньо з користувацького введення без очищення; Рядок JSON формується за допомогою простої конкатенації:

```
$json_string = '{"account":"user","user":"'.$_GET['user'].'","pass":"'.$_GET['pass']
```

Рис.3.11 – Формування JSON ін’єкції

```
{
   "account":"user",
   "user":"john",
   "account":"administrator",
   "pass":"password"
}
```

Рис.3.12 – Результуючий рядок

При читанні збереженого рядка парсер JSON (json_decode) виявляє дві записи account і бере останню, надаючи права адміністратора користувачеві john.

Проста ін'єкція JSON на стороні клієнта може бути виконана наступним чином:

Рядок JSON такий же, як у вищенаведеному прикладі; Сервер отримує рядок JSON з ненадійного джерела; Клієнт аналізує рядок JSON, використовуючи eval:

```
var result = eval("(" + json_string + ")");
document.getElementById("account").innerText = result.account;
document.getElementById("user").innerText = result.name;
document.getElementById("pass").innerText = result.pass;
```

Рис.3.13 – JSON injection

Функція eval викликає alert; Виклик веде до XSS і отримання document.cookie.

Атака захоплення JSON (JSON Hijacking) — це атака, яка в певному сенсі схожа на атаку міжсайтового підділю (CSRF), при якій злоумисник намагається перехопити дані JSON, які веб-додаток отримує від веб-сервера:

1. Атакуючий створює шкідливий веб-сайт і вбудовує скрипт у свій код, який намагається отримати доступ до даних JSON від цільового веб-додатка.
2. Користувач, який взаємодіє з цільовим веб-ресурсом, відвідує шкідливий сайт (наприклад, через методи соціальної інженерії).
3. Оскільки політика однакового походження (SOP) дозволяє включати та виконувати JavaScript з будь-якого сайту в контексті будь-якого іншого сайту, користувач отримує доступ до даних JSON.

4. Шкідливий сайт перехоплює дані JSON.

XML External Entity

Атака внешньою сутністю XML (XXE) є типом атаки, в якому використовується широкодоступна, але рідко використовувана функція синтаксичних аналізаторів XML. Використовуючи XXE, зловмисник може викликати відмову в обслуговуванні (DoS), а також отримати доступ до локального та віддаленого контенту та служб. XXE може використовуватися для виконання піддельних запитів на стороні сервера (SSRF), змушуючи веб-додаток виконувати запити до інших додатків. У деяких випадках XXE може використовуватися навіть для сканування портів та віддаленого виконання коду.

XML (Extensible Markup Language) — дуже популярний формат даних. Він використовується в усьому: від веб-сервісів (XML-RPC, SOAP, REST) до документів (XML, HTML, DOCX) та файлів зображень (дані SVG, EXIF). Для інтерпретації даних XML додатку потрібен аналізатор XML, відомий як XML-процесор. XML можна використовувати не тільки для оголошення елементів, атрибутів і тексту. XML-документи можуть мати визначений тип. Тип вказується в самому документі, оголошуючи визначення типу. Аналізатор XML перевіряє, чи відповідає XML-документ вказаному типу, перш ніж обробляти документ. Ви можете використовувати два варіанти визначень типів: визначення схеми XML (XSD) або визначення типу документа (DTD). Уразливості XXE зустрічаються в останньому варіанті. Хоча DTD можна вважати застарілими, вони все ще широко використовуються.

