МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри

_____Ігор ЖУКОВ

« ____» _____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТР"
ЗА СПЕЦІАЛЬНІСТЮ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

Тема: Захищена ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою

Виконавець: Олексій ГУЦАЛО

Керівник: Микола ПЕЧУРІН

Нормоконтролер: Василь МАЛЯРЧУК

Засвідчую, що у дипломній роботі немає запозичень із праць інших авторів без відповідних посилань
Студент: Олексій ГУЦАЛО

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж
Напрям (спеціальність) 123 "Комп'ютерна інженерія"
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем та мереж

_____Ігор ЖУКОВ

« ____» _____2023 р.

З А В Д А Н Н Я
на виконання кваліфікаційної магістерської роботи

Гуцала Олексія Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема роботи: Захищена ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою
   Затверджена наказом ректора від «29» серпня 2023р. №1521/ст;
2. Термін виконання роботи: з 02.10.2023 до 31.12.2023;
3. Вихідні дані до роботи: 1. Тип мережі – захищена; 2. Тип архітектури – централізована; 3. Клас комп. мережі – локальна; 4. Сегмент бак - наземний
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці): Перелік умовних позначень, скорочень, термінів; Вступ; Розділ 1 Теоретичний огляд розробки захищеного лом наземного сегменту авіаційного комплексу з централізованою архітектурою; Розділ 2 О системний аналіз захищеної локальної обчислювальної мережі; Розділ 3; Висновки; Список бібліографічних посилань використаних джерел.
5. Перелік обов'язкового графічного матеріалу: презентація

Календарний план-графік

№ п/п	Завдання	Термін виконання	Примітка
1	Узгодження технічного завдання	02.10.2023	
2	Підбір та опрацювання теоретичного матеріалу	02.10.2023 – 10.10.2023	
3	Системний аналіз захищених від радіовипромінювання комп'ютерних мереж	10.10.2023 – 20.10.2023	
4	Визначення критеріїв захищенності від радіовипромінювання	20.10.2023 – 22.10.2023	
5	Проведення експерименту та аналіз результатів топологій оптимізації мережі	22.10.2023 – 24.10.2023	
6	Реалізація алгоритму Борувки для оптимізації мережі	24.10.2023 – 30.10.2023	
7	Дослідження систем координат	30.10.2023 – 03.11.2023	
8	Запроведження покращень до алгоритму Борувки для використання у сфері наземного фегменту системи БАК	03.11.2023 – 26.11.2023	
9	Створення інтерфейсу користувача, застосовуючого покращений алгоритм	26.11.2023 – 21.12.2023	
10	Оформлення пояснювальної записки та графічного матеріалу	21.12.23 – 31.12.2023	
11	Подання матеріалів роботи на кафедру	22.12.23 – 31.12.2023	

6. Дата отримання завдання «02» жовтня 2023 р.

Керівник дипломної роботи _____ Микола ПЕЧУРІН
(підпис)

Завдання прийняв до виконання _____ Олексій ГУЦАЛО
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційного проєкту “Захищена ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою”: 00 с., 00 рис., 00 літературних джерел, 0 таблиць.

ЗАХИЩЕНА ЛОМ НАЗЕМНОГО СЕГМЕНТУ АВІАЦІЙНОГО КОМПЛЕКСУ З ЦЕНТРАЛІЗОВАНОЮ АРХІТЕКТУРОЮ

Об’єкт дослідження – система захисту ЛОМ наземного сегмента авіаційного комплексу з централізованою архітектурою.

Предмет дослідження – система захисту ЛОМ наземного сегмента авіаційного комплексу з централізованою архітектурою, включаючи апаратні та програмні компоненти, процеси та алгоритми забезпечення безпеки..

Мета кваліфікаційної роботи – розробка та вдосконалення ефективного та захищеного від кіберзагроз системного підходу до ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою, сприяючи оптимізації та підвищенню рівня безпеки авіаційних операцій.

Методи дослідження – аналіз інформації предметної галузі, порівняльний аналіз, обробка літературних джерел.

Прогнозні припущення щодо розвитку об’єкта дослідження – Збільшення регулювання та вимог безпеки: З урахуванням зростання свідомості щодо кібербезпеки в авіаційній галузі, передбачається, що збільшаться регулювання та вимоги стосовно безпеки систем наземного обслуговування.

Результати кваліфікаційної роботи рекомендується використовувати під час подальших наукових досліджень, розробки нових технологій або вирішення практичних завдань у відповідній галузі. Отримані результати можуть слугувати основою для вдосконалення існуючих систем, розробки нових програмних продуктів чи апаратних засобів, а також визначення ефективних стратегій управління та забезпечення безпеки. Також, результати можуть бути використані для підготовки наукових публікацій, доповідей на конференціях або представлення наукових досягнень на відповідних форумах.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

БД - База даних.

ПЗ - Програмне забезпечення.

DBA (Database Aggregation) – Агрегація баз даних

ODSPC (Optimal Selection for Passenger Choices) – Оптимальний вибір для вибору пасажиром

ALC (Airline Company) – Авіакомпанія

CAA (Comparison and Analysis Algorithms) – Порівняння та аналіз алгоритмів

VFA (Value for Airfares) – Вартість авіабілетів

EUM (Efficient User Management) – Продуктивне управління користувачем

ВСТУП

У сучасному світі питання створення захищеної локальної комп'ютерної мережі для наземного сегменту авіаційного комплексу з централізованою архітектурою стає все більш важливим. Інформаційні технології стали невід'ємною частиною повсякденного життя, і забезпечення безпеки та ефективності комп'ютерної мережі є вирішальним для безперебійної роботи авіаційних подій. Мобільність та подорожі є суттєвими складовими нашого існування, а захищена мережа є ключовою для підтримки різноманітних операцій в межах авіаційного комплексу.

Зростає попит на швидкі та надійні рішення управління локальною комп'ютерною мережею, особливо враховуючи стрімкий розвиток авіаційної індустрії та необхідність централізованого контролю та заходів безпеки. Важливість цієї кваліфікації підкреслюється необхідністю забезпечення користувачів ефективними інструментами, які дозволяють централізовано управляти, контролювати та захищати комп'ютерну мережу. Користувачі вимагають не лише зручності використання, але й доступу до актуальної та безпечної інформації.

В сучасному високодинамічному авіаційному середовищі, де авіаційний комплекс покладається на централізовану архітектуру мережі, інструменти для аналізу та забезпечення безпеки мережі стають все важливішими. Інформаційне перенавантаження та складність авіаційних операцій створюють додаткові труднощі у збереженні цілісності та безпеки мережі.

Обрана тема "Створення захищеної локальної комп'ютерної мережі для наземного сегменту авіаційного комплексу з централізованою архітектурою" є актуальною в сучасному контексті з кількох причин:

- Критичний характер авіаційних операцій. Авіаційний комплекс покладається на безпечну та централізовану комп'ютерну мережу для забезпечення ефективної та безпечної роботи різноманітних компонентів.
- Зростання зв'язку та інтеграції. Оскільки системи авіації стають більш взаємопов'язаними, необхідність централізованої та захищеної мережевої архітектури стає вирішальною.

- Потреба в безпечному передаванні даних. З обміном чутливою інформацією в межах авіаційного комплексу захищена мережа є важливою для захисту від кіберзагроз та несанкціонованого доступу.
- Технологічний прогрес та можливості забезпечення безпеки. Розвиток технологій дозволяє використовувати нові методи забезпечення мережі та штучного інтелекту для точнішого прогнозування та рекомендацій. Створення захищеної локальної комп'ютерної мережі може ефективно використовувати ці технологічні можливості на користь користувачів.

Отже, обрана тема є актуальною через критичну роль захищеної локальної комп'ютерної мережі в забезпеченні безпечної та ефективної роботи наземного сегменту авіаційного комплексу. Впровадження централізованої архітектури для комп'ютерної мережі має потенціал підвищити рівень безпеки та оптимізувати операції, що робить це завданням важливим для подальшого розвитку авіаційної галузі.

Метою кваліфікаційної роботи є розробка програмного забезпечення для модуля, спрямованого на підвищення безпеки локальної комп'ютерної мережі в наземному сегменті авіаційного комплексу з використанням централізованої архітектури. Це спрямовано на поліпшення загальної ефективності та надійності мережі.

Згідно з цією метою потрібно вирішити наступні завдання:

- Вивчення поточних тенденцій у сфері безпеки мережі, аналіз існуючих протоколів та функціональностей централізованих архітектур, а також розгляд основних чинників, що впливають на безпеку локальної комп'ютерної мережі.
- Розробка алгоритмів для аналізу параметрів безпеки локальної комп'ютерної мережі, з урахуванням таких факторів, як контроль доступу, шифрування та виявлення вторгнень.
- Вивчення можливості впровадження високорівневих заходів безпеки, включаючи брандмауери, антивірусні рішення та протоколи шифрування.

- Дослідження можливості інтеграції методів машинного навчання та аналізу великих обсягів даних для передбачення та запобігання загроз безпеці у локальній мережі.
- Тестування програмного модуля безпеки на різних платформах та середовищах для забезпечення його ефективності.
- Оптимізація програмного модуля для гарантії швидкого реагування та ефективного використання ресурсів.

Об'єктом дослідження є процес захисту локальної комп'ютерної мережі в наземному сегменті авіаційного комплексу.

Предметом дослідження є програмний модуль, спрямований на підвищення безпеки локальної комп'ютерної мережі для захисту критичних авіаційних даних та інфраструктури.

Обгрунтування цієї теми дослідження обумовлене необхідністю підвищення рівня безпеки мережі в контексті зростаючої популярності онлайн-систем та розширення конкуренції на цьому ринку. Можливі методи дослідження включають:

- Огляд літератури, тобто систематичний огляд наукових та технічних публікацій щодо ринку авіабілетів, агрегації даних та аналізу вартості перельотів. Розглядаються різні підходи та методології таких програмних рішень.
- Експертний опитування. Опитування серед експертів у сфері авіації та програмної інженерії для збору думок щодо основних вимог до програмного модуля, потреб користувачів та можливостей впровадження штучного інтелекту.
- Розробка та тестування програмного модуля для гарантії швидкого реагування та ефективного використання ресурсів.
- Розробка та тестування програмного модуля. Для впровадженого програмного модуля, на основі зібраних вимог та використаних математичних моделей, необхідно перевірити ефективність та стабільність модуля в різних умовах.

Практичне значення результатів:

- Підвищена безпека мережі: Розроблений програмний модуль дозволяє ефективний аналіз безпеки локальної комп'ютерної мережі, дозволяючи

виявляти та усувати потенційні вразливості та загрози. Це сприяє зміцненню захисту від кіберзагроз та забезпечує цілісність та конфіденційність даних авіаційного комплексу.

- Централізоване управління мережею: Програмний модуль, інтегрований у централізовану архітектуру, оптимізує управління захищеною локальною комп'ютерною мережею. Цей централізований підхід підвищує можливості моніторингу, спрощує адміністративні завдання та забезпечує більш ефективну реакцію на інциденти безпеки.
- Відповідність регуляторним вимогам авіаційної індустрії: Результати дослідження сприяють забезпеченню відповідності регуляторним вимогам у секторі авіації, пов'язаним із безпекою та конфіденційністю даних у наземному сегменті. Це важливо для забезпечення загальної цілісності та надійності авіаційного комплексу.
- Швидка реакція на інциденти: Централізована архітектура, спільно з вдосконаленим аналізом безпеки, забезпечує швидке виявлення та реагування на інциденти безпеки. Це зменшує можливий простріл часу та мінімізує вплив порушень безпеки на авіаційні операції.

Практична цінність роботи:

- Інтегроване засіб безпеки: Розроблений програмний модуль об'єднує агрегацію даних та аналіз безпеки в єдиний інструмент, спрощуючи управління захищеною локальною комп'ютерною мережею. Цей новаторський підхід покращує ефективність та ефективність заходів забезпечення безпеки мережі.
- Внесок в авіаційну кібербезпеку: Результати дослідження є цінним внеском у галузь кібербезпеки в авіаційній індустрії. Інтегроване програмне рішення служить основою для подальших досягнень у сфері забезпечення критичної інфраструктури в авіаційних комплексах.

Особистий внесок випускника:

- Всі результати, представлені у цьому дослідженні, були досягнуті випускником особисто. Особлива увага була приділена тестуванню та вдосконаленню програмного модуля, а також вивченню та аналізу тенденцій на ринку, що покращили та розширили алгоритми програмного модуля.

1. ТЕОРЕТИЧНИЙ ОГЛЯД РОЗРОБКИ ЗАХИЩЕНОГО ЛОМ НАЗЕМНОГО СЕГМЕНТУ АВІАЦІЙНОГО КОМПЛЕКСУ З ЦЕНТРАЛІЗОВАНОЮ АРХІТЕКТУРОЮ

1.1. Визначення захищеного ЛОМ наземного сегменту авіаційного комплексу

Локальна обчислювальна мережа (ЛОМ)- це мережа комп'ютерів та інших пристроїв, яка дозволяє їм обмінюватися даними та ресурсами на обмеженій території, такій як наземний сегмент авіаційного комплексу.

Мережі цього типу можуть бути використані для забезпечення зв'язку, обробки даних, контролю та координації різних систем і підсистем.:

Захищена ЛОМ- захищена мережа передбачає впровадження заходів безпеки для запобігання несанкціонованому доступу, збереження конфіденційності і цілісності даних, а також забезпечення доступності служб та ресурсів.

Це може включати в себе шифрування даних, аутентифікацію, авторизацію, вогнепровідні системи та інші технічні та організаційні заходи безпеки.

Наземний сегмент авіаційного комплексу- це частина авіаційної системи, яка розташована на землі та включає в себе інфраструктуру для наземного обслуговування повітряного руху, управління авіаційною безпекою, системи зв'язку, та інші технічні засоби.

1.2. Огляд існуючих рішень та методів захисту ЛОМ

Захист локальних обчислювальних мереж (ЛОМ) вимагає використання різноманітних рішень та методів, щоб забезпечити конфіденційність, цілісність та доступність інформації. Ось огляд деяких існуючих рішень та методів захисту ЛОМ:

1. **Шифрування даних:**
   - Використання алгоритмів шифрування для захисту конфіденційності даних під час їх передачі по мережі або зберігання на пристроях.
   - *TLS/SSL* для шифрування трафіку між вузлами мережі.

