|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ** | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | |
|  |  | | | |  | | |  | |  | |
| **КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** | | | | | | | | | | | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | |  | | |  | |  | |
| **КВАЛІФІКАЦІЙНА РОБОТА** | | | | | | | | | | | |
| на тему: | | | | | | | | | | | |
| **«Дослідження шляхів та розроблення рекомендацій щодо кібербезпеки критичної інфраструктури»** | | | | | | | | | | | |
| зі спеціальності | | *125 Кібербезпека* | | | | | | |  | | |
| *(код, найменування спеціальності)* | | | | | | | | | | | |
| освітньо-професійної програми | | | | *Інформаційна та кібернетична безпека* | | | | | | |  |
| *(назва програми)* | | | | | | | | | | | |
| *Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*  \_\_\_\_\_\_\_\_\_\_\_\_ Андрій КОВТУН  *(підпис)* | | | | | | | | | | | |
|  |  | | | |  | | |  | |  | |
|  |  | | Виконав: здобувач вищої освіти групи БСД-43 | | | | | | | | |
|  |  | | | | КОВТУН Андрій | | | | | | |
|  |  | | | | *(прізвище, ім’я)* | | | | | | |
|  |  | | Керівник | | | *к.т.н., доцент* БОРСУКОВСЬКИЙ Юрій | | | | | |
|  |  | | *(науковий ступінь, вчене звання, прізвище, ім’я)* | | | | | | | | |
|  |  | | Рецензент | | | |  | | | | |
|  |  | | *(науковий ступінь, вчене звання, прізвище, ім’я)* | | | | | | | | |
|  |  | |
|  |  | |
|  |  | | | |  | | |  | |  | |
|  |  | | | | Київ 2024 | | |  | |  | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**  **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | | | |
| Кафедра | | Інформаційної та кібернетичної безпеки | | | | | | | | | | | | | | | | |
| Ступінь вищої освіти | | | | Бакалавр | | | | | | | |  | | | |  | | |
| Спеціальність | | | 125 Кібербезпека | | | | | | | | |  | | | |  | | |
| Освітньо-професійна програма | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
|  | |  | | | | |  | | | | | ЗАТВЕРДЖУЮ | | | | | | |
|  | |  | | | | |  | | | | | Завідувач кафедри ІКБ | | | | | | |
|  | |  | | | | |  | | | | |  | | | | Галина ГАЙДУР | | |
|  | |  | | | | |  | | | | | “\_\_\_” 2024 року | | | | | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | | | | |  | | |
|  | | **НА КВАЛІФІКАЦІЙНУ РОБОТУ** | | | | | | | | | | | | | |  | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
| Ковтуну Андрію Валерійовичу | | | | | | | | | | | | | | | | | | |
| *(прізвище, ім’я)* | | | | | | | | | | | | | | | | | | |
| 1. Тема кваліфікаційної роботи: | | | | | | | | «Дослідження шляхів та розроблення | | | | | | | | | | |
| рекомендацій щодо кібербезпеки критичної інфраструктури» | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |
| керівник кваліфікаційної роботи | | | | | | | | | к.т.н., доцент Борсуковський Ю.В. | | | | | | | | | |
|  | |  | | | | | *(прізвище, ім’я, науковий ступінь, вчене звання)* | | | | | | | | | | | |
| затверджені наказом Державного університету інформаційно-комунікаційних  технологій від « » \_\_\_\_\_\_\_\_\_ 2024 року № \_\_\_\_. | | | | | | | | | | | | | | | | | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
| 2. Строк подання здобувачем вищої освіти кваліфікаційної роботи | | | | | | | | | | | | | | | | | 31.06.2024 р. | |
|  | |  | | | | |  | | | | |  | | | |  | | |
| 3. Вихідні дані до кваліфікаційної роботи | | | | | | | | | |  | | | | | |  | | |
| інформаційні ресурси критичної інфраструктури; | | | | | | | | | | | | | | | |  | | |
| рішення для підвищення рівня кібербезпеки; | | | | | | | | | | | | | | | | | | |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | | | | | | | | | |
| документи, міжнародні стандарти. | | | | | | | | | | | | | | | | | | |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | | | | | | |
| 1. Дослідження проблеми захисту критичної інфраструктури. | | | | | | | | | | | | | | | | | | |
| 2. Аналіз методів та засобів кібернетичного захисту критичної інфраструктури. | | | | | | | | | | | | | | | | | | |
| 3. Розроблення рекомендацій щодо кібернетичного захисту критичної | | | | | | | | | | | | | | | | | | |
| інфраструктури | | | | | | | | | | | |  | | | |  | | |
| 5. Перелік графічного матеріалу | | | | | | | | | | | |  | | | |  | | |
| Презентація PowerPoint. | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |
| 6. Дата видачі завдання | | | | | 15.04.2024 р. | | | | | | | | | | | | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | | | | | | | | | | |  | | |
|  | |  | | | | |  | | | | |  | | | |  | | |
| №  зп | Назва етапів  кваліфікаційної роботи | | | | | | | | | | | | Строк виконання етапів роботи | | | | | Примітка |
| 1. | Визначення актуальності проблеми кібербезпеки критичної інфраструктури. | | | | | | | | | | | | 15.04.2024 р. | | | | |  |
| 2. | Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи. | | | | | | | | | | | |  | | | | |  |
| 3. | Аналіз методів та засобів кібернетичного захисту критичної інфраструктури. | | | | | | | | | | | |  | | | | |  |
| 4. | Практична реалізація засобів кібернетичного захисту критичної інфраструктури. | | | | | | | | | | | |  | | | | |  |
| 5. | Розроблення рекомендацій щодо застосування методів та засобів кібернетичного захисту критичної інфраструктури. | | | | | | | | | | | |  | | | | |  |
| 6. | Оформлення результатів дослідження. | | | | | | | | | | | |  | | | | |  |
| 7. | Підготовка доповіді до захисту. | | | | | | | | | | | | 31.05.2024 р. | | | | |  |
|  | | | | | | | | | | | | |  | | | | |  |
| Здобувач вищої освіти | | | | | |  | | | | | | |  | Андрій КОВТУН | | | | | |
|  | | | | | | *(підпис)* | | | | | | |  | *(ім’я, прізвище)* | | | | | |
|  | |  | | | | |  | | | |  | | | | |  | | |
| Керівник кваліфікаційної роботи | | | | | | | | |  | | | |  | Юрій БОРСУКОВСЬКИЙ | | | | | | |
|  | | | | | | | *(підпис)* | | | | | | | | *(ім’я, прізвище)* | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | | | | | | | | | | |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ** | | | | | | | | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**  **ПОДАННЯ**  **ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**  **на здобуття освітнього ступеня бакалавра** | | | | | | | | | | | | | | | | | | | | |
| Направляється здобувач | | | | Ковтун А.В. | | | | | до захисту кваліфікаційної роботи | | | | | | | | | | | |
|  | | | | (прізвище та ініціали) | | | | |  | | | | | | | | | | | |
| За спеціальністю 125 Кібербезпека | | | | | | |  | | | |  | | | | |
| освітньо-професійної програми | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | | | | | |
|  | | |  | | | | (шифр і назва спеціальності) | | | | | | | | | | | | | |
| на тему: | «Дослідження шляхів та розроблення рекомендацій щодо кібербезпеки критичної інфраструктури». | | | | | | | | | | | | | | | | | |
| Кваліфікаційна робота і рецензія додаються. | | | | | | | | | | |  | | | | |
| Директор інституту \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Віталій САВЧЕНКО | | | | | | | | | | | | | | | | | | | | |
| (*підпис*) (*Ім’я, ПРІЗВИЩЕ*) | | | | | | | | | | | | | | | | | | | | |
|  | | | **Висновок керівника кваліфікаційної роботи** | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |  | | | | |
| Здобувач ***КОВТУН Андрій*** обрав тему роботи, метою якої було розробити варіант технології кібернетичної безпеки критичної інфраструктури підприємства. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КОВТУН Андрій*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОВТУНА Андрія*** на оцінку **«добре»** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека. | | | | | | | | | | | | | | | | | | | | |
| Керівник кваліфікаційної роботи | | | | | | | | | |  | | | |  | Юрій БОРСУКОВСЬКИЙ | | | | |
|  | |  | | | | *(підпис) (Ім’я, ПРІЗВИЩЕ)* | | | | | | | | | | | | | | |
|  | |  | | | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2024 року | | | | | | | | | | | | | | |
|  | |  | | | |  | | | | | | | | | | | | | | |
| **Висновок кафедри про кваліфікаційну роботу** | | | | | | | | | | | | | | | | | |
| Кваліфікаційна робота розглянута. Здобувач Ковтун А.В. допускається до захисту даної роботи в Екзаменаційній комісії. | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | |
| Завідувач кафедри Інформаційної та кібернетичної безпеки | | | | | | | | | | | |  | | |  | | | | |
| (назва) | | | | | | | | | | | | | | | | | | | |
|  | | |  | | | | | Галина ГАЙДУР | | | |
| *(підпис)* | | | *(Ім’я, ПРІЗВИЩЕ)* | | | | | | | | |

**ВІДГУК РЕЦЕНЗЕНТА**

на кваліфікаційну роботу

здобувача Ковтун Андрій

на тему: «Дослідження шляхів та розроблення рекомендацій щодо кібербезпеки критичної інфраструктури».