Фактично об'єкти XML можуть надходити практично з будь-якого місця, включаючи зовнішні джерела (отже, назва XML External Entity). При цьому XXE може стати видом атаки піддельного запиту на стороні сервера (SSRF). Зловмисник може створити запит, використовуючи URI (відомий в XML як системний ідентифікатор). Якщо синтаксичний аналізатор XML налаштований на обробку зовнішніх сутностей,

і за замовчуванням багато популярних аналізаторів XML на це налаштовані, веб-сервер поверне вміст файлу в системі, потенційно містять конфіденційні дані.

```
POST http://example.com/xml HTTP/1.1
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
]>
<foo>
  &xxe;
</foo>
```

Рис.3.14 – Приклад запиту

```
HTTP/1.0 200 OK

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/u
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/
systemd-resolve:x:103:104:systemd Resolver ,,,:/run/systemd:/usr/sbin/nolog
```

Рис.3.15 – Приклад відповіді

Спробуємо структурувати порівняльну таблицю з урахуванням уразливостей в різних системах.

Таблиця 3.1 – Уразливості web-додатків

Уразливості	Фінансові ІС	ERP-Системи	CRM-Системи	HR-Системи	Системи Аналізу Даних
A1 Ін'єкції	Низька	Середня	Висока	Низька	Середня
A2 Недоліки аутентифікації	Середня	Висока	Висока	Низька	Середня
A3 Розголошення конфіденційних даних	Висока	Середня	Висока	Низька	Висока
A4 Впровадження зовнішніх сутностей XML	Середня	Середня	Середня	Низька	Середня
A5 Недоліки контролю доступу	Висока	Висока	Висока	Низька	Висока
A6 Неправильна конфігурація параметрів безпеки	Середня	Середня	Середня	Низька	Середня
A7 Міжсайтове виконання сценаріїв (XSS)	Середня	Висока	Висока	Низька	Середня
A8 Небезпечна десеріалізація	Середня	Середня	Середня	Низька	Середня
A9 Використання	Середня	Середня	Середня	Низька	Середня

Уразливості	Фінансові ІС	ERP-Системи	CRM-Системи	HR-Системи	Системи Аналізу Даних
компонентів із відомими уразливостями					
A10 Недоліки журналювання та моніторингу	Середня	Висока	Висока	Низька	Висока

Висновок

1. **Фінансові Інформаційні Системи:** Узагальнюючи результати, можна відзначити, що ця система має середні та низькі рівні уразливостей, що робить її відносно безпечною, але слід вдосконалити контроль доступу та обробку конфіденційних даних.

2. **ERP-Системи:** Виявлені високі рівні уразливостей, особливо щодо недоліків аутентифікації та контролю доступу. Рекомендується вдосконалити механізми автентифікації та контролю доступу.

3. **CRM-Системи:** Система виявила високі рівні уразливостей, зокрема у недоліках аутентифікації та розголошенні конфіденційних даних. Рекомендується приділити особливу увагу цим аспектам безпеки.

4. **HR-Системи:** Загалом, система має низькі рівні уразливостей, за винятком недоліків аутентифікації. Рекомендується зосередити зусилля на вдосконаленні механізмів автентифікації.

5. **Системи Аналізу Даних:** Система виявила середні рівні уразливостей. Рекомендується зосередити увагу на контролі доступу та недоліках журналювання та моніторингу.

Ця оцінка заснована на загальному аналізі уразливостей і може змінитися в залежності від конкретних конфігурацій і заходів безпеки, які застосовуються до

кожної системи. Рекомендується регулярно вдосконалювати та апгрейдити заходи безпеки для мінімізації ризиків.

3.3. Оцінка рівня ризиків

Оцінка рівня ризиків — це важливий етап у процесі забезпечення безпеки інформаційних систем. Для цього можна використовувати матрицю оцінки ризиків, яка враховує ймовірність виникнення загрози та вплив цих загроз на бізнес-процеси. Визначимо ключові аспекти оцінки ризиків для різних видів систем, які ми розглядали раніше.