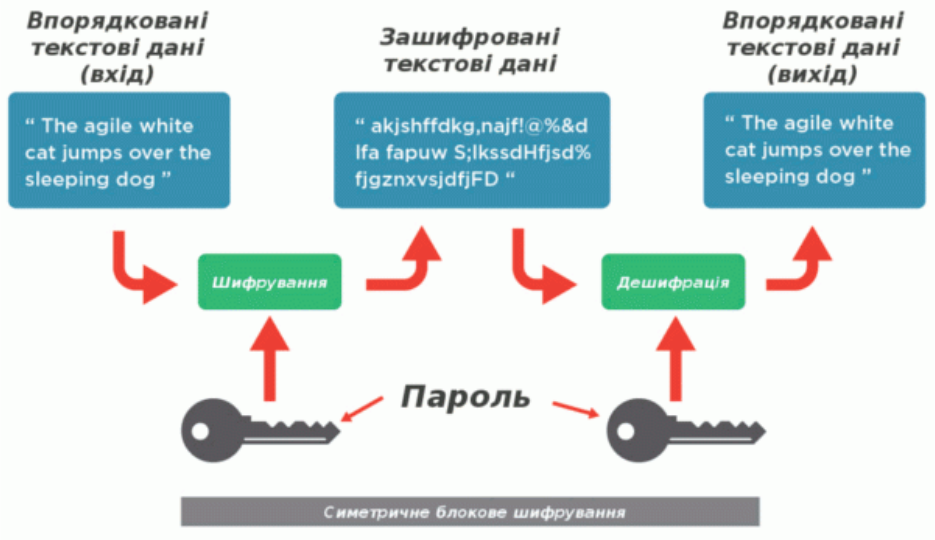

Рис. 1.1.

2. **Віртуальні приватні мережі (VPN):**
   - Застосування VPN для створення безпечного тунелю через незахищені мережі, щоб забезпечити конфіденційність та цілісність даних.

Рис. 1.2.

3. **Файерволи та системи виявлення/захисту вторгнень (IDS/IPS):**
   - Використання файерволів для контролю трафіку та систем IDS/IPS для виявлення та запобігання вторгненням в мережу.

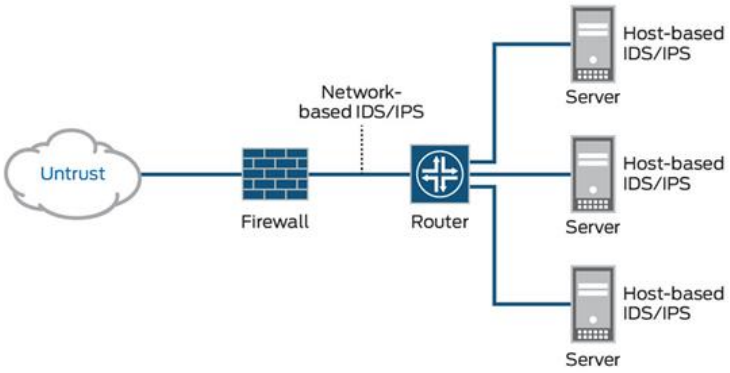

Рис. 1.3.

4. **Системи аутентифікації та авторизації:**
   - Встановлення міцної системи аутентифікації користувачів та пристроїв для забезпечення доступу лише авторизованим особам.

Рис. 1.4.

5. **Захист від вірусів та шкідливого програмного забезпечення:**
   - Використання антивірусного програмного забезпечення та систем захисту від шкідливого коду для запобігання інфікуванню систем.

Рис. 1.5.

6. **Стандарти та протоколи безпеки:**
   - Дотримання стандартів безпеки, таких як ISO 27001, та використання захищених мережевих протоколів.

Рис. 1.6.

7. **Резервне копіювання та відновлення:**
   - Регулярне резервне копіювання даних і розробка планів відновлення для забезпечення доступності та цілісності інформації.

Рис. 1.7.

8. **Оновлення та патчі:**
   - Регулярне оновлення програмного та апаратного забезпечення для усунення вразливостей та запобігання експлойтам.
9. **Організаційні заходи:**
   - Проведення навчань та освіти для персоналу з питань безпеки, а також встановлення політик безпеки в організації.

1.3. Централізована архітектура системи та її роль у забезпеченні безпеки

Централізована архітектура системи передбачає, що функції та ресурси системи зосереджені в одному центральному пункті керування чи обчислення. Це може включати центральний сервер, базу даних або інший головний вузол, який відповідає за координацію та управління роботою всієї системи. Централізована архітектура може використовуватися в різних областях, включаючи інформаційні системи, мережі, телекомунікації та інші.

Роль централізованої архітектури у забезпеченні безпеки може бути визначеною наступним чином:

1. **Контроль доступу:**
   - Централізована архітектура дозволяє ефективно керувати доступом до ресурсів та функцій системи. Усі запити на доступ можуть проходити через центральний пункт, де встановлюються правила та політики доступу.
2. **Моніторинг та аудит:**
   - З централізованим підходом легше відслідковувати та моніторити активність в системі. Це полегшує виявлення ненормальної або підозрілої активності, а також здійснення аудиту подій.
3. **Централізоване управління політиками безпеки:**
   - Можливість визначити та використовувати централізовані політики безпеки для всієї системи. Це забезпечує консистентність та об'єднання заходів безпеки.
4. **Швидка реакція на загрози:**
   - За допомогою централізованої архітектури можна швидко реагувати на потенційні загрози та вживати заходи безпеки з центрального пункту управління.
5. **Зменшення однієї точки відмови (*SPoF*):**
   - За умови правильної реалізації та використання резервних систем, централізована архітектура може допомогти уникнути SPoF, де весь функціонал системи концентрується в одному вузлі.
6. **Оновлення та патчі:**

- Централізована архітектура спрощує процес впровадження оновлень та патчів, оскільки це може бути здійснено в центральному вузлі.

7. **Захист даних:**
   - Можливість централізовано керувати заходами безпеки дозволяє ефективніше захищати дані в системі, включаючи їх шифрування, резервне копіювання та інші методи.

З усім тим, централізована архітектура має свої виклики, зокрема, вона може бути менш стійкою до відмов, і є необхідність у додаткових заходах для забезпечення надійності та доступності системи. Важливо збалансувати переваги та недоліки централізованого підходу у контексті конкретного застосування та потреб безпеки.

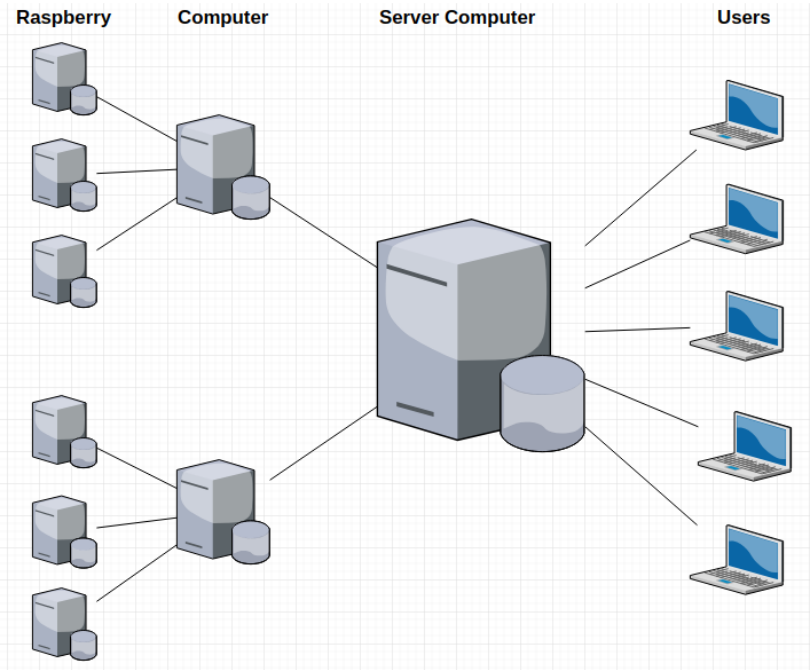

Рис. 1.8.

1.4. Огляд існуючих архітектур та інших видів захисту ЛОМ. Їх переваги і недоліки.

Існує багато різних архітектур та методів захисту для локальних обчислювальних мереж (ЛОМ), і їх вибір залежить від конкретних вимог, обмежень та сценаріїв використання. Нижче подано огляд деяких з них, а також їхні переваги та недоліки.

1. Централізована архітектура:

Централізована серверна система, де всі дані та обчислення концентруються в одному центральному вузлі.

Переваги:

- Легкість управління та підтримки.
- Централізована політика безпеки.

Недоліки:

- Одна точка відмови.
- Збільшення обсягу трафіку в мережі.
- Велике навантаження на центральний вузол.

2. Децентралізована архітектура:

Мережа, де обчислення та обробка даних розподілені між різними вузлами без одного центрального пункту.

Переваги:

- Стійкість до відмов.
- Розподілення навантаження.

Недоліки:

- Ускладнена координація та управління.
- Потреба в ефективному механізмі синхронізації.

3. Гібридна архітектура:

Комбінація централізованих та децентралізованих елементів в системі.

Переваги:

- Поєднання переваг обох підходів.
- Гнучкість та адаптивність.

Недоліки:

- Складність розробки та обслуговування.

4. Захист на рівні мережі:

Використання файерволів, VPN, мережевого інтрузійного виявлення та запобігання (NIDS/NIPS).

Переваги:

- Захист від несанкціонованого доступу та атак.

- Моніторинг та реагування на вторгнення.

Недоліки:

- Потреба у великому обсязі конфігурації та обслуговування.

5. Шифрування даних:

Використання TLS/SSL для захисту комунікацій.

Переваги:

- Конфіденційність та цілісність даних.
- Захист від перехоплення.

Недоліки:

- Збільшення навантаження на систему під час шифрування/розшифрування.

6. Системи виявлення та захисту вторгнень (IDS/IPS):

Використання систем для виявлення та запобігання несанкціонованим вторгненням.

Переваги:

- Вчасне виявлення та відвертання атак.
- Автоматизована реакція на загрози.

Недоліки:

- Ризик ложнопозитивів та ложнонегативів.

1.4.1. Система управління корпоративними ресурсами (ERP) – SAP ERP

Рисунок 1.9. Система управління корпоративними ресурсами SAP ERP.

SAP ERP є однією з найпоширеніших інтегрованих систем управління корпоративними ресурсами у світі. Це програмне забезпечення використовує централізовану архітектуру для об'єднання та управління різними функціональними областями підприємства.

Основні риси централізованої архітектури в SAP ERP:

1. **Централізована база даних:**
   - Всі дані підприємства, включаючи фінанси, логістику, управління кадрами, складський облік, обробляються та зберігаються в єдиної централізованій базі даних.
2. **Централізоване управління процесами:**
   - Управління бізнес-процесами, такими як виробництво, збут, закупівлі, відбувається через централізовані модулі та інтеграцію даних.
3. **Централізована аутентифікація та авторизація:**
   - Централізована система керування доступом визначає права доступу користувачів до різних функціональних областей системи.
4. **Централізований моніторинг та звітність:**
   - Інструменти моніторингу та звітності надають змогу централізовано відслідковувати та аналізувати різні аспекти діяльності підприємства.

Переваги:

1. **Єдина точка керування:**
   - Забезпечує консолідацію та стандартизацію управління бізнес-процесами.
2. **Зручність обслуговування:**
   - Зменшує складність обслуговування через централізоване управління та підтримку.
3. **Єдинообразність даних:**
   - Забезпечує єдинообразність та цілісність даних у всіх підсистемах.

Недоліки:

1. **Одна точка відмови:**

- Існує ризик, що в разі відмови центрального сервера весь бізнес може призупинитися.

2. **Складність масштабування:**
   - Масштабування системи може бути ускладненим завданням при зростанні обсягів даних та обробки.
3. **Велике навантаження на центральний сервер:**
   - Завдяки централізованій природі системи, центральний сервер може виникнути як флагманський пункт завантаження.

Приклад в реальному житті: Багато великих корпорацій, таких як Coca-Cola, Nestle, використовують SAP ERP для управління своєю корпоративною діяльністю. Система забезпечує централізований погляд на різні бізнес-процеси, що сприяє ефективному управлінню та прийняттю стратегічних рішень.

1.4.2 Криптовалютна система - Bitcoin

Реальний приклад децентралізованої архітектури- це криптовалютна система Bitcoin.

Рисунок 1.10. Bitcoin

Bitcoin є децентралізованою криптовалютною системою, яка базується на технології блокчейн. Блокчейн - це розподілена база даних, яка включає у себе послідовні блоки транзакцій, і кожен учасник мережі має копію цієї бази даних.

Основні риси децентралізованої архітектури в Bitcoin:

1. **Розподілені вузли:**
   - Кожен учасник (вузол) мережі Bitcoin має копію блокчейну, що забезпечує розподіл та резервне копіювання даних.
2. **Децентралізована обробка транзакцій:**
   - Транзакції в мережі Bitcoin обробляються децентралізовано - жоден центральний орган не має контролю над процесом.
3. **Система консенсусу:**
   - Всі вузли в мережі працюють разом для досягнення консенсусу щодо стану блокчейну, використовуючи консенсус-протокол Proof of Work (PoW).
4. **Децентралізована емісія:**
   - Процес емісії нових біткойнів також децентралізований, і відбувається через механізм "майнінгу" (видобутку) за участю різних гравців в мережі.

Переваги:

1. **Стійкість до цензури:**
   - Децентралізована природа Bitcoin ускладнює спроби цензури чи маніпуляції даними.
2. **Висока стійкість до відмов:**
   - Завдяки розподіленій природі мережі, вона стає менш вразливою до атак та відмов.
3. **Безпека:**
   - Криптографічні принципи та мережеві протоколи забезпечують високий рівень безпеки та конфіденційності.

Недоліки:

1. **Масштабність:**

- За високого попиту на мережу Bitcoin, обробка транзакцій може бути ускладненою, що призводить до затримок та високих комісій.

2. **Витрати енергії:**
   - Алгоритм PoW, який використовується для майнінгу, вимагає великої кількості обчислювальної потужності та, відповідно, енергії.