**Актуальність:**

Метою кожного підприємства є контроль доступу користувачів до корпоративної мережі, отримання доступу до мережі підприємства, може призвести до руйнації активів, репутації організації. Тому підприємство зосереджує свою увагу на впровадження технологій контролю доступу користувачів до корпоративної мережі. Одним з таких рішень є налаштування міжмережевого екрану Cisco ASA, яке є комплексом технологій управління доступом, моніторингу та аналітики подій, що дозволяє захистити мережу від несанкціонованих дій зловмисників. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

**Позитивні сторони:**

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми встановлення кібербезпеки критичної інфраструктури підприємства.
2. Досліджено методи та засоби управління мережевим доступом підприємства.
3. Запропоновано варіант технології забезпечення захищеного функціонування ІС підприємства на базі міжмережевого екрану компанії Cisco.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

**Недоліки:**

1. У кваліфікаційній роботі доцільно було приділити більше уваги інформації про захищені мережи, які використовуються на підприємствах на даний час.
2. Доцільно було б продемонструвати більше видів протоколів захисту та ефективність запропонованих протоколів на практиці.

**Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Рецензент: |  |  |  |
|  | *підпис* |  | *Ім’я, ПРІЗВИЩЕ* |

**РЕФЕРАТ**

Текстова частина кваліфікаційної роботи: 58 сторінок, 15 рисунків, 2 таблиці 23 джерела.

*Об’єкт дослідження* – критична інфраструктура, яка включає технологічні системи та мережі, що забезпечують функціонування життєво важливих секторів економіки.

*Предмет дослідження* – методи та засоби кібербезпеки, які можуть бути застосовані для захисту критичної інфраструктури.

*Мета роботи* розроблення рекомендацій щодо застосування методів та засобів кібернетичного захисту критичної інфраструктури.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Критична інфраструктура є актуальною та важливою проблемою в сучасному світі, оскільки її безперебійне функціонування забезпечує життєдіяльність суспільства, економічну стабільність і національну безпеку.

В роботі досліджено проблему захисту критичної інфраструктури. Визначено основні типи загроз і вразливостей, які впливають на кібербезпеку критичної інфраструктури. Проаналізовано методи та засоби кібернетичного захисту критичної інфраструктури. Запропоновано рекомендації щодо застосування методів та засобів кібернетичного захисту.

Результати аналізу дозволяють визначити основні загрози і вразливості, проаналізувати методи та засоби кібернетичного захисту, і запропонувати рекомендації для підвищення рівня безпеки критичної інфраструктури.

Галузь використання – кібербезпека інформаційних ресурсів організації.

КІБЕРБЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, ЗАХИСТ ІНФОРМАЦІЇ, МОНІТОРИНГ БЕЗПЕКИ, АТАКИ НА ІНФРАСТРУКТУРУ

**ЗМІСТ**

[**ВСТУП** 8](#_Toc167498339)

[**1 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА** 10](#_Toc167498340)

[1.1 Загрози кібербезпеки критичної інфраструктури підприємства 10](#_Toc167498341)

[1.2 Оцінка потенційних втрат та наслідків 17](#_Toc167498342)

[1.3 Сучасні загрози та підходи до захисту інформаційних систем 18](#_Toc167498343)

[Висновок до розділу 1 24](#_Toc167498344)

[**2 ОГЛЯД МЕТОДІВ ТА ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ** 25](#_Toc167498345)

[2.1 Технології кібернетичного захисту інформаційної системи 25](#_Toc167498346)

[2.2 Технічні засоби захисту інформаційної системи 25](#_Toc167498347)

[2.3 Заходи з фізичного захисту систем 26](#_Toc167498348)

[2.4 Управління доступом, ідентифікація та аудит 27](#_Toc167498349)

[Висновок до розділу 2 29](#_Toc167498350)

[**3 ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА** 30](#_Toc167498351)

[3.1 Огляд існуючої інформаційної системи підприємства 30](#_Toc167498352)

[3.2 Створення та впровадження стратегій посилення кібербезпеки 33](#_Toc167498353)

[3.3 Оцінка ефективності застосування захисних можливостей Cisco ASA 5506-X 37](#_Toc167498354)

[3.4 Пропозиції щодо використання захисної технології для критичної інфраструктури на прикладі Cisco ASA 5506-X 38](#_Toc167498355)

[Висновки до розділу 3 49](#_Toc167498356)

[**ВИСНОВКИ** 50](#_Toc167498357)

[**ПЕРЕЛІК ПОСИЛАНЬ** 51](#_Toc167498358)

[**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ** 54](#_Toc167498359)

# **ВСТУП**

*Актуальність дослідження* обумовлена зростаючою залежністю сучасних суспільств від технологічних систем, які управляють життєво важливими секторами економіки, включаючи енергетику, транспорт, фінанси, охорону здоров'я та комунікації. Порушення роботи цих систем через кібератаки може призвести до значних економічних збитків, збоїв у функціонуванні суспільства та навіть до загроз національній безпеці. Сучасні загрози стають дедалі складнішими та витонченішими, що вимагає постійного вдосконалення методів захисту та швидкої адаптації до нових типів атак.

Крім того, з огляду на глобальну інтеграцію та взаємозалежність критичних інфраструктур, питання кібербезпеки набувають міжнародного значення, потребуючи координації зусиль на державному та міждержавному рівнях. Дослідження в цій сфері допоможе не лише розробити ефективні стратегії захисту, а й підвищити загальну стійкість систем до кібератак, зменшуючи ризики та потенційні наслідки для суспільства. Розроблені рекомендації сприятимуть створенню більш безпечних і надійних інформаційних систем, що забезпечують функціонування критичних інфраструктур, тим самим підтримуючи стабільність та безпеку національної економіки та держави в цілому.

*Об’єкт дослідження* – критична інфраструктура, яка включає технологічні системи та мережі, що забезпечують функціонування життєво важливих секторів економіки.

*Предмет дослідження* – методи та засоби кібербезпеки, які можуть бути застосовані для захисту критичної інфраструктури.

*Мета роботи* розроблення рекомендацій щодо застосування методів та засобів кібернетичного захисту критичної інфраструктури.

*Наукові завдання:*

дослідити сутність проблеми захисту критичної інфраструктури;

визначити та класифікувати основні типи загроз і вразливостей, які впливають на кібербезпеку критичної інфраструктури, з акцентом на сучасні тенденції в кібератаках.

проаналізувати методи та засоби кібернетичного захисту критичної інфраструктури;

розробити рекомендації щодо застосування методів та засобів кібернетичного захисту критичної інфраструктури.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

# **1 АНАЛІЗ ЗАГРОЗ ТА РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА**

# 1.1 Загрози кібербезпеки критичної інфраструктури підприємства

Критична інфраструктура – це сукупність систем, мереж, об'єктів та послуг, які є настільки важливими для суспільства, економіки та держави, що їхнє порушення або знищення матиме серйозні наслідки для національної безпеки, економічного добробуту, здоров'я та безпеки громадян.

Типи кіберзагроз (рис.1.1), які можуть вплинути на критичну інфраструктуру:

Шкідливе програмне забезпечення, а саме віруси, трояни, програми-шантажисти.

Атаки на мережу - DDoS-атаки, перехоплення даних, атаки "людина посередині" (MITM).

Соціальна інженерія - фішинг, обман, використання соціальних мереж для отримання доступу до систем.

І це тільки найбільш поширені типи кіберзагроз на критичну інфраструктуру.