Фінансові Інформаційні Системи

Оцінка ризиків

1. **Ймовірність виникнення фінансових помилок:**
   - Низька ймовірність: Системи, такі як SAP S/4HANA Finance та Oracle Financial Services, зазвичай мають високий рівень точності та автоматизації, що зменшує ймовірність помилок.
   - Середня ймовірність: Залежить від рівня інтеграції та налаштувань системи.
   - Висока ймовірність: Низька автоматизація та велика кількість ручних операцій можуть збільшити ризик помилок.
2. **Загроза кібербезпеки для фінансових даних**
   - Залежить від рівня кіберзахисту кожної платформи.
   - Використання системи з широким спектром заходів безпеки (наприклад, SAP S/4HANA з інтегрованими інструментами безпеки) може зменшити ризик.
3. **Наслідки для оподаткування та звітності**
   - Низькі наслідки: Забезпечені системи з високим рівнем автоматизації та точності.

- Середні наслідки: Відсутність інтеграції може призвести до затримок у звітності.
- Високі наслідки: Помилки в обробці фінансових даних можуть призвести до проблем з оподаткуванням.

ERP-Системи

Оцінка ризиків

1. **Інтеграція та надійність систем**
   - Висока надійність: Якщо ERP-система, така як SAP S/4HANA або Oracle ERP Cloud, має стабільну інтеграцію, ризик втрати даних зменшується.
   - Середня надійність: Відсутність інтеграції може призвести до ризику втрати синхронізації даних.
   - Високий ризик: Неадекватна інтеграція може призвести до втрати даних та втрати функціональності.
2. **Забезпечення конфіденційності даних**
   - Високий рівень конфіденційності: Системи з потужними засобами безпеки та шифруванням.
   - Середній рівень конфіденційності: Відсутність деяких засобів безпеки або обмежена шифрування.
   - Низький рівень конфіденційності: Відсутність відповідних заходів безпеки.
3. **Ефективність та продуктивність**
   - Висока ефективність: Системи, які оптимізовані для високої продуктивності та масштабованості.
   - Середня ефективність: Наявність обмежень, які можуть вплинути на продуктивність.
   - Низька ефективність: Застарілі системи або системи, які не можуть ефективно масштабуватися.

Системи Аналізу Даних

Оцінка ризиків:

1. **Інтеграція з джерелами даних**

- Висока інтеграція: Системи, що легко інтегруються з різними джерелами даних.
- Середня інтеграція: Наявність обмежень у підтримці різних форматів даних.
- Низька інтеграція: Системи, які мають обмежену здатність інтегруватися з іншими джерелами.

2. **Потужність обробки даних**

- Велика потужність: Системи, які можуть швидко та ефективно обробляти великі обсяги даних.
- Середня потужність: Обмеження у ресурсах для обробки великих обсягів даних.
- Низька потужність: Системи, які не підтримують обробку великих обсягів даних.

Ці оцінки ризиків є загальними і враховують різні аспекти безпеки, ефективності та функціональності для кожного типу систем. Важливо враховувати конкретні контекстуальні особливості вашої організації при проведенні оцінки ризиків.

Для наочності сформуємо таблицю оцінки ризиків і подивимось на результат:

Таблиця 3.2 – Оцінка ризиків організацій

Категорія Системи	**Ключові Ризики**	**Рівень Ймовірності**	**Рівень Впливу**	**Рівень Ризику**
Фінансові Інформаційні Системи	1. Помилки в фінансових операціях	Висока	Високий	Високий
	2. Кіберзагрози фінансовим даним	Середня	Високий	Високий

Категорія Системи	Ключові Ризики	Рівень Ймовірності	Рівень Впливу	Рівень Ризику
	3. Проблеми з оподаткуванням та звітністю	Середня	Середній	Середній
ERP-Системи	1. Втрата даних під час інтеграції	Середня	Високий	Високий
	2. Загрози конфіденційності даних	Середня	Високий	Високий
	3. Низька ефективність та продуктивність	Висока	Середній	Високий
Системи Аналізу Даних	1. Низька інтеграція з джерелами даних	Середня	Високий	Високий
	2. Обмежена потужність обробки даних	Середня	Високий	Високий

Фінансові Інформаційні Системи

- Високий ризик виникнення фінансових помилок та кіберзагроз.
- Середній ризик проблем з оподаткуванням та звітністю.