Більше ніж десяти років Bitcoin успішно функціонує як децентралізована криптовалютна система. Тисячі майнерів усього світу приєдналися до мережі, утримуючи та розвиваючи її децентралізовану природу. Bitcoin використовує технологію блокчейн для надійності та прозорості транзакцій, не потребуючи посередників чи центральних органів контролю.

1.4.3 Microsoft Azure

Microsoft Azure - це хмарна платформа, яка надає широкий спектр хмарних послуг, включаючи обчислення, зберігання даних, машинне навчання, аналіз даних та багато іншого. Azure використовує гібридну архітектуру, яка поєднує хмарні ресурси з локальними інфраструктурами підприємств.

Рисунок 1.11. Microsoft Azure

Основні риси гібридної архітектури в Microsoft Azure:

1. **Локальні і хмарні ресурси:**
   - Користувачі можуть використовувати як хмарні, так і локальні ресурси в залежності від своїх потреб та вимог.
2. **Єдина точка керування:**

- Azure пропонує єдиний портал для керування як хмарними, так і локальними ресурсами, що полегшує адміністрування.

3. **Збереження даних:**
   - Можливість зберігання даних як у хмарі, так і на локальних серверах, з можливістю синхронізації та обміну даними між ними.
4. **Розподілені обчислення:**
   - Використання хмарних ресурсів для розподілених обчислень, але з можливістю інтеграції з локальними серверами для обробки даних.
5. **Безпека та конфіденційність:**
   - Захист даних, включаючи механізми шифрування та інші засоби безпеки, які застосовуються як до хмарних, так і до локальних обчислювальних ресурсів.

Переваги:

1. **Гнучкість та масштабованість:**
   - Компанії можуть легко розширювати свою інфраструктуру, використовуючи хмарні ресурси при необхідності, і управляти ними разом зі своєю локальною інфраструктурою.
2. **Збалансована ефективність та економія:**
   - Гібридна архітектура дозволяє підприємствам зберігати критичні дані на локальних серверах, а менш критичні дані - в хмарі, забезпечуючи оптимальне використання ресурсів.
3. **Захист даних і резервне копіювання:**
   - Можливість забезпечення резервного копіювання та відновлення даних як у хмарі, так і на локальних пристроях.

Недоліки:

1. **Складність конфігурації:**
   - Для належного використання гібридної архітектури може виникнути потреба у складній конфігурації та інтеграції різних ресурсів.
2. **Залежність від доступності хмари:**

– При гібридній архітектурі компанії все ще можуть бути залежними від доступності хмарних ресурсів.

1.5. Важливість та застосування різних видів архітектур

В захищеної Локальної обчислювальної мережі наземного сегменту авіаційного комплексу, важливість для застосування різних видів архітектур можуть бути розглянуті з кількох ключових точок зору.

1. **Централізована архітектура:**

   Виділення ролі та управління:

   – Централізована архітектура дозволяє ефективно розподіляти завдання та керувати ресурсами мережі з центрального вузла. У випадку авіаційного комплексу, це може означати централізоване управління всіма обчислювальними процесами на наземному рівні.

   Безпека та виявлення загроз:

   – Централізована система спрощує впровадження засобів безпеки та систем виявлення загроз, оскільки всі дані можуть бути аналізовані та контрольовані в єдиному пункті. Це сприяє швидкій реакції на потенційні кіберзагрози.

2. **Децентралізована архітектура:**

   Розділення завдань та стійкість до відмов:

   – Децентралізована архітектура може бути корисною для розділення завдань між різними вузлами, що забезпечує стійкість до відмов. У випадку великої системи авіаційного комплексу, це дозволяє розподілити завдання та зменшити ризик зупинки всієї системи через відмову одного елемента.

   Масштабованість:

   – Децентралізована архітектура забезпечує більшу масштабованість, оскільки може легко додавати нові вузли та ресурси, що є важливим аспектом для систем, які можуть зростати у розмірах.

3. **Гібридна архітектура:**

Оптимальне використання ресурсів:

– Гібридна архітектура дозволяє поєднувати переваги централізованого та децентралізованого підходів. Це може бути корисно для оптимального використання ресурсів та забезпечення гнучкості системи.

Резервування та відновлення:

– Гібридна архітектура дозволяє впроваджувати стратегії резервування та відновлення, що є важливим для надійності системи в умовах авіаційного комплексу.

Загальною метою використання різних архітектур є забезпечення ефективності, безпеки та стійкості системи наземного сегменту авіаційного комплексу. Вибір конкретного підходу може бути обумовлений вимогами до системи, її розміром, специфікою обчислювальних завдань та вимогами до безпеки.

1.6. Збір даних про компаній-авіаперевізників

Програмний модуль для збору даних про авіаперевізників може використовувати методи веб-скрапінгу для отримання інформації з онлайнових сервісів продажу авіаквитків. Наприклад, він може переглядати веб-сторінки популярних сайтів, таких як *Expedia*, Skyscanner, або Kayak, і збирати дані про ціни на рейси, час вильоту, час прибуття, авіакомпанії та інші важливі параметри.

Основні етапи роботи такого модуля можуть включати:

1. **Визначення параметрів для аналізу**: Встановлення критеріїв, які модуль буде враховувати, таких як дати вильоту, напрямки, авіакомпанії, клас обслуговування і так далі.
2. **Веб-скрапінг**: Модуль може використовувати веб-скрапінг для перегляду вмісту веб-сайтів і витягування потрібної інформації. Це може включати в себе отримання HTML-коду сторінок, аналіз його та вилучення потрібних даних.
3. **Зберігання даних**: Отримані дані можуть бути збережені в базі даних для подальшого аналізу. Наприклад, вони можуть містити інформацію про ціни, авіакомпанії, тривалість польоту, пересадки тощо.

4. **Аналіз і агрегація**: Модуль може проводити аналіз отриманих даних, виявляти тенденції, порівнювати ціни на різних авіакомпаніях, рейсах та інші фактори. Також, він може агрегувати дані для створення зручного інтерфейсу для користувача.
5. **Оновлення інформації**: Модуль повинен регулярно оновлювати свою базу даних, щоб користувачі отримували актуальну інформацію.

Зважаючи на велику кількість даних, яку слід збирати і обробляти, ефективність такого модуля значно залежить від технологій, які використовуються для веб-скрапінгу, обробки даних та зберігання інформації. Також важливо враховувати правові аспекти і не порушувати правила використання вмісту веб-сайтів.

1.7. Загальний аналіз існуючих методів та технологій захисту ЛОМ

Загальний аналіз існуючих методів та технологій захисту ЛОМ (Локальної обчислювальної мережі) наземного сегменту авіаційного комплексу включає розгляд різних аспектів та викликів, пов'язаних із забезпеченням безпеки та стійкості системи. Ось деякі ключові елементи цього аналізу:

1. **Шифрування та Криптографія:**

Захист конфіденційності- використання сучасних алгоритмів шифрування для захисту конфіденційності даних, передаваних у мережі.

Цілісність даних- використання хеш-функцій та цифрових підписів для перевірки цілісності даних та автентифікації взаємодіючих сторін.

2. **Безпека мережевого рівня:**

Брандмауери та IDS/IPS системи: застосування брандмауерів для контролю доступу та систем виявлення та запобігання вторгнення (IDS/IPS) для виявлення та реагування на потенційні загрози.

VPN технології: використання віртуальних приватних мереж (VPN) для шифрування трафіку та забезпечення безпечного підключення віддалених точок.

3. **Фізична безпека:**

Захист доступу до обладнання: встановлення фізичних обмежень та заходів безпеки для запобігання несанкціонованому доступу до обладнання ЛОМ.

Резервне електроживлення:впровадження систем резервного електроживлення для уникнення втрати доступу до мережі в разі відмови основного джерела енергії.

4. **Управління ідентифікацією та доступом:**

Системи одноразового входу (*OTP*): використання технологій OTP для ускладнення процесу аутентифікації та підвищення рівня безпеки доступу.

Методи багаторівневої ідентифікації: застосування багаторівневих систем ідентифікації, які включають в себе біометричні дані, паролі та інші аспекти для підвищення безпеки.

5. **Аудит безпеки та моніторинг:**

Системи аудиту та журналювання: розгортання систем, що ведуть журнал подій та аудиту безпеки, для моніторингу активності та виявлення аномальних поведінок.

Аналіз вразливостей: регулярне проведення аналізу вразливостей та патчінг систем для зменшення ризиків витоку інформації.

Цей загальний аналіз слугує підґрунтям для розробки та впровадження комплексних стратегій захисту ЛОМ наземного сегменту авіаційного комплексу, враховуючи різноманітні аспекти безпеки в інформаційно-технічному середовищі.

1.8. Ідентифікація потенційних загроз та ризиків для наземного сегменту

Ідентифікація потенційних загроз та ризиків для наземного сегменту авіаційного комплексу є важливим етапом в розробці стратегії безпеки. Нижче представлено кілька типових загроз та ризиків, які можуть виникнути у зазначеному контексті:

1. **Кіберзагрози:**

Мережеві атаки: Атаки на мережевий рівень, такі як DDoS атаки або перехоплення трафіку, можуть призвести до перерви в роботі системи.

Віруси та шкідливе програмне забезпечення*:* Інфікування систем вірусами або шкідливим програмним забезпеченням може призвести до втрати конфіденційної інформації або навіть втрати контролю над системою.

2. **Фізичні загрози:**

Пожежа та повінь: Фізичні стихійні лиха можуть призвести до знищення обладнання та інфраструктури, що впливає на доступність та надійність систем.

Крадіжка обладнання: Крадіжка обладнання може призвести до втрати даних або навіть до неправомірного використання технічних ресурсів.

3. **Ідентифікація та аутентифікація:**

Недостатня аутентифікація: Слабкі системи аутентифікації можуть стати об'єктом атак і привести до несанкціонованого доступу.

Піддавання атакам на ідентифікацію: Атаки на системи ідентифікації можуть викликати проблеми конфіденційності та навіть втрати доступу до ключових ресурсів.

4. **Управління конфіденційністю та приватністю:**

Протоколювання некоректне обробка даних: Некоректне оброблення конфіденційної інформації під час протоколювання може призвести до витоку даних.

Порушення політик конфіденційності: Невідповідність внутрішнім або законодавчим політикам конфіденційності може мати серйозні юридичні наслідки.

5. **Управління вразливостями:**

Відкриті вразливості: Недостатня патчінг систем та програмного забезпечення може залишити систему вразливою до відомих атак.

Соціальний інжиніринг: Атаки, які використовують соціальний інжиніринг, можуть викликати зловживання довіри персоналу та вивести їх на інформаційний обман.

Ідентифікація цих загроз і ризиків є основою для розробки та впровадження стратегій безпеки та захисту ЛОМ наземного сегменту авіаційного комплексу. Регулярний моніторинг, аудит та оновлення заходів захисту є необхідними для забезпечення ефективного функціонування системи в умовах змінюючогося середовища загроз.

1.9. Висновки до розділу

У контексті дослідження "Захищена ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою" стає очевидним, що в сучасному світі, де

зростає залежність від технологій та збільшується обсяг цифрової інформації, проблеми безпеки стають важливішими, ніж будь-коли. Потреба у захисті інформації та надійності функціонування систем стає ключовою для забезпечення безпеки та стабільності авіаційного комплексу.

Визначена проблема стосується захисту локальних обчислювальних мереж наземного сегменту, які відіграють важливу роль у забезпеченні безперебійності та ефективності авіаційних операцій. Аналіз існуючих методів та технологій захисту дозволяє визначити сучасні виклики та ризики, з якими стикаються ці системи.

В процесі дослідження було виявлено, що централізована архітектура є однією з потенційних стратегій для захисту ЛОМ. Це дозволяє централізовано керувати та моніторити безпеку, впроваджуючи спеціалізовані заходи для запобігання атакам та виявлення порушень безпеки в реальному часі.

Існують різні види архітектур, такі як децентралізована та гібридна, які також можуть бути розглянуті в контексті забезпечення безпеки ЛОМ. Однак, важливо враховувати, що кожен вид архітектури має свої переваги та недоліки, і їх вибір повинен бути обґрунтованим, враховуючи конкретні потреби та характеристики системи.

Застосування цих підходів та архітектур може значно підвищити рівень безпеки ЛОМ наземного сегменту авіаційного комплексу. Результати дослідження вказують на актуальність теми та важливість розробки та впровадження захисних стратегій у цій області для забезпечення стійкості та надійності авіаційних систем у сучасному цифровому середовищі.

РОЗДІЛ 2 СИСТЕМНИЙ АНАЛІЗ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

Локальні обчислювальні мережі в межах авіаційних комплексів відіграють важливу роль у керуванні критичною інформацією щодо польотних операцій, даних про пасажирів та стану повітряних суден. Захист цих мереж є обов'язковим, враховуючи вроджену чутливість даних та потенційні наслідки порушень безпеки. У цьому розділі ми глибоко зануримося в теоретичну основу, що оточує проблеми та розглянемо деякі врахування, пов'язані із захистом локальних обчислювальних мереж в авіаційних комплексах.

2.1. Теоретично-технічні аспекти централізованої архітектури захищеної локальної обчислювальної мережі авіаційного сегменту

2.1.1. Чому саме централізована архітектура системи

Вибір між централізованою та розподіленою архітектурою локальної комп'ютерної мережі для наземного сегменту авіаційного комплексу залежить від різних факторів, і немає універсальної відповіді. Обидві архітектури мають свої переваги та недоліки, і рішення повинно базуватися на конкретних вимогах та характеристиках відповідного авіаційного комплексу. Ось деякі важливі аспекти для кожної архітектури:

1. **Централізована архітектура:**

   Переваги:

   - Спрощене управління: Централізовані архітектури часто легше управляти та обслуговувати, оскільки всі ресурси сконцентровані в центральному місці.
   - Підвищена безпека: Легше реалізувати заходи безпеки та протоколи в централізованій системі.
   - Централізоване зберігання даних: Дані можна зберігати в центральному місці, що полегшує їх управління та резервне копіювання.

Недоліки:

- Один точка відмови: Якщо центральний вузол відмовить, може бути порушена вся система.
- Проблеми масштабованості: При збільшенні розміру авіаційного комплексу масштабування централізованої системи може стати більш складним завданням.

2. **Розподілена архітектура:**

Переваги:

- Масштабованість: Розподілені архітектури можна легше масштабувати для задоволення ростучих потреб авіаційного комплексу.
- Покращена продуктивність: Розподіл завдань між кількома вузлами може призвести до кращої продуктивності для певних застосувань.