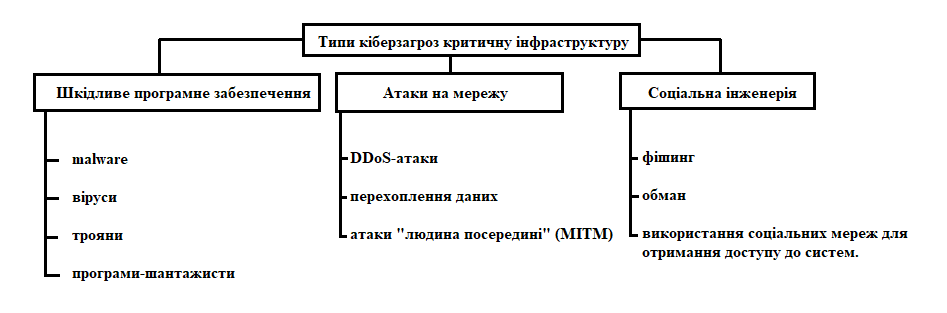


Рис. 1.1 Найпоширеніші типи кіберзагроз

Шкідливе програмне забезпечення, або малваре (від англ. "malware" - malicious software), – це загальний термін, що позначає різні види шкідливих програм, створених для проникнення в комп'ютерні системи, завдання їм шкоди або отримання несанкціонованого доступу до даних. Шкідливе програмне забезпечення може виконувати різні дії, такі як крадіжка інформації, пошкодження даних, знищення файлів або блокування доступу до системи. На рисунку 1.2 зображено частину того що бачить користувач (жертва) під час враження malware.

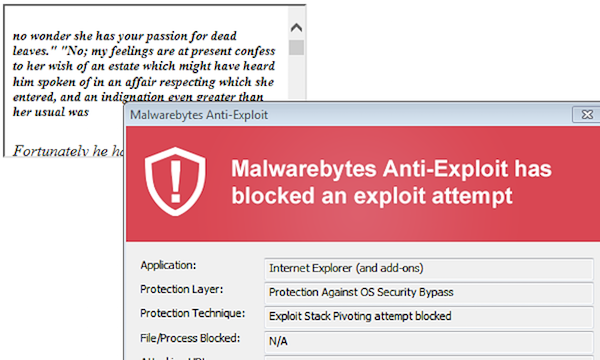


Рис. 1.2 Шкідливе програмне забезпечення

Основні види шкідливого програмного забезпечення включають:

Віруси – це шкідливі програми, які прикріплюються до інших програм або файлів, виконуються разом із ними та поширюються на інші комп'ютери. Віруси можуть пошкоджувати або видаляти файли, уповільнювати роботу системи або викликати інші збої. Вони часто активуються під час запуску заражених програм або файлів.

Трояни – це шкідливі програми, які маскуються під легітимні або корисні програми, але насправді виконують шкідливі дії. Вони можуть надавати зловмисникам віддалений доступ до комп'ютера, красти конфіденційну інформацію або встановлювати інші шкідливі програми. Трояни не можуть самостійно поширюватися, як віруси чи черв'яки.

Черв'яки – це саморозповсюджувані шкідливі програми, які використовують мережеві з'єднання для поширення своїх копій на інші комп'ютери. Вони не потребують взаємодії з користувачем для розповсюдження і можуть швидко інфікувати велику кількість систем. Черв'яки часто спричиняють перевантаження мережі, сповільнюючи її роботу.

Ransomware – це шкідливі програми, які шифрують файли на комп'ютері жертви, роблячи їх недоступними. Зловмисники вимагають викуп за відновлення доступу до зашифрованих файлів. Випадки Ransomware можуть бути особливо руйнівними для підприємств і організацій, спричиняючи значні фінансові втрати.

Spyware – це шкідливі програми, які збирають інформацію про користувача або систему без його відома і передають її третім особам. Spyware може відслідковувати натискання клавіш, збирати паролі, записувати історію браузера або викрадати особисті дані. Воно часто встановлюється разом з іншими програмами без відома користувача.

Adware – це програми, які показують небажану рекламу або перенаправляють браузер на рекламні сайти. Хоча Adware не завжди є шкідливим, воно може уповільнювати роботу системи, викликати нав'язливу рекламу і спричиняти небажані перенаправлення. Деякі види Adware також можуть збирати інформацію про користувача для цільової реклами.

Rootkits – це програми, які приховують своє існування або існування інших шкідливих програм на комп'ютері, забезпечуючи зловмисникам віддалений доступ до системи. Rootkits можуть модифікувати операційну систему для приховування слідів своєї діяльності та забезпечення стійкості шкідливого ПЗ. Вони часто використовуються для збереження контролю над зараженою системою.

Backdoors – це програми, які створюють приховані шляхи для доступу до комп'ютера, дозволяючи зловмисникам контролювати систему без відома користувача. Бекдори можуть бути встановлені зловмисниками або вбудовані розробниками в легітимні програми для технічного обслуговування. Використання бекдорів може призвести до несанкціонованого доступу до конфіденційної інформації та системних ресурсів.

Шкідливе програмне забезпечення є серйозною загрозою для безпеки інформаційних систем і потребує застосування ефективних заходів захисту, таких як антивірусні програми, фаєрволи, регулярні оновлення програмного забезпечення та навчання користувачів основам кібербезпеки.

Атака на мережу - це спроба отримати несанкціонований доступ до комп'ютерної мережі або здійснити ряд дій, спрямованих на завдання шкоди системі, даним чи іншим компонентам мережі.

Рисунок 1.3 показує загальний процес атаки на мережу, починаючи з вибору цілі атаки і пошуку вразливостей в системі. Після використання вразливостей зловмисники можуть отримати доступ до системи та виконати атаку. Після цього вони можуть намагатися приховати свої сліди, щоб уникнути виявлення.

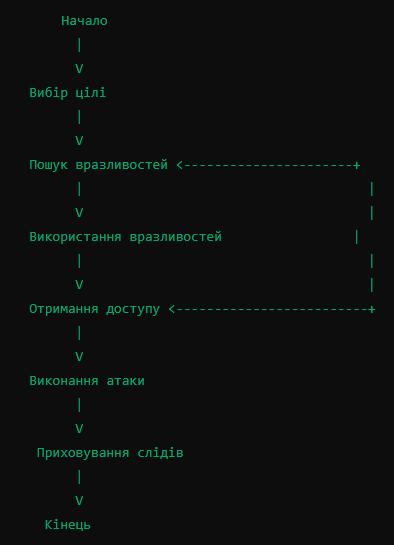


Рис. 1.3 Загальний процес атаки на мережу

Найпоширеніші види атак:

1. Перехоплення даних (Sniffing), цей вид атаки використовується для перехоплення чутливої інформації, що передається по мережі, такої як паролі, інформація про банківські рахунки або конфіденційні дані. Зловмисники можуть використовувати програми-сніфери для перехоплення пакетів даних і зчитування їх вмісту.

2. Перехоплення сеансів (Session Hijacking), цей вид атаки використовується для отримання контролю над активним сеансом зв'язку між двома комп'ютерами. Зловмисники можуть використовувати цей метод для відправлення фальшивих команд або отримання конфіденційної інформації.

3. DDoS-атаки (Distributed Denial of Service), цей вид атаки використовується для перевантаження мережевих ресурсів шляхом надсилання великої кількості запитів на обробку до цільового сервера. Це може призвести до тимчасової недоступності сервера для легітимних користувачів.

4. Мережеві вразливості (Exploiting Network Vulnerabilities), цей вид атаки використовується для зловживання вразливостей у мережевих протоколах або програмах для отримання несанкціонованого доступу до системи або даних.

5. Фішинг (Phishing), цей вид атаки використовується для отримання конфіденційної інформації, такої як паролі або банківські дані, шляхом введення користувачів у оману. Зловмисники відправляють лукаві електронні листи або створюють фальшиві веб-сайти, щоб переконати користувачів надати свої дані.

6. Атаки "людина посередині" (Man-in-the-Middle), цей вид атаки використовується для перехоплення та модифікації комунікації між двома сторонами, яка здійснюється через взаємодію зловмисника, який знаходиться між ними.

7. Сканування портів (Port Scanning), цей вид атаки використовується для виявлення відкритих мережевих портів на цільовій системі, що може допомогти зловмисникам знайти вразливості в системі для подальших атак.