ERP-Системи

- Високий ризик втрати даних під час інтеграції та загроз конфіденційності даних.
- Середній ризик низької ефективності та продуктивності.

Системи Аналізу Даних

- Високий ризик обмеженої інтеграції з джерелами даних та обмеженої потужності обробки даних.

Враховуючи ці оцінки, необхідно вжити заходів для зниження ризиків у кожній категорії. Для фінансових систем важливо покращити кіберзахист та точність операцій. В ERP-системах потрібно приділити увагу інтеграції та забезпеченню

конфіденційності даних. У системах аналізу даних необхідно покращити інтеграцію та потужність обробки даних.

Висновки до розділу

Аналіз інформаційної системи організації виявив, що комплекс систем складається з різноманітних платформ, таких як фінансові інформаційні системи, ERP-системи, CRM-системи, системи управління персоналом, системи аналізу даних та системи виявлення вразливостей в веб-ресурсах.

Щодо виявлення вразливостей в веб-ресурсах, були ідентифіковані різні типи атак, такі як ін'єкції, недостатки аутентифікації, розголошення конфіденційних даних, впровадження зовнішніх сутностей XML, атаки через JSON та інші. Це вказує на необхідність ретельного аудиту та подальших заходів забезпечення безпеки веб-додатків.

Оцінка рівня ризиків показала, що існують високі ризики в розділах фінансових інформаційних систем та ERP-систем. Це вимагає негайних заходів з усунення виявлених вразливостей та підвищення загального рівня безпеки.

У висновках виділено, що організація повинна приділити особливу увагу заходам безпеки, вжити необхідні корективи та розробити стратегію для подальшого забезпечення інформаційної безпеки на всіх рівнях її інфраструктури.

РОЗДІЛ 4. ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

4.1. Загальні висновки з дослідження

Після ретельного аналізу інформаційної системи організації та виявлення вразливостей в веб-ресурсах можна зробити кілька ключових висновків.

Перше, аудит інформаційної системи підтвердив наявність кількох серйозних уразливостей у різних частинах системи. Особливо високий ризик було виявлено в фінансових інформаційних системах та ERP-системах.

Друге, недоліки в забезпеченні безпеки веб-ресурсів створюють потенційні загрози для конфіденційності та цілісності даних. Велике число виявлених уразливостей, таких як ін'єкції, недостатки аутентифікації та розголошення конфіденційних даних, вказує на те, що дотримання стандартів безпеки в цих областях залишається актуальною проблемою.

Третє, рекомендації з покращення системи безпеки включають в себе проведення регулярних аудитів безпеки, виправлення виявлених уразливостей, впровадження механізмів моніторингу та виявлення вторгнень, а також надання пріоритету питанням безпеки при розробці та впровадженні нових функціональностей.

Загальною рекомендацією є впровадження комплексного підходу до інформаційної безпеки, охоплюючи як технічні, так і організаційні аспекти, для максимального забезпечення захищеності інформаційних ресурсів організації.

4.2. Рекомендації щодо покращення інформаційної безпеки

На підставі виявлених уразливостей та загроз інформаційної системи, пропонуються конкретні рекомендації для поліпшення рівня інформаційної безпеки:

Зміцнення безпеки фінансових інформаційних систем

У контексті зміцнення безпеки фінансових інформаційних систем рекомендується проведення повного аудиту з метою ідентифікації та усунення можливих слабких місць. Аудит дозволить докладно вивчити існуючі системи, визначити потенційні точки доступу для несанкціонованої діяльності та вжити заходів для їх подальшого усунення.

Додатково, пропонується впровадження технологій шифрування для забезпечення високого рівня захисту фінансових даних під час їх збереження та передачі. Шифрування даних є ефективним засобом запобігання несанкціонованому доступу та забезпечення конфіденційності.