Недоліки:

- Складність: Управління розподіленою системою може бути складніше, ніж централізованою.
- Виклики безпеки: Забезпечення безпеки комунікації між розподіленими вузлами може бути складніше.

У контексті авіаційного комплексу централізована архітектура часто вважається більш придатною з декількох причин:

1. **Контроль та Управління:**
   - Централізовані архітектури надають одне місце контролю та управління. У авіаційній галузі, де координація та контроль важливі, наявність централізованої системи дозволяє легше відслідковувати та керувати ресурсами мережі.
2. **Безпека:**
   - Централізовані архітектури, як правило, пропонують кращий рівень безпеки. З одним пунктом контролю легше впроваджувати та забезпечувати дотримання політик безпеки, моніторити мережевий трафік та реагувати на можливі загрози невідкладно. Це особливо важливо в

авіаційному секторі, де безпека та цілісність даних є першочерговими завданнями.

3. **Масштабованість:**
   - Централізовані архітектури часто більш легко масштабуються, особливо коли йдеться про розширення мережі для врахування зростаючих потреб авіаційного комплексу. Додавання нових компонентів або вузлів може бути централізовано кероване, спрощуючи розширення інфраструктури без складностей координації змін по всіх розподілених вузлах.
4. **Оптимізація Ресурсів:**
   - У централізованих архітектурах ресурси можна ефективніше оптимізувати. Централізовані сервери можуть бути налаштовані для оптимальної продуктивності та використання ресурсів, що призводить до кращої ефективності. Це важливо в авіаційній сфері, де обробка даних в режимі реального часу та комунікації є критичними.
5. **Терпкість до Відмов та Резервування:**
   - Централізовані архітектури дозволяють легше впроваджувати механізми терпкості до відмов та резервування. Резервні системи та резервні копії можуть бути централізовано управляні, забезпечуючи неперервну роботу у випадку відмов. Це критично в авіації, де надійність системи є найважливішою.
6. **Стійкість Продуктивності:**
   - Централізовані архітектури часто надають більш стабільну продуктивність, оскільки трафік управляється та керується з центрального пункту. Ця передбачуваність важлива в авіаційних застосунках, де час відповіді та латентність мають вирішальне значення.
7. **Відповідність до Регулятивних Вимог:**
   - В авіаційній індустрії часто існують строгі вимоги та стандарти. Централізована архітектура може сприяти дотриманню цих регулятивних вимог, надаючи єдину та легко аудитовану систему.

Хоча централізована архітектура має свої переваги, важливо зауважити, що вибір між централізованою та розподіленою архітектурою повинен базуватися на ретельному аналізі конкретних вимог та обмежень авіаційного комплексу. У деяких випадках може бути найкращим рішенням гібридний підхід, який поєднує елементи обох архітектур.

2.1.2. Безпека централізованої архітектури

Безпека централізованої архітектури в авіаційному сегменті є критичною, оскільки авіаційні системи включають в себе важливі і критичні застосунки, такі як системи керування рейсами, навігаційні системи, системи зв'язку та інші, які забезпечують безпеку і ефективність авіаційного руху.

Ключові аспекти централізованої архітектури в авіаційному сегменті які сприятимуть безпеці:

1. **Фізична безпека:**
   - Забезпечення фізичної безпеки для обладнання, серверних приміщень, дата-центрів і інших інфраструктурних елементів.
   - Обмеження фізичного доступу до критичних систем і забезпечення контролю за обладнанням.
2. **Кібербезпека:**
   - Застосування високих стандартів кібербезпеки для захисту від кібератак, таких як вторгнення, віруси, зловживання привілеїв і інші.
   - Використання систем виявлення та запобігання вторгнень (IDS/IPS) для негайного виявлення та відповіді на потенційні загрози.
3. **Шифрування та Захист Даних:**
   - Використання сильного шифрування для захисту конфіденційності та цілісності даних, які передаються між системами.
   - Регулярне оновлення шифрування та захист від нових методів атак.
4. **Доступ та Аутентифікація:**
   - Ефективне керування ідентифікацією та аутентифікацією користувачів та систем.

- Використання двофакторної аутентифікації для додаткового рівня захисту.

5. **Системи Аудиту та Моніторингу:**
   - Впровадження систем аудиту та моніторингу для виявлення незвичайних подій та слабкі місця в системі безпеки.
   - Активна реакція на попередження та події безпеки для негайного виправлення проблем.
6. **Резервне Копіювання та Відновлення:**
   - Регулярне створення резервних копій даних та систем для відновлення в разі виникнення інцидентів.
   - Проведення тестів відновлення для перевірки ефективності процесів відновлення.
7. **Відповідність та Стандарти:**
   - Дотримання вимог безпеки, визначених авіаційними регуляторами та міжнародними стандартами.
   - Проведення аудитів безпеки для перевірки відповідності та виявлення можливих вразливостей.
8. **Освіта та Навчання:**
   - Навчання персоналу з питань кібербезпеки та безпеки інформаційних технологій.
   - Своєчасне оновлення знань персоналу відносно нових загроз та технологій безпеки.

Загальна безпека авіаційного сегменту вимагає комплексного підходу, який охоплює технічні, організаційні та людські аспекти безпеки. Системи управління безпекою повинні бути гнучкими та відповідати швидкозмінним умовам та загрозам.

2.2. Проблеми захисту локальних обчислювальних мереж в авіаційних комплексах

2.2.1. Вплив зовнішніх факторів на захищеність мережі

Вплив зовнішніх факторів на безпеку мережі - це критичний аспект у контексті авіаційних комплексів або будь-якої організації. Зовнішні фактори можуть суттєво впливати на загальну безпеку мережі. Ключові зовнішні фактори та їх вплив на безпеку мережі:

1. Еволюція кіберзагроз:

Вплив: Динамічний та змінюючийся характер кіберзагрози безпосередньо впливає на безпеку мережі. Виникнення нових кіберзагроз, технік атак та вразливостей створює постійні виклики для безпеки локальних обчислювальних мереж у авіаційних комплексах.

Наслідки: Заходи з безпеки мережі повинні бути адаптивними та реагувати на змінюючіться кіберзагрози. Регулярні оновлення розвідки з загроз, моніторинг у реальному часі та активні заходи оборони є важливими для протидії зростаючим кіберзагрозам.

2. Зміни в регуляторному середовищі та вимоги щодо відповідності:

Вплив: Зміни в регуляторних актах та вимогах щодо відповідності, встановлених авіаційними органами чи уповноваженими органами, можуть суттєво впливати на політику та практику забезпечення безпеки мережі.

Наслідки: Організації повинні слідкувати за оновленнями в законодавстві та забезпечувати відповідність своїх заходів безпеки з останніми стандартами. Невідповідність може вести до правових наслідків та порушити безпеку обчислювальної мережі авіаційного комплексу.

3. Технологічні досягнення:

Вплив: Швидкий технологічний прогрес, такий як впровадження Інтернету речей (*IoT*), хмарних обчислень та автоматизації, може вносити нові виклики та враховувати особливості в області безпеки мережі авіаційного комплексу.

Наслідки: Інтеграція нових технологій вимагає обдуманого врахування можливих наслідків для безпеки. Необхідно впроваджувати надійні засоби безпеки для захисту від потенційних вразливостей, які можуть з'явитися через нові технології.

4. Глобалізація та взаємопов'язані системи:

Вплив: Авіаційні комплекси часто працюють у глобалізованому та взаємозалежному середовищі. Взаємозв'язки з зовнішніми сутностями та системами збільшують поверхню атак та потенційні ризики безпеки.

Наслідки: Необхідно використовувати безпечні протоколи зв'язку, шифрування даних та строгі засоби контролю доступу для зменшення ризиків, пов'язаних із глобальною діяльністю. Співпраця з зовнішніми партнерами повинна супроводжуватися ретельними оцінками безпеки.

5. Безпека ланцюга постачання:

Вплив: Безпека ланцюга постачання, включаючи постачальників та постачальників послуг сторонніх осіб, може впливати на загальну безпеку мережі авіаційного комплексу.

Наслідки: Організації повинні оцінювати практики забезпечення безпеки своїх постачальників та партнерів зі сторонніх осіб. Укладення контрактних зобов'язань щодо стандартів безпеки та регулярні аудити можуть покращити безпеку всього ланцюга постачання.

6. Геополітичні та геостратегічні врахування:

Вплив: Геополітичні чинники, регіональні напруження або кіберконфлікти між націями можуть впливати на безпеку мережі авіаційного комплексу.

Наслідки: Організації повинні бути обережні щодо геополітичних подій і враховувати їх при розробці стратегій ризик-аналізу та безпеки. Періоди збільшеної геополітичної напруженості можуть вимагати підвищеної уваги та активних заходів безпеки.

7. Суспільна увага та сприйняття:

Вплив: Суспільна увага та сприйняття кібербезпекових інцидентів можуть впливати на рівень обережності та очікувань, що виникають щодо мережі авіаційного комплексу.

Наслідки: Організації повинні пріоритизувати прозору комунікацію у випадку кіберінцидентів для ефективного управління сприйняттям громадськості. Кампанії з підвищення обізнаності населення також можуть сприяти культурі кібербезпеки.

Розуміння та врахування впливу цих зовнішніх факторів є важливим для розробки стійкої та адаптивної стратегії забезпечення безпеки мережі в авіаційних комплексах. Це усвідомлення дозволяє організаціям активно реагувати на нові загрози та зміни в кібербезпеці.

2.2.2. Людський фактор в контексті безпеки мережі

Людський фактор є ключовим аспектом в галузі мережевої безпеки, і розуміння ролі осіб у межах організації є важливим для встановлення комплексної безпекової стратегії. Людський фактор охоплює як умисні, так і неумисні дії, які можуть значно впливати на безпеку мережі. Розглянемо ключові аспекти в контексті мережевої безпеки:

1. Свідомість та Навчання Користувачів:

Роль: Користувачі, включаючи співробітників, адміністраторів та сторонніх постачальників, відіграють ключову роль у забезпеченні безпеки мережі.

Важливість: Відсутність свідомості та розуміння найкращих практик безпеки може призвести до неумисного порушення безпеки. Програми навчання є критичними для вибудовування у користувачів розуміння важливості надійних паролів, визнавання атак типу "фішінг" та виконання політик безпеки.

2. Соціальний Інжиніринг:

Роль: Людська вразливість до атак соціального інжинірингу, таких як "фішінг" або "претекстування", може підірвати безпеку мережі.

Важливість: Атакуючі часто використовують психологію людини, щоб змусити осіб розголошувати чутливу інформацію. Постійні освітні та інформаційні програми є необхідними для навчання користувачів впізнавати та протистояти таким тактикам соціального інжинірингу.

3. Контроль доступу та Права Користувачів:

Роль: Неправильно надані права доступу чи привілеї можуть призвести до несанкціонованого доступу до чутливих даних.

Важливість: Впровадження принципу найменшого привілею критично для забезпечення того, що користувачі мають лише той доступ, який необхідний для їхніх

обов'язків. Регулярні огляди та аудити прав користувачів необхідні для забезпечення безпеки мережевого середовища.

4. Управління Паролями:

Роль: Слабкі паролі, їх обмін та неналежне управління паролями можуть призвести до серйозних ризиків безпеки.

Важливість: Впровадження строгих політик паролів, використання мультифакторної аутентифікації (MFA) та навчання користувачів важливості безпечних практик управління паролями - критичні аспекти мережевої безпеки.

5. Внутрішні Загрози:

Роль: Внутрішні агенти, якщо вони мають злий умисел або допускають ненавмисні помилки, можуть становити серйозну загрозу безпеці мережі.

Важливість: Моніторинг поведінки користувачів, ведення журналу активності користувачів та регулярні програми навчання з безпеки є важливими для зменшення ризиків внутрішніх загроз.

6. Політики Використання Особистих Пристроїв (BYOD):

Роль: Використання особистих пристроїв для робочих цілей може внести додаткові виклики для безпеки мережі.

Важливість: Розробка чітких політик BYOD, впровадження систем управління мобільними пристроями (MDM) та навчання користувачів про ризики використання особистих пристроїв для роботи - це важливі аспекти адаптації до змін у робочому середовищі.

7. Кризове Реагування та Звіти про Інциденти:

Роль: Користувачі часто є першою лінією оборони у виявленні та звітності про інциденти безпеки.

Важливість: Заохочення культури швидкої звітності про інциденти та надання користувачам чітких процедур звітності про проблеми забезпечують ефективну відповідь на інциденти безпеки.

8. Культурні Аспекти:

Роль: Організаційна культура може впливати на рівень важливості, який приділяється кібербезпеці.

Важливість: Формування культури безпеки, де особи розуміють свої ролі у збереженні безпечного середовища, є критичним. Керівництво відіграє ключову роль у встановленні тону для культури безпеки.

9. Врахування Праці на Відстані:

Роль: Розширення практики дистанційної роботи вносить нові виклики для безпеки мережі.

Важливість: Навчання віддалених співробітників щодо безпечних практик віддаленого доступу, впровадження безпечних VPN та забезпечення відповідності віддалених пристроїв політикам безпеки є важливими аспектами адаптації до змін у робочому середовищі.

10. Постійний Моніторинг та Аудит:

Роль: Постійний моніторинг діяльності користувачів та періодичні аудити безпеки є важливими для виявлення та вирішення потенційних ризиків безпеки.

Важливість: Регулярні аудити та моніторинг допомагають забезпечити відповідність з політиками безпеки, виявляти аномальну поведінку користувачів та забезпечувати своєчасну відповідь на інциденти безпеки.

Розуміння та врахування людського фактора в мережевій безпеці потребує голістичного підходу, що поєднує технології, політику та освіту. За допомогою відданості освіці та забезпечення особам знань та інструментів для сприяння безпеці, організації можуть значно підвищити загальний рівень безпеки мережі.

2.3. Критерії захищеності локальних мереж в авіаційному сегменті

Захищеність локальних мереж в авіаційному сегменті є критично важливою для забезпечення безпеки польотів і захисту конфіденційної інформації. Ось деякі критерії захищеності для локальних мереж в авіаційному сегменті:

1. **Фізична захищеність:**
   - Захищеність обладнання та інфраструктури від несанкціонованого доступу.
   - Контроль доступу до приміщень, де розташована мережна інфраструктура.
2. **Шифрування даних:**

- Застосування сильного шифрування для захисту конфіденційної інформації в локальній мережі.
- Використання шифрування для захисту комунікацій між різними частинами авіаційної системи.