Для захисту від атак на мережу важливо використовувати надійне програмне та апаратне забезпечення, встановлювати оновлення безпеки, використовувати сильні паролі та двофакторну аутентифікацію, а також надавати навчання користувачам з питань кібербезпеки.

Соціальна інженерія - це метод атаки, який використовує маніпулювання людьми з метою отримання конфіденційної інформації або здійснення несанкціонованих дій. Вона базується на експлуатації психологічних вразливостей людей, а не на використанні технічних аспектів атаки. На рисунку 1.3 представлений приклад соціальної інженерії «типова схема вимагання». З користувачем (жертвою) ввічливо спілкуються та пропонують перейти за посиланням для отримання коштів, ну як за посиланням – перейти на фішинговий сайт, який дещо трохи відрізняється наповнення від офіційного, але домен сайту інший, з мінімальною зміною. Тому потрібно завжди звертати увагу на посилання та користуватися офіційними додатками.

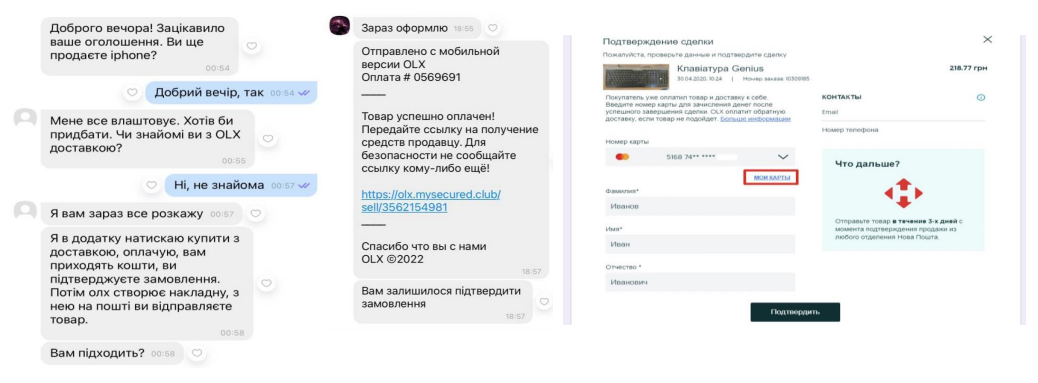


Рис. 1.3 Приклад використання соціальної інженерії

Зазвичай соціальна інженерія включає в себе використання хитромудрих та переконливих сценаріїв для отримання інформації або доступу до системи. Наприклад, зловмисники можуть виглядати як співробітники компанії або службовці підтримки, щоб отримати паролі, ідентифікатори або іншу конфіденційну інформацію від недбалих користувачів. Вони також можуть використовувати соціальні мережі для створення довірливих стосунків з потенційними жертвами та отримання інформації через маніпулювання їхніми друзями або колегами.

Фішинг (Phishing), це вид атаки, який використовує лукаві електронні листи, текстові повідомлення або веб-сайти, щоб виглядати як легітимні, з метою викликати користувача надати конфіденційну інформацію, таку як паролі або банківські реквізити. Наприклад, атакувач може відправити електронний лист, який виглядає як повідомлення від банку, у якому проситься оновити свої дані за посиланням, яке насправді веде на фальшивий сайт, призначений для крадіжки інформації.

Обман (Impersonation), цей вид атаки включає в себе видачу себе за іншу особу або організацію з метою отримання конфіденційної інформації або виконання шахрайських дій. Наприклад, атакувач може виглядати як співробітник підтримки компанії та зателефонувати до користувача, щоб отримати його пароль або іншу конфіденційну інформацію.

Використання соціальних мереж для отримання доступу до систем, цей метод включає в себе створення довірливих стосунків з потенційними жертвами через соціальні мережі. Зловмисники можуть створювати облікові записи, що виглядають довірливо, та взаємодіяти з друзями або колегами жертви, щоб отримати доступ до конфіденційної інформації.

Клікбейт (Clickbait), цей метод використовується для залучення уваги користувачів шляхом створення заголовків або описів, які обіцяють цікавий або шокуючий контент. Після того як користувачі переходять за посиланням, вони можуть бути перенаправлені на шкідливі веб-сайти або викликати виконання шкідливого коду на їхніх пристроях.

Соціальний інженеринг в офлайні (Offline Social Engineering), цей метод включає в себе використання маніпуляційних технік в офлайн-середовищі для отримання доступу до конфіденційної інформації. Наприклад, атакувач може проникнути в будівлю підприємства, вигадати, що він є підтримкою та отримати доступ до захищених областей.

# 1.2 Оцінка потенційних втрат та наслідків

Наслідки атаки - це результати та вплив атаки на цільову систему, мережу або організацію. Це можуть бути шкоди, втрати, порушення безпеки або інші негативні наслідки, що виникають внаслідок дій зловмисника. Наслідки атаки можуть включати:

1. Втрата конфіденційності: Несанкціонований доступ до конфіденційної інформації може мати серйозні наслідки для організації. Наприклад, у випадку втрати конфіденційних даних клієнтів, які містять особисту інформацію, таку як імена, адреси або фінансові дані, це може призвести до порушення законодавства про захист персональних даних та покладання штрафів на організацію.

2. Втрата цілісності даних: Зміна або видалення даних може призвести до втрати надійності та точності інформації, що може спричинити помилки у прийнятті рішень та негативно позначитися на роботі організації.

3. Втрата доступності: Недоступність системи або даних може призвести до припинення роботи організації, втрати продуктивності та негативно вплинути на задоволення клієнтів.

4. Фінансові втрати: Шкода, крадіжка або втрата фінансових ресурсів може викликати серйозні проблеми для організації, зокрема, ускладнення її фінансового стану та можливість припинення діяльності.

5. Порушення репутації: Виявлення недостатньої безпеки може призвести до втрати довіри клієнтів та партнерів, що може вплинути на репутацію організації та її можливості залучення нових клієнтів.

6. Правові наслідки: Порушення законодавства про захист даних або кібербезпеку може призвести до штрафів та судових позовів, що може серйозно підірвати фінансову стійкість організації.

7. Припинення діяльності: Недоступність критичних систем або процесів може призвести до припинення або обмеження діяльності організації, що може спричинити втрату прибутку та ризики для подальшого функціонування.

8. Втрата даних: Втрата конфіденційних або важливих даних може призвести до втрати важливої інформації для бізнесу та може важко відновлюватися.

9. Вплив на інфраструктуру: Пошкодження або недоступність фізичної інфраструктури може призвести до припинення роботи організації та потребувати серйозних витрат на відновлення.

Запобігання наслідків атаки передбачає забезпечення цілісності, доступності і конфіденційності інформації. Основні положення в цьому контексті включають:

1. Цілісність (Integrity) - гарантування, що дані не піддаються незаконному чи несанкціонованому зміненню, втраті або пошкодженню. Це може бути досягнуто за допомогою методів шифрування даних, контролю доступу та механізмів перевірки цілісності.

2. Доступність (Availability) - забезпечення того, щоб системи та дані були доступні відповідним користувачам у відповідний час. Це може включати резервне копіювання даних, використання високодоступних систем та мереж, а також заходи забезпечення безперебійної роботи систем.

3. Конфіденційність (Confidentiality) - захист інформації від несанкціонованого доступу. Це може включати шифрування даних, використання механізмів аутентифікації та авторизації, а також забезпечення безпеки мережі для запобігання проникненню зловмисників.

# 1.3 Сучасні загрози та підходи до захисту інформаційних систем

Фішинг є одним з найпоширеніших видів кіберзлочинів у Сполучених Штатах, призводячи щорічно до значних фінансових втрат. Основна мета цього виду атак полягає в отриманні конфіденційних даних та облікових записів, таких як паролі або дані кредитних карток, шляхом обману людей. Зловмисники можуть використовувати різноманітні методи, щоб обійти системи безпеки та отримати доступ до корпоративних даних незамітно.

Смішинг використовує той же принцип, що й фішинг, але замість електронної пошти зловмисники надсилають спеціально створені текстові повідомлення. Вони можуть виглядати як повідомлення від довіреної особи чи компанії та спрямовуються на мобільні пристрої. Одержавши доступ до такого пристрою, зловмисники можуть викрасти конфіденційну інформацію. Коли ці пристрої підключаються до корпоративної мережі, вони можуть отримати доступ до даних клієнтів та співробітників, а також до внутрішнього коду організації.