Для миттєвого реагування на потенційні загрози, слід вдосконалити систему моніторингу заходів безпеки. Це включає в себе вдосконалення алгоритмів виявлення аномалій та впровадження засобів реагування в реальному часі. Ефективний моніторинг дозволяє оперативно виявляти незвичайну активність та приймати необхідні заходи для забезпечення безпеки фінансових інформаційних систем.

Підвищення безпеки веб-ресурсів

Для підвищення безпеки веб-ресурсів рекомендується систематично виправляти уразливості, які були виявлені під час проведення аудиту. Особлива увага повинна бути приділена усуненню можливих ін'єкцій та недоліків в системі аутентифікації, оскільки це звільнює можливість для несанкціонованого доступу.

Впровадження відповідних механізмів фільтрації та обробки вхідних даних є важливим етапом в забезпеченні безпеки. Це дозволяє відсіювати потенційно шкідливі або несанкціоновані дані, що надходять на веб-ресурс.

Застосування принципу найменших прав доступу має на меті обмеження привілеїв користувачів. Це означає, що кожен користувач має доступ лише до тих

ресурсів і функцій, які необхідні для виконання його конкретних завдань. Цей принцип допомагає уникнути непотрібного розголошення чутливих даних і зменшити ризик несанкціонованого доступу.

Покращення моніторингу та виявлення вторгнень

Щоб підвищити рівень безпеки, рекомендується впровадити систему централізованого моніторингу безпеки. Ця система дозволить в реальному часі виявляти невідомі загрози та вторгнення, надаючи можливість оперативно реагувати на потенційні атаки.

Для ефективного виявлення непередбачуваних дій рекомендується використовувати сучасні системи виявлення аномалій та поведінкового аналізу. Ці системи здатні аналізувати зміни в патернах поведінки користувачів та виявляти аномальні активності, що може свідчити про потенційні загрози. Використання таких інструментів сприятиме ранньому виявленню вторгнень і дозволить вжити необхідних заходів для їхнього усунення.

Забезпечення оновлення та патчінгу

Щоб підвищити рівень безпеки, рекомендується впровадити систему централізованого моніторингу безпеки. Ця система дозволить в реальному часі виявляти невідомі загрози та вторгнення, надаючи можливість оперативно реагувати на потенційні атаки.

Для ефективного виявлення непередбачуваних дій рекомендується використовувати сучасні системи виявлення аномалій та поведінкового аналізу. Ці системи здатні аналізувати зміни в патернах поведінки користувачів та виявляти аномальні активності, що може свідчити про потенційні загрози. Використання таких

інструментів сприятиме ранньому виявленню вторгнень і дозволить вжити необхідних заходів для їхнього усунення.

Навчання персоналу та свідомість щодо безпеки

Ефективна система інформаційної безпеки передбачає активну участь та розуміння персоналом загроз та заходів безпеки. Для цього рекомендується організовувати регулярні тренінги для всього персоналу, які охоплюють ключові аспекти інформаційної безпеки.

На тренінгах персонал може отримати навички та знання щодо виявлення соціально-інженерних атак, правильного використання паролів, та інших аспектів безпеки. Важливим є підвищення свідомості про те, як виявляти та уникати потенційні загрози, що дозволяє персоналу діяти відповідально та враховувати аспекти безпеки у повсякденній роботі.

4.3. Перспективи подальших досліджень

Доцільним напрямком подальших досліджень є:

1. **Розширення аналізу уразливостей** – Провести більш глибокий аналіз уразливостей та виявлення нових можливих загроз в інформаційних системах. Врахувати нові тенденції та технології у сфері інформаційної безпеки.
2. **Розвиток методів виявлення загроз** – Розробка та вдосконалення методів виявлення потенційних загроз, враховуючи сучасні техніки атак та використання штучного інтелекту для виявлення аномалій.
3. **Створення систем безпеки нового покоління** – Дослідження та розробка нових технологій та архітектур для побудови ефективних систем безпеки, що враховують специфіку конкретних секторів та підвищують рівень стійкості до атак.