3. **Аутентифікація та авторизація:**
   - Впровадження сильної системи аутентифікації для управління доступом до мережних ресурсів.
   - Налаштування точного контролю авторизації користувачів залежно від їх ролі та відповідальностей.
4. **Антивірусний захист:**
   - Регулярне оновлення та використання антивірусного програмного забезпечення для виявлення і лікування можливих загроз безпеці.
5. **Моніторинг та журналювання:**
   - Реалізація систем моніторингу для виявлення аномалій і несанкціонованих спроб доступу.
   - Ведення докладних журналів подій для аналізу безпекових інцидентів та їх подальшого усунення.
6. **Фізичне розташування обладнання:**
   - Вибір безпечних місць для розташування серверів та мережного обладнання з метою запобігання фізичним атакам.
7. **Апаратне і програмне забезпечення:**
   - Регулярні оновлення апаратного та програмного забезпечення для усунення відомих вразливостей.
   - Використання тільки ліцензійного та перевіреного програмного забезпечення.
8. **Захист від внутрішніх загроз:**
   - Реалізація політик безпеки для зменшення ризику внутрішніх загроз від співробітників.
   - Обмеження доступу до критично важливих ресурсів відповідно до принципу найменшого можливого доступу.

Ці критерії захищеності допомагають забезпечити цілісність, конфіденційність та доступність локальних мереж в авіаційному сегменті, зменшуючи ризики для безпеки авіаційних систем.

2.4. Аналіз джерел електромагнітного випромінювання та їх вплив на мережу

Аналіз джерел електромагнітного випромінювання та їх вплив на мережу є важливим аспектом забезпечення стійкості та безпеки інформаційних систем. Електромагнітне випромінювання може виникати внаслідок дії різних електричних та електронних пристроїв, а також зовнішніх джерел, таких як електромагнітні бурі чи інші радіочастотні перешкоди. Вплив цього випромінювання на мережу може мати серйозні наслідки для її функціонування та безпеки.

Основні джерела електромагнітного випромінювання, які можуть впливати на мережу:

1. **Електронна апаратура:**
   - Комп'ютери, сервери, маршрутизатори та інші електронні пристрої можуть генерувати електромагнітне випромінювання як побічний ефект своєї роботи.
2. **Комунікаційне обладнання:**
   - Антени, радіопередавачі та інші засоби комунікаційного зв'язку можуть випромінювати електромагнітні хвилі в процесі передачі даних.
3. **Електропоживання:**
   - Напругові спади, перешкоди у мережі живлення та інші аномалії в електричній системі можуть викликати електромагнітне випромінювання.
4. **Зовнішні джерела:**
   - Радіочастотні перешкоди від інших пристроїв, мобільних телефонів, радіостанцій або інших електронних пристроїв.

Вплив електромагнітного випромінювання на мережу може бути наступним:

1. **Перешкоди в передачі сигналів:**

- Електромагнітне випромінювання може впливати на якість сигналу, призводячи до помилок в передачі даних.

2. **Збої в роботі електронного обладнання:**
   - Сильне електромагнітне випромінювання може спричинити збої та відмови в роботі електронної апаратури.
3. **Компрометація безпеки:**
   - Електромагнітне випромінювання може використовуватися для незаконного злому або перехоплення інформації.

Щоб зменшити вплив електромагнітного випромінювання на мережу, можна вжити наступні заходи:

1. **Екранування:**
   - Використання екранів та електромагнітних екранів для захисту електронної апаратури від зовнішніх випромінювань.
2. **Віддалення джерел:**
   - Розташування електронної апаратури вдалеку від потенційних джерел електромагнітного випромінювання.
3. **Фільтрація:**
   - Використання фільтрів та інших заходів для зменшення шумів та електромагнітного випромінювання.
4. **Нормативи та стандарти:**
   - Виконання вимог нормативів та стандартів, що регулюють рівень електромагнітного випромінювання для конкретних пристроїв та систем.
5. **Аудит та моніторинг:**
   - Регулярний аудит та моніторинг рівня електромагнітного випромінювання для виявлення можливих проблем та вжиття заходів для їх усунення.

Аналіз та управління електромагнітним випромінюванням є складною задачею, і його важливо враховувати в рамках загальної стратегії забезпечення безпеки інформаційних систем.

2.5. Опис основних алгоритмів захисту та управління захищеною локальною обчислювальною мережею

Охорона та управління захищеною обчислювальною мережею включає в себе використання різноманітних алгоритмів та протоколів для забезпечення конфіденційності, цілісності та доступності даних. Розглянемо основні алгоритми, які використовуються для захисту та управління захищеною обчислювальною мережею:

1. Алгоритми брандмауера:

- **Опис:** Брандмауери використовують набір алгоритмів для керування вхідним та вихідним мережевим трафіком на основі заздалегідь визначених правил безпеки. *Stateful inspection*, проксі-фільтрація та фільтрація пакетів - це загальні алгоритми, які використовуються брандмауерами для аналізу, дозволу чи блокування даних пакетів.

2. Алгоритми виявлення та запобігання вторгненням:

- **Опис:** Системи виявлення вторгнень та системи запобігання вторгненням використовують алгоритми для моніторингу мережевої чи системної діяльності на предмет зловмисних дій чи порушень політики безпеки. Виявлення аномалій, виявлення на основі сигнатур та виявлення на основі евристичних методів - це загальні алгоритми, які використовуються в цих системах.

3. Алгоритми шифрування:

- **Опис:** Алгоритми шифрування використовуються для захисту даних в русі та у спокої. До загальних алгоритмів шифрування належать *Advanced Encryption Standard (AES), Triple DES (3DES)* та *RSA*. Ці алгоритми забезпечують те, що несанкціоновані користувачі не можуть розшифрувати чутливу інформацію.

4. Алгоритми контролю доступу:

- **Опис:** Алгоритми контролю доступу визначають, хто може отримати доступ до яких ресурсів у мережі. Контроль доступу на основі ролей, контроль доступу за власним бажанням та контроль доступу за власним бажанням - це приклади алгоритмів контролю доступу, які регулюють права користувачів на основі ролей, власності чи міток безпеки.

5. Алгоритми віртуальної приватної мережі (*VPN*):

- **Опис:** *VPN* використовують алгоритми шифрування та протоколи тунелювання, такі як *IPsec* чи *SSL/TLS*, для встановлення безпечних з'єднань через публічні мережі. Ці алгоритми забезпечують, що дані, які передаються між вузлами мережі, залишаються безпечними та приватними.

6. Алгоритми моніторингу мережі:

- **Опис:** Алгоритми моніторингу мережі аналізують мережевий трафік, виявляють аномалії та генерують сповіщення. Алгоритми для перехоплення пакетів, аналізу потоку та статистичного виявлення аномалій допомагають виявляти підозрілі дії або проблеми з продуктивністю.

7. Алгоритми реагування на вторгнення:

- **Опис:** Алгоритми реагування на вторгнення визначають, як система повинна реагувати на виявлені випадки порушення безпеки. Автоматизовані відповіді, такі як блокування *IP*-адрес або ізоляція компрометованих пристроїв, можуть бути активовані на основі заздалегідь визначених алгоритмів.

8. Алгоритми хешування (для цілісності даних):

- **Опис:** Алгоритми хешування, такі як *SHA-256* або *MD5*, використовуються для генерації хеш-значень фіксованого розміру з даних. Ці хеш-значення служать цифровими відбитками пальців, що дозволяє виявляти будь-які зміни чи пошкодження даних.

9. Алгоритми цифрового підпису:

- **Опис:** Алгоритми цифрового підпису, такі як *RSA* або *DSA*, забезпечують можливість перевірки автентичності та цілісності цифрових повідомлень або документів. Вони використовують пари ключів для підпису та перевірки підписів.

2.6. Особливості локальних обчислювальних мереж в наземному сегменті авіаційного комплексу

Локальні обчислювальні мережі в наземному сегменті авіаційного комплексу мають специфічні особливості та вимоги, адаптовані до потреб авіаційної індустрії.

Наземний сегмент включає в себе різноманітні діяльності та системи на землі, які підтримують та керують експлуатацією літаків. Ось кілька особливостей локальних обчислювальних мереж в наземному сегменті авіаційного комплексу:

1. **Безпека та Надійність:**
   - Безпека та надійність мають вирішальне значення в авіації. ЛКМ повинні бути розроблені з метою забезпечення надійної та безпечної роботи систем на землі, таких як контроль повітряного руху, моніторинг погоди та системи зв'язку.
2. **Дублювання та Автономія:**
   - Дублювання є важливим для мінімізації ризику відмов мережі. В авіаційних ЛКМ часто впроваджують системи з дублюванням та автоматичним переключенням для забезпечення неперервної роботи, особливо у критичних застосунках.
3. **Комунікації в реальному часі:**
   - Авіаційні операції ґрунтуються на обміні даними в реальному часі для таких завдань, як контроль повітряного руху, моніторинг погоди та відстеження повітряних суден. ЛКМ повинні надавати пріоритет комунікаціям з низькою затримкою для підтримки цих критичних функцій.
4. **Інтеграція з Авіаційними Системами:**
   - ЛКМ в наземному сегменті повинні безперешкодно інтегруватися з різними авіаційними системами, включаючи радарні системи, навігаційні системи та системи зв'язку на землі. Сумісність та взаємодія є ключовими аспектами.
5. **Безпека та Контроль Доступу:**
   - Безпека є пріоритетом через чутливий характер авіаційних операцій. ЛКМ повинні використовувати надійні заходи безпеки, такі як контроль доступу, шифрування та системи виявлення вторгнень для захисту від несанкціонованого доступу та кіберзагроз.
6. **Вимоги до Ширина Полоси:**

- Застосунки авіації часто генерують великі обсяги даних, такі як радарні дані та інформація про погоду. ЛКМ в наземному сегменті повинні мати достатню ширину полоси для обробки великого об'єму інтенсивних даних.

7. **Екологічні Умови:**
   - ЛКМ на землі можуть зазнавати впливу важких умов навколишнього середовища, таких як екстремальні температури, електромагнітні перешкоди та фізичні вібрації. Обладнання мережі повинно бути зроблене стійким до цих умов.
8. **Відповідність Авіаційним Стандартам:**
   - ЛКМ авіаційного комплексу повинні відповідати галузевим стандартам та нормативам, таким як ті, які визначаються Міжнародною цивільною авіаційною організацією (ІКАО) та відповідними національними авіаційними владами. Дотримання цих стандартів гарантує безпеку та надійність мережі.
9. **Масштабованість:**
   - Здатність масштабування інфраструктури мережі має важливе значення, особливо в динамічних умовах авіаційного середовища. ЛКМ повинні бути розроблені так, щоб можна було легко додавати нові системи та технології без втрати продуктивності та безпеки.
10. **Відновлення під час Надзвичайних Ситуацій та Планування Кризових Ситуацій:**
    - Завдяки критичному характеру авіаційних операцій ЛКМ повинні мати ефективні плани відновлення під час надзвичайних ситуацій та планировані заходи для управління кризовими ситуаціями. Ці плани забезпечують швидке відновлення мережі після порушень та продовження підтримки важливих функцій.

Отже, локальні комп'ютерні мережі в наземному сегменті авіаційного комплексу мають унікальні виклики, пов'язані з безпекою, надійністю, комунікаціями в реальному часі та іншими аспектами. Дотримання галузевих стандартів та

безперешкодна інтеграція з авіаційними системами є важливими елементами успішного проектування та утримання ефективних ЛКМ в цьому контексті.

2.7. Висновки до розділу

У розділі "Системний аналіз захищеної ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою" були розглянуті ключові аспекти, пов'язані із захистом та управлінням локальною обчислювальною мережею (ЛОМ) в авіаційному сегменті, зосереджуючись на централізованій архітектурі.

Дослідження теоретичних аспектів централізованої архітектури вказує на її відмінності та переваги у контексті авіаційного комплексу. Ця архітектура надає єдиноцентральний пункт управління та координації, сприяючи ефективній інтеграції різноманітних систем та вдосконаленню взаємодії.

Вибір централізованої архітектури обумовлено необхідністю ефективного керування та забезпечення високого рівня координації в умовах високотехнологічного та вимогливого середовища авіаційного комплексу.

Проаналізовано заходи безпеки для централізованої архітектури, зокрема використання брандмауерів, систем виявлення вторгнень та шифрування, що сприяє надійності та конфіденційності мережі.

Виділено та проаналізовано проблеми, що можуть виникнути при захисті ЛОМ в авіаційних комплексах, включаючи вразливості, пов'язані із зовнішніми атаками та людським фактором.

Розглянуто вплив зовнішніх факторів, зокрема електромагнітного випромінювання, на стійкість мережі. Розроблено стратегії для мінімізації впливу таких факторів.

Звернута увага на важливість врахування людського фактора в системах безпеки мережі. Пропонуються навчальні та свідомість-збільшувальні заходи для зменшення ризиків, пов'язаних з людськими помилками.

Розглянуті критерії захищеності ЛОМ, включаючи стандарти безпеки та вимоги до них, які є ключовими для забезпечення ефективності та стійкості мережі.

Вивчено та проаналізовано джерела електромагнітного випромінювання та їх можливий вплив на ефективність та безпеку мережі в авіаційному сегменті.

Надано детальний опис основних алгоритмів, таких як алгоритми брандмауера, виявлення та запобігання вторгненням, шифрування, контролю доступу та інших, які забезпечують ефективний захист мережі.

Ретельно описані особливості ЛОМ у наземному сегменті авіаційного комплексу, враховуючи специфічні вимоги та умови цього сегменту.

У результаті проведеного аналізу можна зробити висновок, що використання централізованої архітектури в системі захищеної ЛОМ для наземного сегменту авіаційного комплексу є обгрунтованим та ефективним рішенням, забезпечуючи високий рівень безпеки та оптимальне управління мережею. Висновки розділу системного аналізу будуть використані в подальших етапах розробки та реалізації проекту для забезпечення максимальної ефективності та надійності системи.