Існує низка заходів, які організація може вжити для захисту від фішингу. По-перше, важливо проводити регулярні тренування для співробітників з метою вдосконалення їхніх навичок у розпізнаванні підозрілих повідомлень. Також слід заохочувати працівників повідомляти про будь-яку підозрілу діяльність. Додатково, важливо мати ефективні системи виявлення вторгнень і спам-фільтри, які допоможуть вчасно виявляти та блокувати шкідливі повідомлення. Не менш важливим є використання надійних засобів автентифікації, таких як багатофакторна аутентифікація та регулярно змінювані паролі, щоб ускладнити життя потенційним зловмисникам.

Кожна компанія має свої особливості та слабкі місця, тому важливо вживати індивідуальний підхід до захисту від фішингу. З цією метою багато компаній звертаються до професіоналів у галузі кібербезпеки для проведення аудиту та розробки індивідуальних стратегій захисту.

Щодо зловмисного програмного забезпечення, це є серйозною загрозою для будь-якої організації. Зловмисники розробляють різноманітні види зловмисного програмного забезпечення з метою отримання доступу до корпоративних пристроїв і викрадення даних. Одним з найбільш поширених методів їх поширення є використання фішингових електронних листів. Тому, важливо мати ефективні заходи захисту від цих загроз, такі як регулярне оновлення програмного забезпечення та використання надійних антивірусних програм.

Інфекції комп'ютерів шкідливим програмним забезпеченням є досить поширеним явищем, яке може серйозно зашкодити вашій мережі. Вони можуть спричинити крадіжку даних та паролів, уповільнення роботи системи та повне видалення файлів. Крім того, обладнання, що постраждало від вірусів, часто стає непридатним для використання, що може призвести до витрат на його заміну, що особливо негативно впливає на малі та середні підприємства.

Зловмисне програмне забезпечення може поширюватися дуже швидко по мережі організації і призвести до компрометації всієї структури. Тому важливо вживати комплексних заходів безпеки для запобігання цим загрозам. Оцінка ризиків кібербезпеки є одним з ефективних заходів, які можуть допомогти забезпечити безпеку вашої компанії.

Маючи на увазі всі ці ризики, важливо вживати заходів безпеки, таких як використання надійного програмного забезпечення для захисту від вірусів і шкідливого ПЗ, регулярне оновлення системи та мережі, а також проведення навчання з безпеки для співробітників. Тільки комплексний підхід може ефективно захистити вашу компанію від цих загроз.

Шкідливе програмне забезпечення може стати серйозною загрозою для будь-якої компанії, особливо для малих та середніх підприємств. Його наслідки можуть бути катастрофічними, включаючи крадіжку даних і паролів, уповільнення роботи системи та повне видалення файлів. Крім того, обладнання, що постраждало від вірусів, може виявитися непридатним для використання, що призводить до додаткових витрат на його заміну.

Оскільки шкідливе програмне забезпечення може швидко поширюватися по мережі організації і скомпрометувати всю структуру, важливо вживати комплексних заходів безпеки. Одним з таких заходів є оцінка ризиків кібербезпеки, яка допоможе ідентифікувати потенційні загрози та визначити шляхи їх запобігання.

Для захисту від шкідливого програмного забезпечення необхідно використовувати надійне програмне забезпечення для захисту від вірусів та регулярно оновлювати системи. Також важливо навчати співробітників правилам безпеки та вчасно реагувати на будь-які підозрілі дії в мережі. Тільки комплексний підхід може забезпечити ефективний захист від цих загроз.

Програми-вимагачі, це форма шкідливого програмного забезпечення, можуть великою мірою нашкодити бізнесу. Після того, як вони проникають у вашу систему, вони блокують доступ до критично важливих даних і вимагають викуп за їхнє відновлення. Це ставить компанії перед складним вибором між сплатою викупу та втратою даних і доступу. Багато компаній змушені сплачувати викуп, але навіть після цього можуть не отримати повернення до своїх даних.

З розвитком програм-вимагачів, методи атак хакерів стали складнішими, і навіть малі підприємства стали предметом їхніх атак. Хакери звертають увагу на те, що малі компанії не завжди мають належні засоби для резервного копіювання даних і можуть бути схильні заплатити викуп для збереження бізнесу в робочому стані.

Щоб запобігти програмам-вимагачам, важливо вжити профілактичних заходів, таких як використання сучасних систем безпеки і систем резервного копіювання. Також важливо проводити аудит безпеки, щоб виявити потенційні загрози і вжити заходів для їх усунення. Навчання співробітників про безпеку даних і розпізнавання шкідливих програм також може допомогти у попередженні атак програм-вимагачів.

Послуги віртуальних приватних мереж (VPN): VPN є важливим інструментом для забезпечення безпеки під час підключення до загальнодоступних мереж Wi-Fi, оскільки вони допомагають захистити ваші дані від загроз.

Плани реагування на інциденти: заздалегідь плануйте вашу стратегію реагування на інциденти, щоб забезпечити безперервну роботу у випадку атаки. Аналізуйте вашу реакцію на інциденти, виявляйте слабкі місця і робіть корективи для підготовки до можливих атак програм-вимагачів.

Компрометація бізнес-електронної пошти (BEC) є серйозним загрозою інформаційній безпеці. Зловмисники отримують доступ до електронної пошти компанії, щоб обманом отримати фінансову вигоду. Цей процес починається зі злому бізнес-систем для отримання доступу до інформації про платіжні системи. Потім вони надсилають шахраянські повідомлення співробітникам, що спонукають їх здійснити платежі на фальшиві банківські рахунки замість реальних.

Шахрайство BEC може відбутися швидко і вимагає від співробітників уваги під час обробки платіжних запитів. Навчання персоналу та дотримання найкращих практик кібербезпеки є важливими. Для запобігання таким атакам організації можуть вживати наступні заходи безпеки:

1. Створення надійних паролів і зміна їх регулярно. Використання складних паролів і уникання використання особистої інформації.

2. Використання ефективного програмного забезпечення, такого як брандмауери та антивірусне програмне забезпечення, для захисту від зловмисного програмного забезпечення.

3. Перевірка платіжних запитів, зокрема перевірка телефоном або особистий контакт для підтвердження будь-яких змін у реквізитах рахунку або платіжних процесах.

4. Використання багатофакторної автентифікації для ускладнення доступу до систем для зловмисників, які не мають необхідних даних для авторизації.

Ці заходи можуть допомогти зменшити ризик від шахрайства BEC та забезпечити безпеку ваших фінансових та інших даних.

1.4 Вимоги до захисту інформаційної системи

В сучасному бізнес-світі безпека інформаційної системи визначається як ключовий фактор конкурентоспроможності та стійкості підприємства. Розглянемо основні аспекти, які визначають ефективність та надійність заходів захисту інформаційних активів підприємства.

1. Строгі вимоги до аутентифікації та авторизації, початок безпеки інформаційної системи починається з чіткої ідентифікації та авторизації користувачів. Важливо використовувати сучасні методи багаторівневої аутентифікації та точного контролю над правами доступу.

2. Шифрування та захист конфіденційної інформації, механізми шифрування необхідно впроваджувати для захисту конфіденційної інформації під час її передачі та зберігання. Використання сучасних алгоритмів шифрування є важливою частиною стратегії захисту.

3. Захист від мережевих атак, створення ефективних мережевих бар'єрів та використання систем виявлення вторгнень є обов'язковими для запобігання атак зовнішніх загроз.

4. Заходи захисту від внутрішніх загроз, важливо впроваджувати стратегії для виявлення та запобігання внутрішнім загрозам. Моніторинг дій персоналу та обмеження прав доступу відіграють ключову роль.

5. Регулярні аудити та тестування безпеки, аудит безпеки та пенетраційне тестування інформаційної системи регулярно проводяться для виявлення та усунення слабких місць у заходах захисту.

6. Ефективне управління інцидентами, важливо мати ефективну систему управління інцидентами для оперативного реагування на потенційні загрози та відновлення нормального функціонування після атаки.

7. Забезпечення безпеки фізичної інфраструктури, крім цифрових заходів, важливо не забувати про захист фізичних активів, таких як серверні приміщення та обладнання.

8. Антивірусні заходи, використання ефективних програм антивірусного та антималware захисту є обов'язковим для забезпечення інформаційної системи від загроз з боку шкідливих програм.

Цей аналіз вимог до захисту інформаційної системи підприємства визначає комплексний підхід до забезпечення безпеки, охоплюючи технічні, організаційні та процесуальні аспекти. Впровадження цих заходів спрямоване на мінімізацію ризиків та забезпечення надійності інформаційної системи підприємства в сучасному високотехнологічному середовищі.