4. **Оптимізація стратегій реагування на інциденти** – Розробка та впровадження оптимальних стратегій реагування на інциденти, враховуючи реалії конкретного сектору та найефективніші засоби відновлення.

5. **Вивчення соціально-інженерних аспектів безпеки** – Поглиблене дослідження аспектів соціально-інженерних атак, розробка заходів для підвищення свідомості персоналу та вивчення психології атак.

6. **Створення рекомендацій для стандартів безпеки** – Формулювання та розробка рекомендацій для стандартів безпеки, що враховують специфіку досліджуваного сектору та сприяють створенню більш безпечних інформаційних систем.

Ці напрямки досліджень можуть сприяти подальшому вдосконаленню систем безпеки та забезпечити ефективний захист інформаційних ресурсів в умовах постійно зростаючих загроз та технологічних викликів.

Висновки до розділу

Дослідження інформаційних систем виявило кілька серйозних вразливостей, що загрожують безпеці даних. Загальний рівень інформаційної безпеки є низьким, що потребує негайних заходів для усунення проблем.

Рекомендації щодо покращення інформаційної безпеки:

- *Фінансові інформаційні системи:* Провести повний аудит, впровадити шифрування та покращити систему моніторингу безпеки.
- *Веб-ресурси:* Виправити уразливості, впровадити механізми фільтрації та обмежити права доступу.
- *Моніторинг та виявлення вторгнень:* Впровадити централізовану систему моніторингу та використовувати сучасні засоби виявлення аномалій.
- *Оновлення та патчінг:* Регулярно оновлювати компоненти системи та автоматизувати встановлення патчів.
- *Навчання персоналу:* Організувати регулярні тренінги з питань інформаційної безпеки.

Для поглиблення розуміння інформаційної безпеки слід досліджувати соціально-інженерні аспекти та розвивати нові технології виявлення загроз.

ВИСНОВКИ

Ця робота ставила за мету провести комплексний аналіз інформаційної безпеки організації, охопивши різноманітні аспекти, від опису існуючих систем до виявлення вразливостей та оцінки ризиків.

Дослідження фінансових інформаційних систем показало присутність серйозних проблем у забезпеченні конфіденційності та цілісності даних. Рекомендації, спрямовані на проведення аудиту та впровадження технологій шифрування, є критичними для запобігання можливим загрозам.

Аналіз веб-ресурсів підтвердив наявність уразливостей, які можуть бути використані для атак типу ін'єкцій та недоліків аутентифікації. Рекомендації стосуються виправлення виявлених проблем і впровадження фільтрації вхідних даних.

Моніторинг та виявлення вторгнень мають велике значення для реагування на потенційні загрози в реальному часі. Запропоновані рекомендації, такі як централізована система моніторингу та використання засобів виявлення аномалій, спрямовані на підвищення ефективності цих процесів.

Оновлення та патчінг є ключовими аспектами управління інформаційною безпекою. Регулярне оновлення компонентів системи та автоматизація встановлення патчів допоможуть зменшити вразливість перед новими загрозами.

Тренування персоналу є важливим елементом заходів з підвищення інформаційної безпеки. Розроблені рекомендації з навчання персоналу спрямовані на підготовку до виявлення та управління можливими загрозами.

У цілому, проведений аналіз дозволяє зробити висновок, що існують серйозні проблеми в інформаційній безпеці організації, але застосування рекомендацій може значно підвищити рівень захищеності та готовності до майбутніх викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Книги, підручники

1. Захист веб-додатків: кращі практики та засоби. 2021. URL: owasp.org (дата звернення: 13.11.2023).

2. Спрощений підхід до захисту веб-ресурсів. Національний Інститут Стандартів і Технологій. 2018. URL: csrc.nist.gov (дата звернення: 05.12.2023).