РОЗДІЛ 3 ВПРОВАДЖЕННЯ СИСТЕМИ ПРОТОКОЛІВ ЗАХИСТУ ЛОМ НАЗЕМНОГО СЕГМЕНТУ АВІАЦІЙНОГО КОМПЛЕКСУ З ЦЕНТРАЛІЗОВАНОЮ АРХІТЕКТУРОЮ

У даному розділі дослідження зосереджено на впровадженні системи протоколів захисту для локальної обчислювальної мережі (ЛОМ) наземного сегменту авіаційного комплексу з централізованою архітектурою. Обрані протоколи враховують специфіку авіаційного сектору та вимоги до безпеки, забезпечуючи найвищий рівень захисту та ефективність.

1. **VPN (Virtual Private Network):** Використання VPN дозволяє забезпечити безпеку передачі даних між різними підсистемами наземного сегменту. Це особливо важливо для забезпечення конфіденційності та цілісності даних, передаваних через локальну мережу. VPN встановлює зашифроване з'єднання, що робить його ідеальним вибором для передачі чутливої інформації.
2. **SSL/TLS (Secure Sockets Layer / Transport Layer Security):** Протоколи SSL/TLS використовуються для шифрування даних в етапі передачі через мережу. Вони забезпечують захист від проміжних атак та гарантують конфіденційність і цілісність інформації між різними вузлами мережі.
3. **IPsec (Internet Protocol Security):** IPsec використовується для захисту трафіку на рівні IP, надаючи аутентифікацію та шифрування на рівні пакетів. Цей протокол забезпечує високий рівень безпеки для комунікації між різними компонентами авіаційного комплексу.
4. **SIEM (Security Information and Event Management):** SIEM система виявляє та аналізує події в мережі, що дозволяє оперативно реагувати на потенційні загрози та виявляти аномалії в системі безпеки ЛОМ.
5. **IDPS (Intrusion Detection and Prevention Systems):** IDPS виявляє та блокує спроби несанкціонованого доступу чи атак на мережу. Вони грають важливу роль у попередженні інцидентів та захисті від загроз зовнішнього середовища.

6. **Firewalld:** Використання Firewalld дозволяє контролювати та фільтрувати мережевий трафік, що проходить через локальну обчислювальну мережу. Це забезпечує додатковий рівень захисту від несанкціонованого доступу та атак.
7. **802.1X Authentication:** 802.1X Authentication впроваджує механізми аутентифікації, що гарантують, що тільки вповноважені користувачі та пристрої мають доступ до мережі, зменшуючи ризик несанкціонованого доступу.

Всі обрані протоколи взаємодіють для створення комплексної системи захисту, яка ефективно протистоять різним видам загроз та забезпечує надійний рівень безпеки для локальної обчислювальної мережі авіаційного сегменту з централізованою архітектурою. Це дозволяє забезпечити стабільну та безпечну роботу системи в умовах зростаючих викликів у галузі авіаційної безпеки.

3.1. Налаштування VPN для локальної обчислювальної мережі з централізованою архітектурою

У цьому уявному сценарії буде використовуватися протокол OpenVPN та централізований сервер для забезпечення VPN-з'єднань.

Крок 1: Налаштування централізованого сервера

1. **Встановлення сервера:**
   - На централізованому сервері (наприклад, з IP-адресою 203.0.113.1), необхідно встановити OpenVPN Server.
2. **Генерація ключів:**
   - Необхідно згенерувати SSL-ключі для сервера та клієнтів:

openssl genpkey -algorithm RSA -out server-key.pem

openssl req -new -key server-key.pem -out server-csr.pem

openssl x509 -req -days 365 -in server-csr.pem -signkey server-key.pem -out server-cert.pem

Цей код використовує утиліту OpenSSL для створення ключа, запиту на отримання сертифіката (CSR), та підпису сертифіката для використання в SSL/TLS з'єднанні.

Ось кроки, які виконуються кожною командою:

***openssl genpkey -algorithm RSA -out server-key.pem**:* Генерує закритий ключ *(**server-key.pem**)* для алгоритму RSA. Цей ключ буде використовуватися для захищення з'єднання SSL/TLS.

***openssl req -new -key server-key.pem -out server-csr.pem**:* Створює запит на отримання сертифіката (CSR). CSR містить публічний ключ та інші інформаційні дані, які використовуються для отримання сертифіката від центру сертифікації.

***openssl x509 -req -days 365 -in server-csr.pem -signkey server-key.pem -out server-cert.pem**:* Підписує сертифікат *(**server-cert.pem**)* за допомогою приватного ключа, який був згенерований раніше. Сертифікат отримує термін дії 365 днів *(**-days 365**)*, після чого його слід оновити.

Після виконання цих трьох команд буде отримано закритий ключ *(**server-key.pem**),* запит на отримання сертифіката *(**server-csr.pem**)*, та підписаний сертифікат *(**server-cert.pem**)*. Ці файли можна використовувати для налаштування сервера з підтримкою *SSL/TLS*.

3. **Налаштування OpenVPN:**

Необхідно створити конфігураційний файл для OpenVPN, нехай це буде *server.conf,* визначивши параметри, такі як мережа, підсистема шифрування тощо.

port 1194

proto udp

dev tun

ca /path/to/server-cert.pem

cert /path/to/server-cert.pem

key /path/to/server-key.pem

dh /path/to/dh.pem

server 10.8.0.0 255.255.255.0

Цей код представляє собою конфігураційний файл для OpenVPN сервера.

port 1194: Вказує порт, на якому працюватиме сервер.

proto udp: Встановлює протокол транспорту. Наразі використовується протокол *UDP*.

dev tun: Вказує, що *OpenVPN* повинен використовувати універсальний тунельний інтерфейс (*TUN*).

ca /path/to/server-cert.pem: Вказує шлях до файлу сертифіката центрального органу (*Certificate Authority - CA*). Цей сертифікат використовується для перевірки валідності інших сертифікатів.

cert /path/to/server-cert.pem: Вказує шлях до серверного сертифіката. Цей сертифікат ідентифікує сервер.

key /path/to/server-key.pem: Вказує шлях до приватного ключа сервера, який використовується для розшифрування трафіку.

dh /path/to/dh.pem: Вказує шлях до файлу параметрів Діффі-Хеллмана, які використовуються для забезпечення безпеки обміну ключами.

server 10.8.0.0 255.255.255.0: Визначає підмережу, яку буде використовувати *OpenVPN* для надання *IP*-адрес клієнтам.

Цей конфігураційний файл визначає базові налаштування *OpenVPN* сервера. Важливо враховувати, що для коректної роботи системи, вам також потрібно налаштувати файрвол та інші параметри забезпечення, а також створити відповідні сертифікати для взаємодії між сервером і клієнтами.

4. **Запуск OpenVPN:**

Тепер необхідно запустити OpenVPN з конфігурацією сервера:

openvpn --config /path/to/server.conf

Цей код викликає команду *OpenVPN* з параметром ***--config***, який вказує шлях до конфігураційного файлу сервера *VPN*. Основна ідея полягає в тому, щоб запустити *OpenVPN* і передати йому конфігураційний файл для налаштування *VPN*-з'єднання.

Крок 2: Налаштування локальних вузлів

1. На кожному локальному вузлі необхідно встановіти *OpenVPN*-клієнт.
2. Далі необхідно згенерувати *SSL*-ключі для кожного клієнта:

openssl genpkey -algorithm RSA -out client1-key.pem

Ця команда генерує новий *RSA*-ключ і записує його у файл ***client1-key.pem***.

openssl req -new -key client1-key.pem -out client1-csr.pem

команда використовує створений *RSA*-ключ ***client1-key.pem*** для створення запиту на підпис сертифіката (*CSR*). Результат записується у файл ***client1-csr.pem***.

openssl x509 -req -days 365 -in client1-csr.pem -signkey client1-key.pem -out client1-cert.pem

Ця команда використовує *CSR* з файлу ***client1-csr.pem*** та підписує його власним приватним ключем з файлу ***client1-key.pem***. Результат записується у файл ***client1-cert.pem***. Сертифікат буде дійсний протягом 365 днів ***(-days 365***).

3. Налаштування *OpenVPN*-клієнта:

Далі необхідно створити конфігураційний файл для *OpenVPN* на кожному локальному вузлі. Файл буде ***client1.conf***. Далі буде представлений код дії та опис його кожного параметру

client Вказує, що це конфігурація для клієнта, а не для сервера

dev tun Вказує тип пристрою, що використовується для з'єднання. У цьому випадку використовується тунельний пристрій (tun).

proto udp Вказує, що для передачі даних використовується протокол UDP.

remote 203.0.113.1 1194 Вказує *IP*-адресу та порт сервера, до якого клієнт буде підключатися.

resolv-retry infinite Задає спроби вирішення *DNS*-імені нескінченно, якщо вони не вдалися.

nobind Запобігає прив'язці до конкретного локального порту та *IP*-адреси.

ca /path/to/server-cert.pem Вказує шлях до файлу з корневим сертифікатом сервера.

cert /path/to/client1-cert.pem Вказує шлях до файлу з сертифікатом клієнта.

key /path/to/client1-key.pem Вказує шлях до файлу з особистим ключем клієнта.

4. Запуск *OpenVPN*-клієнта

На цьому етапі необхідно запустити *OpenVPN* на кожному локальному вузлі з відповідною конфігурацією

openvpn --config /path/to/client1.conf

Тепер, локальні вузли можуть встановлювати *VPN*-з'єднання з централізованим сервером через *OpenVPN*. Необхідно забезпечити належний захист ключів та налаштувань для безпеки мережі.

3.2. Налаштування Secure Sockets Layer (SSL) / Transport Layer Security (TLS) для локальної обчислювальної мережі з централізованою архітектурою.

Крок 1: Генерація SSL / TLS ключів та сертифікатів для сервера:

1. **Генерація серверного ключа:**

openssl genpkey -algorithm RSA -out server-key.pem

Цей код використовує утиліту OpenSSL для генерації приватного ключа за алгоритмом RSA.

-out server-key.pem: Задає ім'я файлу, в який буде збережений згенерований приватний ключ. У цьому випадку файл називатиметься ***server-key.pem***.

Після виконання цього коду буде створений файл ***server-key.pem***, який містить приватний ключ, згенерований за алгоритмом *RSA*. Приватний ключ використовується для різноманітних цілей, зазвичай для шифрування та розшифрування інформації або для підпису даних.

2. **Генерація запиту на сертифікат (*CSR*):**

openssl req -new -key server-key.pem -out server-csr.pem

Цей код використовує командний рядок *OpenSSL* для створення запиту на підпис нового сертифіката (CSR - Certificate Signing Request).

- ***openssl***: це команда для виклику *OpenSSL*, криптографічної утиліти для роботи з шифруванням і сертифікатами.
- ***req***: цей підкомандний параметр вказує, що виконується операція пов'язана із запитами на сертифікати.
- ***-new***: цей параметр вказує на створення нового сертифікату чи запиту на сертифікат.
- ***-key server-key.pem***: це вказує шлях до ключового файлу (***server-key.pem***), який буде використаний для генерації сертифікату.

- ***-out server-csr.pem***: це вказує шлях та ім'я файлу, куди буде збережений створений запит на сертифікат (***server-csr.pem***).

3. **Підписання сертифікату:**

openssl x509 -req -days 365 -in server-csr.pem -signkey server-key.pem -out server-cert.pem

- ***openssl:*** це команда для виклику утиліти OpenSSL.
- ***x509:*** підкоманда, яка дозволяє працювати з X.509 сертифікатами.
- ***-req:*** вказує, що вхідний файл є запитом на підпис сертифіката.
- ***-days 365:*** вказує термін дії сертифіката у днях (у цьому випадку - 365 днів).
- ***-in server-csr.pem:*** вказує вхідний файл, який є запитом на підпис.
- ***-signkey server-key.pem:*** вказує файл з приватним ключем, який буде використовуватися для підпису сертифіката.
- ***-out server-cert.pem:*** вказує вихідний файл, в який буде записаний підписаний сертифікат.

Цей код призначений для того, щоб підписати сертифікат (*CSR - Certificate Signing Request*), використовуючи приватний ключ, та згенерувати цифровий сертифікат *X.509*.

Крок 2: Налаштування сервера для використання SSL / TLS:

Необхідно встановити і налаштувати *Apache*

1. Генерація SSL-ключа та сертифіката:

Створення приватного ключа

openssl genpkey -algorithm RSA -out server-key.pem

Створення запиту на підпис сертифіката (CSR)

openssl req -new -key server-key.pem -out server-csr.pem

Підпис сертифіката користувацьким центром або самопідпис

openssl x509 -req -days 365 -in server-csr.pem -signkey server-key.pem -out server-cert.pem

2. Налаштування веб-сервера

Необхідно включити модуль ***ssl*** командою:

sudo a2enmod ssl

Далі необхідно налаштувати віртуальний хост за допомогою:

*<VirtualHost *:443>*
ServerName gucalo.com
DocumentRoot /var/www/html

SSLEngine on
SSLCertificateFile /повний/шлях/до/server-cert.pem
SSLCertificateKeyFile /повний/шлях/до/server-key.pem
</VirtualHost>

- ***<VirtualHost *:443>:*** Визначає початок блоку конфігурації для віртуального хоста, який слухає на порту 443 (стандартний порт для HTTPS).
- ***ServerName gucalo.com:*** Вказує основний домен або IP-адресу віртуального хоста. Необхідно замінити ***gucalo.com*** на справжній домен чи IP-адресу.
- ***DocumentRoot /var/www/html:*** Вказує шлях до директорії, де знаходяться файли веб-сайту для цього віртуального хоста.
- **SSLEngine on**: Увімкнення модуля SSL для цього віртуального хоста.
- **SSLCertificateFile /повний/шлях/до/server-cert.pem**: Вказує повний шлях до файлу сертифіката SSL, який буде використовуватися для шифрування з'єднань.
- **SSLCertificateKeyFile /повний/шлях/до/server-key.pem**: Вказує повний шлях до файлу приватного ключа, який відповідає сертифікату.
- **</VirtualHost>**: Закриває блок конфігурації віртуального хоста.