# Висновок до розділу 1

Проаналізовано технології кібернетичного захисту інформаційної системи. Було виявлено, що використання сучасних технологій, таких як шифрування даних, системи виявлення вторгнень та багатофакторна аутентифікація, є ключовими для забезпечення безпеки інформаційних систем.

Розглянуто технічні засоби захисту інформаційної системи. Виокремлено, що використання сучасних антивірусних програм, брандмауерів, систем виявлення вторгнень та інших технічних засобів є важливим для забезпечення безпеки інформаційних систем. Проаналізовано різні технології та їх ефективність у захисті від різних типів кіберзагроз.

Проаналізовано заходи з фізичного захисту систем. Було виявлено, що правильне розташування серверних приміщень, застосування систем контролю доступу та відеоспостереження є важливими для забезпечення безпеки фізичної інфраструктури. Проаналізовано різні методи та підходи до фізичного захисту систем, що дозволяють підвищити рівень безпеки інформаційних систем.

Розглянуто управління доступом, ідентифікацію та аудит. Було виявлено, що ефективне управління доступом, використання ідентифікаційних та аудиторських механізмів дозволяє підвищити рівень безпеки інформаційних систем. Проаналізовано різні підходи та методи управління доступом, що дозволяють ефективно контролювати доступ користувачів до інформаційних ресурсів.

# **2 ОГЛЯД МЕТОДІВ ТА ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

# 2.1 Технології кібернетичного захисту інформаційної системи

Захист інформаційно-комунікаційної безпеки стає стратегічним завданням у контексті сучасного цифрового світу. Це важливий аспект для підприємств у кіберпросторі, оскільки він забезпечує безпеку інформаційних ресурсів та процесів. Загрози, які становляться для конфіденційної інформації, можуть призвести до серйозних фінансових збитків та підірвати довіру клієнтів до бренду компанії.

Важливість безпеки даних відображається у декількох аспектах. По-перше, вона забезпечує безпеку інтелектуальної власності та зберігає цілісність даних. Крім того, вона гарантує дотримання нормативних вимог та правових стандартів. Ці аспекти стають важливими, особливо в контексті зберігання та обробки чутливої інформації.

Безпека даних важлива з таких причин:

1. Забезпечує безпеку вашої інтелектуальної власності.

2. Зберігає цілісність даних.

3. Забезпечує дотримання нормативних та правових стандартів.

Одним із ключових аспектів є конфіденційність даних, оскільки підприємства часто працюють з особистими даними клієнтів та фінансовою інформацією. Недостатній захист може призвести до витоку даних та порушення законодавства, що має негативний вплив на репутацію підприємства.

Також важливою є надійність інфраструктури, оскільки доступність та надійність інформаційних систем є ключовими для безперебійної роботи підприємства. Атаки та вторгнення можуть призвести до втрати доступу до даних та послуг, що може вплинути на продуктивність та ділові процеси [8, 9].

Захист від фінансових втрат є однією з важливих складових безпеки інформаційних систем. Кіберзлочинці можуть використовувати різноманітні атаки, такі як вимагання викупу, викрадання фінансової інформації або фінансові маніпуляції, що може призвести до серйозних фінансових втрат для підприємства. Ефективний захист інформаційних систем є важливим аспектом у запобіганні таким ситуаціям та мінімізації фінансових ризиків.

Дотримання законодавства та стандартів є ще одним важливим аспектом у сфері інформаційної безпеки. Багато країн встановлюють законодавчі вимоги щодо захисту конфіденційності даних та інших аспектів інформаційної безпеки. Недотримання цих вимог може призвести до юридичних проблем, штрафів та інших негативних наслідків для підприємства.

Захист від репутаційних ризиків також має велике значення для підприємства. Втрати даних або вразливість до кібератак можуть суттєво пошкодити репутацію підприємства та викликати втрату довіри з боку клієнтів та партнерів, що може негативно вплинути на прибуток та довгостроковий успіх бізнесу [9].

Ще однією важливою складовою захисту інформаційної безпеки є захист від шпигунства та крадіжок інтелектуальної власності. Підприємства інвестують значні кошти у розробку нових продуктів та інноваційні проекти, тому важливо забезпечити безпеку цієї інформації для збереження конкурентної переваги та запобігання незаконному використанню чи крадіжці.

Узагальнюючи, ефективний захист інформаційної безпеки є критично важливим для забезпечення стійкості та успіху підприємства в умовах швидко зростаючих кіберзагроз [10].

# 2.2 Технічні засоби захисту інформаційної системи

Технічні засоби захисту інформаційних систем (ІС) представляють собою важливий компонент в сфері інформаційної безпеки. Вони призначені для забезпечення безпеки інформації та захисту ІС від небажаного доступу, втручань, а також витоку чи втрати даних. Різноманітність цих технічних засобів дозволяє реалізувати різні аспекти політики безпеки.

1. ***Брандмауери (Firewalls).*** Вони відіграють ключову роль у захисті мережі підприємства. Брандмауери фільтрують мережевий трафік на основі заданих правил безпеки та контролюють зв'язок між внутрішньою та зовнішньою мережами. Основні функції брандмауерів включають фільтрацію пакетів, stateful інспекцію для прийняття рішень на основі історії з'єднання, а також підтримку VPN для безпечного з'єднання на рівні мережі [10].

2. Типи Брандмауерів:

* Мережеві (Network) брандмауери\*\*: Роблять фільтрацію на рівні мережевого рівня (OSI Model) та контролюють трафік між мережами.
* Прикладні (Application) брандмауери\*\*: Фільтрують трафік на рівні застосунків та аналізують дані, що передаються через конкретні додатки.

Одні з основних функцій брандмауерів включають захист від вторгнень, фільтрацію доменних імен для блокування доступу до певних сайтів, а також контроль за використанням мережевих ресурсів. Ці технічні рішення допомагають підприємствам забезпечувати безпеку мережі та захищати їхні інформаційні активи від потенційних загроз [10].

Firewalls виступають як не лише окремий захисний шар, але й ключова складова багатошарових систем захисту. Вони можуть інтегруватися з іншими системами безпеки, щоб створювати комплексні стратегії захисту. Запис подій та інцидентів дозволяє аналізувати мережеву активність та виявляти аномалії, що допомагає у вчасному реагуванні на потенційні загрози.

Постійний моніторинг мережевого трафіку дозволяє вчасно виявляти потенційно шкідливі або аномальні патерни та дії, забезпечуючи реакцію на них перед тим, як вони стануть серйозними проблемами. Інтеграція з іншими засобами захисту, такими як Intrusion Detection System/Intrusion Prevention System (IDS/IPS), дозволяє обмінюватися інформацією для виявлення та блокування загроз на рівні мережі [10].

Окрім цього, Firewalls можуть блокувати недозволені підключення та забезпечувати безпеку беспровідних з'єднань, що є важливим для підтримки безпеки мережі в умовах ростущої загрози кібератак. Ця інтеграція та співпраця з іншими системами забезпечує більш ефективний та надійний рівень захисту інформаційних ресурсів підприємства.

2. ***Антивірусне та антимальварне програмне забезпечення (ПЗ)*** відіграє важливу роль у захисті інформаційних систем від шкідливого програмного забезпечення, такого як віруси, черв'яки, троянські коні та інші види малвари. Ці програми розроблені для виявлення, блокування та видалення такого шкідливого коду, що може нанести шкоду системі.

Основні функції антивірусного ПЗ включають:

1. Сканування файлів. Ця функція здійснює регулярне сканування файлів та системних ресурсів для виявлення потенційно шкідливого коду.

2. Автоматичне оновлення. Програми автоматично завантажують та встановлюють оновлення баз даних для розпізнавання нових видів загроз.

3. Резидентний режим. ПЗ має постійний моніторинг активності системи для виявлення загроз у реальному часі.

4. Карантин та вилучення. Підозрілі файли можуть бути поміщені в карантин та вилучені для забезпечення безпеки системи [11].

Програми виявляють різні типи загроз, включаючи віруси, черв'яки, троянські коні та шпигунське ПЗ, які можуть завдати шкоди інформаційній системі.