3. United States Government Accountability Office. Cybersecurity & Infrastructure Security Agency: підручник. United States Government Accountability Office, 2021.

4. Топ-5 інструментів для аналізу та захисту веб-ресурсів. Ліга.Захист. 2020. URL: ligazahist.com (дата звернення: 16.11.2023).

5. Жилін А., Худинцев М., Літвінов М. ФУНКЦІОНАЛЬНА МОДЕЛЬ СИТУАЦІЙНОГО ЦЕНТРУ КІБЕРЗАХИСТУ. 2018. URL: ela.kpi.ua (дата звернення: 04.11.2023).

6. Dias M., Sanches I. Захист веб-додатків в інформаційних системах організацій: сучасні виклики. м. Київ. 2020.

7. Смірнова О. Аналіз загроз і методи захисту веб-ресурсів в умовах сучасних технологій. Інформаційна Безпека. 2019.

8. C L., Wang L. Інноваційні технології захисту веб-ресурсів в умовах розвитку хмарних сервісів. Інформаційні Технології. 2020.

9. Баранов С., Григоров Д. Актуальні проблеми та перспективи захисту веб-ресурсів в інформаційних системах підприємств. Інформаційна безпека. 2017.

10. Stivens J. Практичні аспекти. Монографія. Захист веб-ресурсів : монографія. 2017.

Наукові статті

11. Міллер Ч., Ванген Й. Технології і методи кібербезпеки для інформаційних систем : підручник. Львів : Львів. ун-т, 2019.

12. Сідоров О. Захист веб-додатків: аналіз, тестування, практика : підручник. Київ : Техн. Літ., 2018.

13. Локхарт Г., Стіл К. Кібербезпека: напрямки та виклики : підручник. Одеса : Астропринт, 2020.

14. Мартінес А. Захист веб-серверів: технології та практики : монографія. Київ : Інформ. Безпека, 2017.

15. Іванов Д., Попова Л., Чернишова Ю. Забезпечення кібербезпеки веб-ресурсів в умовах інтеграції з інформаційними системами. Міжнар. конф. "Інформ. безпека та кібернетика", 2018.

16. Шевченко В., Кузьменко О., Григоренко О. Методи та засоби захисту веб-додатків в умовах зростання загроз. Інформаційна безпека. 2017.

17. Яценко Л., Литвиненко С., Ковальчук О. Аналіз та підвищення безпеки веб-сервісів організацій. Конференція. Сучасні проблеми інформатики : 2016, 8 лип. 2016.

Електронні ресурси

18. Кондрашин М. Захист кінцевих точок у сучасних умовах: інструменти та основні проблеми. 2019. URL: ko.com.ua (дата звернення: 17.11.2023).

19. Качін М. Аналіз ризику – методологічна основа для розв’язання проблем безпеки людини та довкілля. Екологічна безпека. 2018. URL: niss.gov.ua (дата звернення: 19.11.2023).

20. Кожухівський А. Імітаційне моделювання систем та процесів кібербезпеки в середовищі MATLAB. Практикум. 2020.

21. Microsoft security center of excellence // TechNet. – Электрон. дан. – Редмонд, США : Корпорація Майкрософт, 2006. – Режим доступа: technet.microsoft.com.

22. Ситник, С. Захист Web-ресурсів в інформаційних системах. Матеріали конференції CyberSec. (2016).

23. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С (2020). Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ ННІЗІ.

Журнальні статті

24. Петренко А. В. Актуальні питання технології захисту Web-ресурсів в інформаційних системах / Петренко А. В. // Зв’язок та Інтернет. 2023. № 2 (56). С. 45–52.

25. Іванченко С. М. Інноваційні методи захисту Web-ресурсів в сучасних інформаційних системах / Іванченко С. М. // Інформаційна безпека та кібернетика. 2022. Т. 15, № 3. С. 78–85.