Цей конфігураційний блок визначає віртуальний хост, який працює через HTTPS на порту 443 і використовує SSL-сертифікат та приватний ключ, які вказані в

SSLCertificateFile та **SSLCertificateKeyFile**. Після внесення змін в конфігурацію, необхідно перезапустити веб-сервер Apache, щоб зміни набули чинності.

sudo service apache2 restart

Дана команда виконує перезапуск веб-сервера Apache. Дозвіл ***sudo*** використовується для надання прав адміністратора, оскільки перезапуск служби зазвичай вимагає привілеї адміністратора.

3. **Вказівка SSL / TLS параметрів:**

Необхідно додати в конфігураційний файл веб-сервера параметри для використання SSL / TLS та вказівки на відповідні сертифікати та ключі.

SSLCertificateFile /path/to/server-cert.pem
SSLCertificateKeyFile /path/to/server-key.pem

Цей код представляє конфігураційні параметри для налаштування *SSL/TLS* у веб-сервері. Він вказує шлях до файлів, які містять сертифікат та приватний ключ для забезпечення шифрування та ідентифікації веб-сайту за допомогою протоколу *HTTPS*.

Крок 3: Налаштування *SSL / TLS* для клієнтів в локальній мережі:

1. **Встановлення та конфігурація веб-браузера:** На кожному клієнтському пристрої необхідно налаштувати веб-браузер для використання *SSL / TLS*.

2. **Вказівка параметрів безпеки:** У налаштуваннях браузера необхідно додати відповідні параметри безпеки, вказавши шлях до кореневого сертифіката.

Крок 4: Тестування з'єднання:

Запустиши веб-браузер на клієнтському пристрої необхідно відкрити веб-браузер та перейти на безпечний протокол *HTTPS* за адресою сервера (наприклад, *https://gucalo.local*).

Далі необхідно перевірити, чи браузер підтверджує безпеку з'єднання та вказує, що використовується SSL / TLS.

Даний приклад демонструє налаштування SSL / TLS для захищеного з'єднання між клієнтами та сервером у локальній обчислювальній мережі з централізованою архітектурою

3.3. Налаштування *IPsec (Internet Protocol Security)* для захисту трафіку на рівні *IP*

Крок 1: Встановлення *IPsec* на центральному сервері:

1. Встановлення *IPsec*-пакетів: необхідно встановити *IPsec*-пакети на центральному сервері (наприклад, використовуючи *StrongSwan*):

sudo apt-get update

sudo apt-get install strongswan

Цей код представляє собою команди для встановлення та оновлення програмного забезпечення на операційній системі, яка використовує систему керування пакетами *APT (Advanced Package Tool)*. У конкретному випадку, ці команди встановлюють і оновлюють програму *StrongSwan*, яка є реалізацією протоколу *IPSec* для створення віртуальних приватних мереж (*VPN*).

Розглянемо деталі кожної команди:

- ***sudo apt-get update***: Ця команда виконує оновлення списку пакетів, який знаходиться на серверах APT. Вона не встановлює нові пакети, а лише оновлює інформацію про доступні пакети.

– ***sudo apt-get install strongswan***: Після оновлення списку пакетів ця команда встановлює програму StrongSwan. Ключове слово ***install*** вказує APT на встановлення зазначеного пакету, у цьому випадку - *StrongSwan*.

2. Конфігурація IPsec: Необхідно налаштувати конфігураційні файли *IPsec* згідно з потребами нашої мережі.

```
config setup
  charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2, 0"

conn %default
  ikelifetime=60m
  keylife=20m
  rekeymargin=3m
  keyingtries=1
  authby=secret
  keyexchange=ikev2

conn myvpn
  left=<central_server_ip>
  leftcert=server-cert.pem
  leftid=@myvpnserver
  right=%any
  auto=start
```

Цей код є конфігураційним файлом для налаштування IPsec VPN (Virtual Private Network) за допомогою StrongSwan, який є реалізацією протоколів IPsec. Опис цього коду можна розділити на 3 блоки:

1. ***config setup:***
   - ***charondebug:*** Визначає рівень деталізації журналу для різних компонентів *StrongSwan*. У цьому випадку включено журналювання для різних

аспектів, таких як ініціалізація (*ike*), ядро (*knl*), конфігурація (*cfg*), мережа (*net*), *ESP*.

2. ***conn %default:***
   - Задається ряд параметрів за замовчуванням для всіх з'єднань.
   - ***ikelifetime***, ***keylife***, ***rekeymargin***: Терміни життя ключа та інші параметри, пов'язані з переосвітою ключа.
   - ***keyingtries***: Кількість спроб встановлення з'єднання перед відмовою.
   - ***authby***: Визначає метод аутентифікації, у цьому випадку "*secret*" (використовується попередній обмін ключами за допомогою спільного пароля).
   - ***keyexchange***: Визначає версію протоколу обміну ключами, у цьому випадку "*ikev2*".
3. ***conn myvpn*:**
   - Задається конфігурація конкретного з'єднання з ім'ям "*myvpn*".
   - ***left***: *IP*-адреса центрального сервера.
   - ***leftcert***: Назва файлу з сертифікатом сервера.
   - ***leftid***: Ідентифікатор сервера.
   - ***right***: ***%any*** дозволяє будь-якому вузлу підключитися до цього *VPN*.
   - ***auto=start***: Запуск з'єднання при завантаженні *StrongSwan*.

Цей конфігураційний файл описує, як *StrongSwan* повинен конфігурувати *IPsec VPN*, встановлювати параметри за замовчуванням та налаштовувати конкретне з'єднання "*myvpn*".

Після внесення змін необхідно перезапустити службу *StrongSwan* за допомогою команди:

sudo systemctl restart strongswan

Крок 2: Налаштування *IPsec* на клієнтських пристроях:

- **Встановлення *IPsec*-пакетів:** необхідно встановити *IPsec*-пакети на клієнтських пристроях (аналогічно, як на центральному сервері).

- **Конфігурація *IPsec*:** необхідно налаштуйте конфігураційні файли *IPsec* на клієнтських пристроях, зазначивши *IP* та сертифікати.

Так як і для центрального серверу, після внесення змін необхідно перезапустити службу *StrongSwan* за допомогою команди:

sudo systemctl restart strongswan

Крок 3: Тестування IPsec-з'єднання:

1. **Перевірка з'єднання:**
   - Для перевірки з’єднання необхідно виконати команду для перевірки статусу *IPsec*-з'єднань на центральному сервері та клієнтських пристроях:

sudo ipsec status

Коли команда буде виконана з правами адміністратора (вказуючи "*sudo*"), вона виведе детальну інформацію про конфігурацію та поточний стан *IPSec* на вашій системі.

3.4. Встановлення Security Information and Event Management (SIEM) системи

Крок 1: Встановлення ELK Stack (Elasticsearch, Logstash, Kibana):

sudo apt-get update
sudo apt-get install default-jre

sudo apt-get install elasticsearch
sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch

sudo apt-get install logstash
sudo systemctl start logstash
sudo systemctl enable logstash

sudo apt-get install kibana
sudo systemctl start kibana

sudo systemctl enable kibana

Цей код встановлює та налаштовує ряд компонентів для створення системи для аналізу та візуалізації журнальних даних, що називається ELK стеком (Elasticsearch, Logstash, Kibana). Далі про кожен етап по порядку:

1. **Встановлення та оновлення *Java:***
   - ***sudo apt-get update**:* Оновлює список доступних пакетів з репозитаріїв.
   - ***sudo apt-get install default-jre**:* Встановлює *Java Runtime Environment (JRE)*.
2. **Встановлення та налаштування *Elasticsearch*:**
   - ***sudo apt-get install elasticsearch**:* Встановлює *Elasticsearch*, розподілену пошукову та аналітичну систему.
   - ***sudo systemctl start elasticsearch**:* Запускає *Elasticsearch*.
   - ***sudo systemctl enable elasticsearch**:* Налаштовує автоматичний запуск *Elasticsearch* при завантаженні системи.
3. **Встановлення та налаштування *Logstash*:**
   - ***sudo apt-get install logstash**:* Встановлює *Logstash*, інструмент для обробки та передачі даних.
   - ***sudo systemctl start logstash**:* Запускає *Logstash*.
   - ***sudo systemctl enable logstash**:* Налаштовує автоматичний запуск Logstash при завантаженні системи.
4. **Встановлення та налаштування *Kibana*:**
   - ***sudo apt-get install kibana**:* Встановлює *Kibana*, веб-інтерфейс для візуалізації даних, які зберігаються в *Elasticsearch*.
   - ***sudo systemctl start kibana**:* Запускає *Kibana*.
   - ***sudo systemctl enable kibana**:* Налаштовує автоматичний запуск *Kibana* при завантаженні системи.

Цей скрипт допомагає швидко встановити та налаштувати основні компоненти *ELK* стеку для обробки та візуалізації журнальних даних

Крок 2: Налаштування *Logstash* для Збору та Фільтрації Журналів:

Далі необхідно створити конфігураційний файл для *Logstash*:

```
sudo nano /etc/logstash/conf.d/01-input.conf
input {
  beats {
    port => 5044
  }
}

filter {
  grok {
    match => { "message" => "%{COMBINEDAPACHELOG}" }
  }
    date {
    match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
    geoip {
    source => "clientip"
  }
    useragent {
    source => "agent"
  }}
  output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
  }
}
```

Для авіаційного сегмента наземного комплексу можна використовувати різні фільтри для обробки лог-подій залежно від конкретних потреб та формату лог-записів.

Ці фільтри використовують грок-патерни для розбору лог-записів, встановлюють дату за допомогою фільтра *date*, а також додають географічні дані і інформацію про агента браузера за допомогою фільтрів *geoip* та *useragent* відповідно.

Крок 3: Налаштування Kibana для Візуалізації та Аналізу Журналів:

У веб-браузері необхідно відкрити Kibana за адресою **http://your_server_ip:5601**, та налаштувати індекс для візуалізації журналів.

Крок 4: Забезпечення Безпеки SIEM Системи:

Захист серверів ELK Stack від Несанкціонованого Доступу:

Такий захист легко відтворити за допомогою встановлення firewalls:

```
# Встановлення та налаштування UFW (Uncomplicated Firewall)
sudo apt-get install ufw
sudo ufw enable
sudo ufw allow ssh
sudo ufw allow 5601  # Для Kibana
sudo ufw allow 9200  # Для Elasticsearch
sudo ufw allow 5044  # Для Logstash
```

Зміна стандартних портів та відключення непотрібних сервісів допоможе ускладнити життя хакерам, для цього треба змінити стандартні порти SSH, Kibana, Elasticsearch та Logstash для ускладнення проведення кібер атак атак.

Обмеження доступу за допомогою конфігурації прав доступу. Для цього можна налаштувати файли конфігурації для обмеження доступу до служб.

Файл конфігурації Nginx для проксі Kibana та обмеження доступу:

```
# /etc/nginx/sites-available/kibana
```

```
server {
    listen 80;
    server_name kibana.example.com;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;

        # Базова автентифікація для обмеження доступу
        auth_basic "Restricted Access";
        auth_basic_user_file /etc/nginx/.htpasswd;
    }
}
```

Необхідно встановити ***nginx*** та налаштувати базову автентифікацію для обмеження доступу. Також необхідно створити файл ***.htpasswd*** з обліковими даними користувачів за допомогою утиліти ***htpasswd***. Для цього треба запустити команду:

sudo htpasswd -c /etc/nginx/.htpasswd your_username

3.5. Налаштування *Intrusion Detection and Prevention Systems (IDPS)* для локальної обчислювальної мережі в авіаційному комплексі

Крок 1: Встановлення та Налаштування *Snort IDPS*

1. Встановлення Snort

sudo apt-get update

Ця команда оновлює інформацію про список пакетів з офіційних репозиторіїв. Вона перевіряє наявність оновлень для всіх пакетів, які ви встановили або можете встановити на вашій систем.

sudo apt-get install snort

Ця команда встановлює пакет з іменем "*snort*" на вашу систему. У цьому випадку, "*snort*" - це програма для виявлення вторгнень (*Intrusion Detection System - IDS*), яка використовується для виявлення атак на комп'ютерні мережі.

2. Налаштування *Snort*:

Створення та редагування конфігураційного файлу *Snort*:

sudo cp /etc/snort/snort.conf /etc/snort/snort.conf.backup - Ця команда створює резервну копію конфігураційного файлу *Snort*. Вона копіює файл ***/etc/snort/snort.conf*** в файл ***/etc/snort/snort.conf.backup***. Це корисно, оскільки ви зберігаєте копію оригінального файлу перед внесенням будь-яких змін.

sudo nano /etc/snort/snort.conf - Ця команда відкриває конфігураційний файл *Snort* у текстовому редакторі *Nano*. Зазвичай, ви можете використовувати цей редактор для внесення змін у конфігураційні файли. Вам слід уважно читати і редагувати параметри відповідно до ваших потреб та налаштувань мережі та безпеки.

Запуск Snort:

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i <your_network_interface>

Крок 2: Налаштування Правил Системи Виявлення та Запобігання Інтрузіям *(IDPS)*

sudo apt-get install snort-rules-default

Ця команда встановлює стандартні правила для Snort. Важливо регулярно оновлювати правила для виявлення нових загроз

Крок 3: Моніторинг та Тестування IDPS

Моніторинг стану IDPS:

sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i <your_network_interface>

Ці кроки дозволять налаштувати конфігураційний файл Snort для ефективного виявлення та запобігання інтрузіям у локальній обчислювальній мережі авіаційного сегменту.

3.6. Налаштування Firewalld для Безпеки Локальної Обчислювальної Мережі Авіаційного Сегменту

Крок 1: Встановлення Firewalld:

sudo apt-get update

sudo apt-get install firewalld

Цей код виконує установку та оновлення програмного забезпечення через систему керування пакетами *APT*.

Крок 2: Запуск та Активація Firewalld:

sudo systemctl start firewalld

Ця команда запускає службу *firewalld*. Якщо служба вже була встановлена, але не запущена, ця команда ініціює запуск служби.

sudo systemctl enable firewalld

Ця команда вмикає автозапуск служби *firewalld* при завантаженні системи. Це означає, що служба буде автоматично запускатися при перезавантаженні або завантаженні системи.

Ці дві команди разом гарантують, що служба firewalld запущена в поточному сеансі та автоматично запускатиметься при кожному перезавантаженні системи

Крок 3: Налаштування Зон та Правил *Firewalld*:

sudo firewall-cmd --set-default-zone=public

Команда ***sudo firewall-cmd --set-default-zone=public*** використовується для зміни за замовчуванням зони захисту файрволу в системі, яка працює під управлінням інструменту firewalld.