Антивірусне та антимальварне ПЗ може інтегруватися з IDS/IPS для обміну інформацією та забезпечення більш ефективного виявлення та блокування загроз на рівні мережі. Виробники надають мультиплатформенні рішення для різних операційних систем, а також забезпечують можливість централізованого управління для корпоративних мереж, що дозволяє встановлювати, конфігурувати та оновлювати ПЗ на великій кількості комп'ютерів з централізованої консолі.

Такий підхід дозволяє ефективно захищати інформаційні ресурси підприємства від широкого спектру потенційних загроз [11].

3. ***Система виявлення атак та запобігання вторгненням (IDS/IPS)*** є ключовою складовою в сучасних стратегіях кібербезпеки. IDS відповідає за виявлення аномальної або потенційно шкідливої активності в мережі чи системі, в той час як IPS може автоматично реагувати та блокувати несанкціоновані дії.

IDS використовується для моніторингу та аналізу активності в мережі чи на окремій системі. Він оперативно реагує на незвичайні або підозрілі події, аналізуючи мережевий трафік та системні журнали. Ця система використовує два основних методи виявлення атак: сигнатурний аналіз, який порівнює активність із відомими сигнатурами відомих атак, та аномалійний аналіз, який виявляє невідомі атаки шляхом виявлення неприродних патернів чи аномалій у поведінці системи.

Основною метою IDS є виявлення можливих загроз та сповіщення адміністраторів чи безпекового персоналу про тривожні ситуації. IDS не блокує трафік самостійно, але надає інформацію для подальшого аналізу та втручання.

У відміну від IDS, система запобігання вторгненням (IPS) має активні функції блокування та утримання атак. IPS автоматично реагує на виявлені загрози, блокуючи чи обмежуючи трафік, що викликає тривожні події. Це надає системі можливість запобігти потенційно шкідливим вторгненням та забезпечує реальний захист [10].

IDS і IPS часто інтегруються для створення комплексного захисного обрамлення для мережі чи інформаційної системи. Їх взаємодія надає організаціям засіб ефективного виявлення та захисту від широкого спектру кіберзагроз. Такий підхід дозволяє забезпечити високий рівень безпеки та захисту цінних інформаційних ресурсів.

4***. Шифрування даних*** відіграє важливу роль у сучасних системах безпеки та забезпечує конфіденційність та цілісність інформації. Цей процес застосовується для захисту даних від несанкціонованого доступу та забезпечення їхньої безпеки під час передачі та зберігання [10, 11].

Шифрування ґрунтується на математичних або алгоритмічних методах перетворення звичайного тексту у криптограму, яка може бути розшифрована лише за допомогою спеціального ключа. Основні принципи включають в себе використання різних алгоритмів шифрування та ключів.

Алгоритми шифрування використовуються для зміни структури даних таким чином, щоб вони стали нерозпізнаваними без відповідного ключа. Ключі можуть бути симетричними, коли один ключ використовується як для шифрування, так і для розшифрування даних, або асиметричними, коли для цих операцій використовуються різні ключі.

Симетричне шифрування, як, наприклад, Advanced Encryption Standard (AES), використовує один і той же ключ для обох операцій, тоді як асиметричне (публічний ключ) шифрування, як RSA (Rivest-Shamir-Adleman), використовує два ключі - публічний та приватний.

Хешування - це ще один метод шифрування, де для даних створюється фіксований "хеш" або хеш-сума, яка використовується для перевірки цілісності даних [11].

Шифрування даних вважається важливою складовою для захисту інформації на підприємствах, оскільки воно забезпечує високий рівень конфіденційності та захист від несанкціонованого доступу. Його ключові переваги включають в себе забезпечення безпеки та конфіденційності важливих даних, а також довіреність та відсутність можливості несанкціонованого доступу до них.

5. ***Безпека мережі***, зокрема через використання віртуальних приватних мереж (VPN) та віртуальних локальних мереж (VLAN), грає ключову роль у забезпеченні захисту мережевого трафіку та конфіденційності даних під час їх передачі через мережу.

Віртуальні приватні мережі (VPN) створюють зашифроване з'єднання між користувачем та мережею, що дозволяє передавати дані через неприватну мережу (таку як Інтернет) з високим рівнем конфіденційності. VPN забезпечує захист інформації, що передається між користувачем та мережею, шляхом шифрування даних та встановленням безпечного тунелю з надійними протоколами передачі даних [12].

Віртуальні локальні мережі (VLAN) дозволяють створювати логічні сегменти в мережі, які ізолюють та обмежують доступ до даних для певних користувачів або пристроїв. Це допомагає уникнути несанкціонованого доступу до чутливої інформації та збереження конфіденційності даних. VLAN дозволяють розділяти мережевий трафік на логічні групи, що зменшує ризик перехоплення чи маніпулювання даними в мережі [12].

6. ***Системи резервного копіювання та відновлення даних*** відіграють важливу роль у сучасних стратегіях забезпечення інформаційної безпеки та управління даними. Вони забезпечують надійне зберігання і можливість відновлення даних у випадку втрати або пошкодження, що є критично важливим для забезпечення безперервності бізнес-процесів.

Ключові аспекти включають розробку чіткого плану резервного копіювання, у тому числі визначення стратегій копіювання (повного, інкрементального, диференціального), використання надійних систем зберігання даних з можливістю стиснення та шифрування, а також тестування та перевірку процесів відновлення та планів аварійного відновлення [12].

Технологічна інфраструктура включає в себе сучасні системи зберігання та автоматизацію щоденних завдань за допомогою управління та моніторингу. Надійна система резервного копіювання також повинна враховувати заходи безпеки, такі як обмеження доступу та антивірусний захист, щоб забезпечити захист копій від потенційних загроз [12].

Основна увага приділяється надійності процесу відновлення, включаючи регулярне тестування та врахування резервного відновлення в рамках загального плану аварійного відновлення організації. Розробка систем резервного копіювання зосереджена на інтеграції хмарних рішень та використанні аналітичних інструментів для оптимізації стратегій резервного копіювання.

7. ***Ідентифікація та автентифікація*** є важливими елементами у сфері інформаційної безпеки, спрямованими на забезпечення безпечного та авторизованого доступу до ресурсів. Ці концепції використовуються як у особистих, так і у корпоративних середовищах для визначення особи чи системи, яка намагається отримати доступ, і визначення, чи має ця особа чи система дійсно право на доступ [13].

Автентифікація використовує унікальний ідентифікатор, такий як ім'я користувача, для ідентифікації особи чи системи. Цей ідентифікатор має бути унікальним і однозначно ідентифікувати конкретного користувача або систему. Після ідентифікації особи або системи проводиться процес автентифікації, який визначає, чи може ця особа або система дійсно отримати доступ. Для цього використовуються різні фактори автентифікації, такі як паролі, біометричні дані, смарт-карти тощо.

Принципи ідентифікації та автентифікації полягають у забезпеченні високого рівня безпеки без ускладнення процесу використання для законних користувачів. Двофакторна автентифікація стає стандартом для забезпечення додаткового рівня безпеки, оскільки вона вимагає введення двох різних факторів для підтвердження ідентичності [13].

Сучасні технології включають біометричну аутентифікацію та синхронізацію з мобільними пристроями. Управління ідентифікацією та доступом використовує централізовані системи для керування користувачами та їхніми дозволами, а аудит і журналювання допомагають виявляти аномалії та контролювати доступ.

8. ***Засоби авторизації в інформаційних системах*** є ключовими елементами забезпечення безпеки та управління доступом до ресурсів. Цей процес визначає права та можливості конкретного користувача або системи після успішної автентифікації та включає різні технічні та організаційні аспекти.

Визначення прав доступу є ключовим елементом інструментів авторизації, де автентифікованим користувачам призначаються певні дії та ресурси. Авторизація на основі ролей спрощує керування доступом, призначаючи користувачам ролі з відповідними дозволами.

Автоматизовані політики безпеки визначають правила авторизації на основі стандартів і вимог внутрішньої безпеки [14]. Двофакторна аутентифікація використовує додатковий метод разом із звичайним паролем, що підвищує рівень безпеки.

Моніторинг і аудит дій користувачів є важливим аспектом інструментів авторизації, які виявляють несподівані або потенційно небезпечні взаємодії. Управління сеансами та моніторинг активних сеансів користувачів забезпечують додатковий рівень безпеки [14].

Усі ці аспекти засобів авторизації призначені для забезпечення ефективного та безпечного адміністративного контролю над доступом до ресурсів інформаційної системи. Вони сприяють забезпеченню конфіденційності, цілісності та доступності інформації, а також дозволяють управляти ризиками та забезпечувати виконання внутрішніх політик безпеки.