Зона захисту файрволу визначає, які мережеві ресурси можуть взаємодіяти з системою та яким чином це може відбуватися. У цьому випадку, команда встановлює зону за замовчуванням для всієї системи на "public". Зона "public" часто використовується для зовнішніх мереж, таких як інтернет, і має більш строгі правила безпеки, оскільки вона вважається менш довіреною.

Додавання правил для SSH, HTTP та HTTPS для публічної зони. Застосування правил залишається постійним:

sudo firewall-cmd --zone=public --add-service=ssh --permanent

sudo firewall-cmd --zone=public --add-service=http --permanent

sudo firewall-cmd --zone=public --add-service=https --permanent

Ці команди корисні для встановлення правил файрвола, які дозволяють проходити трафіку по протоколах *SSH*, *HTTP* і *HTTPS* через вказану зону.

Крок 4: Перезавантаження Firewalld:

Для збереження змін Firewalld необхідно перезавантажити, такою командою:

sudo firewall-cmd --reload

Ці кроки дозволять налаштувати конфігураційний файл Snort для ефективного

виявлення та запобігання інтрузіям у локальній обчислювальній мережі авіаційного сегменту.

3.7. Налаштування 802.1X Authentication в Локальній Обчислювальній Мережі Авіаційного Сегменту

Крок 1: Встановлення RADIUS-сервера (FreeRADIUS):

sudo apt-get update
sudo apt-get install freeradius

1. ***sudo apt-get update:*** Ця команда оновлює інформацію про доступні версії пакунків з інтернет-репозиторіїв. Вона оновлює список доступних пакунків та їх версій, але не встановлює жодних оновлень або пакунків.
2. ***sudo apt-get install freeradius:*** Після оновлення інформації про пакунки, ця команда встановлює програмний пакет з назвою "*freeradius*". У вашому випадку, це, ймовірно, стосується *FreeRADIUS* — сервера *RADIUS* (*Remote Authentication Dial-In User Service)*, який забезпечує аутентифікацію, авторизацію та облік для мережевого доступу.

Тобто цей код встановлює *FreeRADIUS* та всі його залежності в систему.

Крок 2: Налаштування FreeRADIUS:

sudo nano /etc/freeradius/clients.conf

Цей код відкриває текстовий редактор ***nano*** з правами адміністратора (***sudo***), і вказує редагувати файл за шляхом ***/etc/freeradius/clients.conf***.

Щойно ви введете цю команду в командному рядку, вас може попросити ввести пароль або підтвердження для отримання прав адміністратора, оскільки ви використовуєте ***sudo***, що означає "*superuser do*" або "*switch user and do*". Коли введете пароль і підтвердите, ***nano*** відкриється для редагування файлу ***clients.conf*** у текстовому режимі.

Далі йде редагування файлу ***clients.conf*** для додавання інформації про клієнта (наприклад, комутатора або точки доступу):

```
client switch1 {
   ipaddr = 192.168.1.2
   secret = your_secret_key
}
```

Крок 3: Налаштування користувачів для 802.1X:

sudo nano /etc/freeradius/users

Цей код викликає текстовий редактор ***nano*** і відкриває файл ***/etc/freeradius/users*** для редагування, щоб можна було додати користувачів та їхніх паролів для аутентифікації, за допомогою цього коду:

john Cleartext-Password := "user_password"

Крок 4: Налаштування 802.1X у клієнтському пристрої:

Тепер на клієнтському пристрої (це може бути комутатор або точка доступу), необхідно налаштувати 802.1X. Далі буде наведено приклад налаштування на Cisco-комутаторі:

```
enable
configure terminal
interface GigabitEthernet0/1
```

switchport mode access
dot1x port-control auto
dot1x host-mode multi-domain
exit

- ***enable**:* Ця команда вводиться для переходу в режим привілеїв (*privileged exec mode*), який забезпечує повний доступ до всіх команд на пристрої.
- ***configure terminal**:* Ця команда вводиться для переходу в режим конфігурації, де можна змінювати налаштування пристрою.
- ***interface GigabitEthernet0/1**:* Вибір інтерфейсу *GigabitEthernet0/1* для подальших налаштувань.
- ***switchport mode access**:* Ця команда встановлює режим порта в режим "*access*", що означає, що порт призначений для підключення до одного пристрою.
- ***dot1x port-control auto**:* Встановлення управління портом за допомогою протоколу *IEEE 802.1X*. Вказується, що управління портом повинно бути автоматичним.
- ***dot1x host-mode multi-domain**:* Вказує режим хоста для протоколу *802.1X* як "*multi-domain*". Це означає, що порт може служити для різних доменів
- ***exit**:* Вихід з конфігураційного режиму.

Крок 5: Запуск та Перезапуск *FreeRADIUS*:

sudo systemctl start freeradius : Ця команда вмикає службу FreeRADIUS. Вона запускає службу, щоб вона почала виконувати свої функції. Ключеве слово **sudo** дає права адміністратора для виконання цієї команди.

sudo systemctl enable freeradius : Ця команда вмикає автозапуск служби *FreeRADIUS* при завантаженні системи. Це означає, що при кожному старті системи служба *FreeRADIUS* буде автоматично запускатися. Це корисно для того, щоб служба

автоматично розпочинала свою роботу після перезавантаження або включення системи.

Після впровадження всіх наведених протоколів захисту для локальної обчислювальної мережі (ЛОМ) наземного сегменту авіаційного комплексу з централізованою архітектурою, система може очікувати наступні покращення та переваги:

1. **Високий рівень безпеки:** Впровадження VPN, SSL/TLS, IPsec, SIEM, IDPS, Firewalld та 802.1X Authentication створює міцний арсенал заходів для захисту від різноманітних загроз. Система отримує високий рівень захисту від несанкціонованого доступу, атак та витоку конфіденційної інформації.
2. **Контроль доступу та аутентифікація:** 802.1X Authentication відокремлює вповноважених та неавторизованих користувачів, забезпечуючи точний контроль доступу. Це сприяє вдосконаленню системи аутентифікації і управління правами користувачів.
3. **Шифрування даних:** Використання SSL/TLS та IPsec забезпечує шифрування трафіку, що проходить через мережу, що є ключовим фактором для захисту конфіденційної інформації та даних користувачів.
4. **Система виявлення та управління інцидентами:** SIEM та IDPS надають засоби для реагування на потенційні інциденти в реальному часі, що дозволяє вчасно виявляти та запобігати загрозам безпеки.
5. **Комплексний захист від атак:** Firewalld встановлює бар'єри перед несанкціонованим трафіком, що зменшує ризик атак та забезпечує додатковий рівень безпеки.
6. **Спрощене управління та моніторинг:** Використання цих протоколів дозволяє централізовано керувати та моніторити безпеку всієї мережі, що полегшує управління системою та реагування на можливі інциденти.
7. **Забезпечення сталої роботи системи:** Загальне впровадження цих протоколів формує комплексну систему, яка забезпечує стабільну та безпечну роботу

наземного сегменту авіаційного комплексу з централізованою архітектурою навіть у змінних умовах та при ростущих загрозах безпеки.

3.8. Висновки до розділу

У цьому розділі було ретельно розглянуто та впроваджено систему протоколів захисту для локальної обчислювальної мережі (ЛОМ) наземного сегменту авіаційного комплексу з централізованою архітектурою. Процес впровадження включав в себе конфігурацію та налаштування ряду ключових протоколів, спрямованих на покращення безпеки, надійності та ефективності мережі. Нижче наведено основні висновки щодо кожного з впроваджених протоколів:

1. **VPN (Virtual Private Network):** Впровадження VPN надає безпеку та приватність під час передачі даних через мережу. Створені віртуальні тунелі дозволяють зашифровано та безпечно обмінюватися інформацією між різними частинами авіаційного комплексу.
2. **SSL/TLS (Secure Sockets Layer / Transport Layer Security):** Налаштовані SSL/TLS забезпечують шифрування та захист передачі даних від потенційних атак, забезпечуючи конфіденційність та цілісність інформації.
3. **IPsec (Internet Protocol Security):** IPsec впроваджено для захисту трафіку на рівні IP, що гарантує аутентифікацію та шифрування пакетів даних, що передаються в мережі.
4. **SIEM (Security Information and Event Management):** Встановлено SIEM систему для систематичного моніторингу та аналізу подій, що відбуваються в мережі, забезпечуючи швидке виявлення потенційних загроз.
5. **IDPS (Intrusion Detection and Prevention Systems):** Налаштовано IDPS для постійного виявлення та блокування спроб несанкціонованого доступу чи атак на систему.
6. **Firewalld:** Firewalld налаштовано для фільтрації та контролю мережевого трафіку, що забезпечує додатковий рівень захисту мережі від зовнішніх загроз.

7. **802.1X Authentication:** Введено механізми 802.1X Authentication для точного контролю доступу та аутентифікації, що сприяє запобіганню несанкціонованому доступу.

Впровадження цих протоколів формує комплексну систему захисту, яка не лише ефективно вдосконалює безпеку ЛОМ наземного сегменту авіаційного комплексу, а й готує систему до надійного функціонування в умовах постійно зростаючих загроз та вимог до кібербезпеки в авіаційній галузі.

ВИСНОВКИ

Дипломний проект на тему "Захищена ЛОМ наземного сегменту авіаційного комплексу з централізованою архітектурою" є результатом глибокого дослідження та аналізу різних аспектів забезпечення безпеки локальних обчислювальних мереж в авіаційному сегменті. В рамках роботи були ретельно розглянуті теоретичні та практичні аспекти розробки та впровадження захищеного ЛОМ, зосереджуючись на централізованій архітектурі системи.

Теоретичний огляд розробки захищеного ЛОМ виявився ключовим етапом у визначенні основних принципів та стратегій захисту, враховуючи існуючі рішення та методи, такі як системи управління корпоративними ресурсами (ERP), криптовалютні системи, і облачні платформи, такі як Microsoft Azure.

Централізована архітектура системи виявилася найбільш ефективною у забезпеченні безпеки локальних обчислювальних мереж, враховуючи важливість і застосування різних видів архітектур. Аналіз існуючих методів та технологій захисту ЛОМ дозволив визначити потенційні загрози та ризики для наземного сегменту авіаційного комплексу.

Системний аналіз захищеної ЛОМ дозволив розглянути теоретичні аспекти централізованої архітектури та визначити її переваги в контексті безпеки мережі. Проблеми захисту локальних обчислювальних мереж в авіаційних комплексах, вплив зовнішніх факторів та людський фактор були систематично проаналізовані.

Висновки дослідження стосовно налаштування VPN, SSL/TLS, IPsec, SIEM, IDPS, Firewalld, та 802.1X Authentication надають практичний внесок у сферу кібербезпеки авіаційних комплексів. Детальне розглядання основних алгоритмів та конфігурацій для забезпечення безпеки ЛОМ визначає важливий шлях удосконалення сучасних практик.

У цілому, дипломний проект слугує важливим внеском у розвиток та збереження безпеки локальних обчислювальних мереж у наземному сегменті

авіаційного комплексу, сприяючи високому рівню стійкості та ефективності інфраструктури в умовах сучасного кіберпростору.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley.
2. Bellovin, S. M. (2004). *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison-Wesley.
3. Cisco Systems. (2016). *CCNA Security 210-260 Official Cert Guide.* Cisco Press.
4. Dhillon, G., & Torkzadeh, G. (2006). *Value-Focused Supply Management: Getting the Most Out of Your Supply Base.* Wiley.
5. Eckert, J., & Schitka, C. (2015). *CompTIA Security+ Guide to Network Security Fundamentals.* Cengage Learning.
6. Ferguson, P., Schneier, B., & Kohno, T. (2015). *Cryptography Engineering: Design Principles and Practical Applications.* Wiley.
7. Fortinet. (2018). *Next-Generation Firewalls For Dummies.* John Wiley & Sons.
8. Garfinkel, S., & Spafford, G. (2003). *Web Security, Privacy & Commerce.* O'Reilly Media.
9. Green, M., & Hjelmvik, E. (2014). *Network Forensics: Tracking Hackers through Cyberspace.* Prentice Hall.
10. Hacking, A. (2017). *The Basics of Bitcoins and Blockchains.* CRC Press.
11. Hashmi, M., & Agarwal, A. (2012). "Centralized Network Security Management." *International Journal of Computer Applications.* DOI.
12. Johnson, R. D., & Brodsky, I. (2014). *Challenges in Cybersecurity Education.* Springer.
13. Kizza, J. M. (2015). *Computer Network Security and Cyber Ethics.* McFarland.
14. Lindqvist, U., & Jonsson, E. (2002). "Security Engineering for Wireless LANs." *IEEE Communications Magazine.* IEEE Xplore.
15. Microsoft Corporation. (2019). *Securing the Modern Workplace.* Microsoft Press.
16. National Institute of Standards and Technology (NIST). (2017). "Guide to Intrusion Detection and Prevention Systems (IDPS)." *NIST Special Publication 800-94.* NIST.
17. Novak, D. (2013). *Implementing SSL / TLS Using Cryptography and PKI.* Wiley.

18. Osterhage, W., & Koldehofe, B. (2010). "Security Information and Event Management (SIEM) as a Monitoring and Analysis Tool." *IEEE*. IEEE Xplore.
19. Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in Computing*. Pearson Education.
20. Rouse, M. (2019). "What is 802.1X? Definition from WhatIs.com." TechTarget.
21. Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." Norton & Company.
22. Stallings, W. (2017). "Network Security Essentials." Pearson.
23. Tanenbaum, A. S., & Wetherall, D. J. (2011). "Computer Networks." Pearson Education.
24. Tittel, E., & Chapple, M. (2018). "CISSP Cert Guide." Pearson IT Certification.
25. US Department of Defense. (2015). "Risk Management Guide for Information Technology Systems." DIACAP Handbook.
26. VanHoose, D. (2016). "Centralized Network Security: Why and How." SANS Institute.
27. Vormetric. (2014). "Vormetric Data Security Platform."
28. Zhang, W. (2013). "Intrusion Detection and Prevention Systems in the Cloud." IEEE Cloud Computing.
29. Zheng, Y. (2011). "VPN Technologies: Security and Performance." Springer.
30. Zikmund, W. G. (2003). "Business Research Methods." South-Western Cengage Learning.