9. ***Системи моніторингу та аудиту*** в інформаційних системах компаній є комплексним підходом, спрямованим на виявлення, ідентифікацію та відстеження подій, які можуть вплинути на безпеку та надійність інформації.

Наявні системи відстежують можливі загрози та події в режимі реального часу, виявляючи аномалії та спроби несанкціонованого доступу в мережевому трафіку. Аудит активності користувачів передбачає детальну реєстрацію всіх дій в системі, від авторизації користувача до взаємодії з файлами та ресурсами [15].

Такі системи також можуть виявляти аномалії та незвичність за допомогою алгоритмів та штучного інтелекту, щоб попереджати про можливі загрози. Головний акцент робиться на захисті інфраструктури та даних, включаючи моніторинг серверів, мережевого обладнання та інших критичних компонентів.

Крім того, система забезпечує глибокий аналіз журналів подій для виявлення вразливостей і слабких місць системи. Вона також взаємодіє з програмами реагування на інциденти для ефективного блокування загроз та відновлення стабільності системи [15].

Важливим аспектом є забезпечення відповідності та аудиту, коли система сприяє детальному обліку змін і доступу, забезпечуючи відповідність інформаційних систем нормативним вимогам і стандартам.

2.3 Заходи з фізичного захисту систем

Забезпечення фізичної безпеки важливе для забезпечення безпеки інформаційних систем на підприємстві. Нижче наведено перелік ключових заходів, які можна впровадити для досягнення цієї мети:

1. Контроль доступу до приміщень:

* Встановлення системи контролю доступу, таких як електронні картки або біометричні системи.
* Обмеження доступу до приміщень, де розташовані серверні кімнати та інші важливі ресурси.

2. Відеоспостереження:

* Встановлення системи відеоспостереження для моніторингу важливих зон та точок доступу.
* Розміщення камер в областях, де зберігається або обробляється важлива інформація.

3. Фізична охорона:

* Наявність фізичної охорони для моніторингу та контролю доступу.
* Здійснення регулярних перевірок та обходів для виявлення будь-яких незвичайних ситуацій.

4. Захист інфраструктури:

* Розташування серверних кімнат внутрішньої частини будівлі для ускладнення фізичного доступу.
* Захист інфраструктури від природних катастроф, таких як пожежі, повені або землетруси.

5. Безпека обладнання:

* Фізичне закріплення серверів, комутаторів та іншого обладнання, щоб уникнути його крадіжки чи неправомірного доступу.
* Використання захисних корпусів та кабельних систем.

6. Забезпечення резервного живлення:

* Для систем інформаційної обробки та зберігання, щоб уникнути можливих втрат даних в разі відключення електроенергії.

7. Безпека пристроїв зберігання даних:

* Захист фізичного доступу до пристроїв зберігання даних, таких як серверні багатоплатформенні системи чи файлові сервери.

8. Ідентифікація та маркування обладнання:

* Застосування систем ідентифікації та маркування обладнання для визначення власності та виявлення неправомірного використання [9-11].

Важливо помітити, що окрім перелічених вище заходів, існують інші способи забезпечення фізичної безпеки інформаційних систем на підприємстві. Один з таких методів - регулярне навчання персоналу щодо правил безпеки та процедур реагування на небезпеку. Інформування співробітників про потенційні загрози, виклики та найкращі практики є важливою складовою фізичної безпеки.

Ретельне планування і розробка процедур евакуації та надзвичайних ситуацій можуть допомогти у зменшенні можливих ризиків. Це включає в себе розробку ефективних планів евакуації, навчання персоналу діяти у випадку пожежі, природних катастроф або інших надзвичайних ситуацій, а також проведення регулярних перевірок та тренувань для підтримання готовності до дій у будь-який час. Тільки комплексний підхід до фізичної безпеки може забезпечити ефективний захист інформаційних систем від потенційних загроз [12].

2.4 Управління доступом, ідентифікація та аудит

Управління доступом, ідентифікація та аудит є важливими складовими системи захисту інформаційної інфраструктури підприємства, спрямованими на забезпечення безпеки та конфіденційності даних [12].

Управління доступом включає такі аспекти:

***Ролева модель***. Це система, що визначає ролі користувачів та надає їм відповідні права доступу, що спрощує процес управління доступом та зменшує ризики надання непотрібних прав.

***Система контролю доступу***. Вона сприяє використанню сучасних засобів, таких як електронні картки або біометричні методи, для обмеження доступу до важливих приміщень та ресурсів.

***Централізоване управління***. Включає створення централізованої системи управління, яка дозволяє ефективно керувати доступом та внесенням змін у права користувачів.

***Двофакторна аутентифікація***. Використання двофакторної аутентифікації для підвищення рівня безпеки, наприклад, за допомогою коду з смарт-карти чи мобільного пристрою [12].

Ідентифікація включає такі кроки:

* Використання унікальних ідентифікаторів для кожного користувача або системи, таких як логіни, паролі та/або біометричні дані.
* Централізоване керування ідентифікацією для ефективного управління реєстрацією та скасуванням доступу для користувачів.
* Активне відстеження для негайного виявлення та реагування на несанкціонований доступ або використання ідентифікаторів.

Аудит включає такі аспекти:

* Система журналювання подій для реєстрації всіх подій, пов'язаних із змінами в системі та доступом користувачів.
* Глибокий аналіз журналів подій для виявлення аномалій, вторгнень чи інших потенційно небезпечних ситуацій.
* Регулярні аудити системи безпеки для виявлення та виправлення слабких місць та забезпечення відповідності стандартам безпеки.

Завдяки ефективному управлінню доступом, ідентифікацією користувачів та аудитуванням системи можна забезпечити високий рівень безпеки інформації, захистити конфіденційні дані та запобігти несанкціонованому доступу до системи [13, 14].

Висновок до розділу 2

Досліджено, що вивчення технологій захисту інформаційних систем є невід'ємною частиною підготовки до сучасних викликів у сфері інформаційної безпеки. Проаналізовано, що ключовими аспектами, які сприяють створенню комплексної системи захисту, є використання технічних засобів, заходів фізичного захисту та управління доступом.

Зазначено, що використання технічних засобів, таких як антивірусне програмне забезпечення, брандмауери та системи IDS/IPS, є надзвичайно важливим для ефективного захисту інформаційної інфраструктури. Вони взаємодіють між собою, щоб виявляти та запобігати загрозам безпеки, створюючи таким чином надійний бар'єр перед потенційними атаками.

Виокремлено, що заходи фізичного захисту, такі як контроль доступу та використання систем відеоспостереження, також відіграють критичну роль у забезпеченні безпеки інформаційних ресурсів. Їхня ефективна реалізація доповнює захист, забезпечений технічними засобами, створюючи комплексний підхід до захисту.

Зроблено висновок, що ефективне управління доступом, ідентифікацією користувачів та аудитом є важливими складовими системи захисту. Їхнє правильне впровадження і поєднання дозволяють забезпечити конфіденційність, цілісність та доступність даних у сучасному цифровому середовищі.

**3 ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА**

3.1 Огляд існуючої інформаційної системи підприємства

У прагненні до покращення інформаційної системи, компанія ТОВ "Intellias" акцентує увагу на захисті конфіденційної інформації, включаючи дані про своїх співробітників, які відіграють ключову роль у сфері кібербезпеки. Особлива увага приділяється розвитку та забезпеченню безпеки інформаційної інфраструктури підприємства.

Центральна будівля, де розташовані обмежені області доступу до важливої інформації, підтримується постійною чергою охоронців, системою контролю доступу та відеоспостереженням. На малюнку 3.1 зображено структуру відділів та робочі місця працівників, а також місцезнаходження серверного обладнання [14].

Різні підрозділи забезпечують обробку різних категорій даних, що гарантує ефективність роботи та безпеку передачі інформації між ними. Наприклад, бухгалтерія та юридичний відділ мають особливе значення, оскільки вони зберігають фінансові та юридичні документи, які потребують найвищого рівня захисту.

Таким чином, "Intellias" вкладає значні зусилля в забезпечення надійності і безпеки своєї інформаційної системи, розуміючи, що це є ключовим фактором для забезпечення стабільності та успішного функціонування компанії.

Якщо ці дані буде втрачено або змінено, бізнес може зазнати значних збитків або навіть повністю припинити своє існування [15].

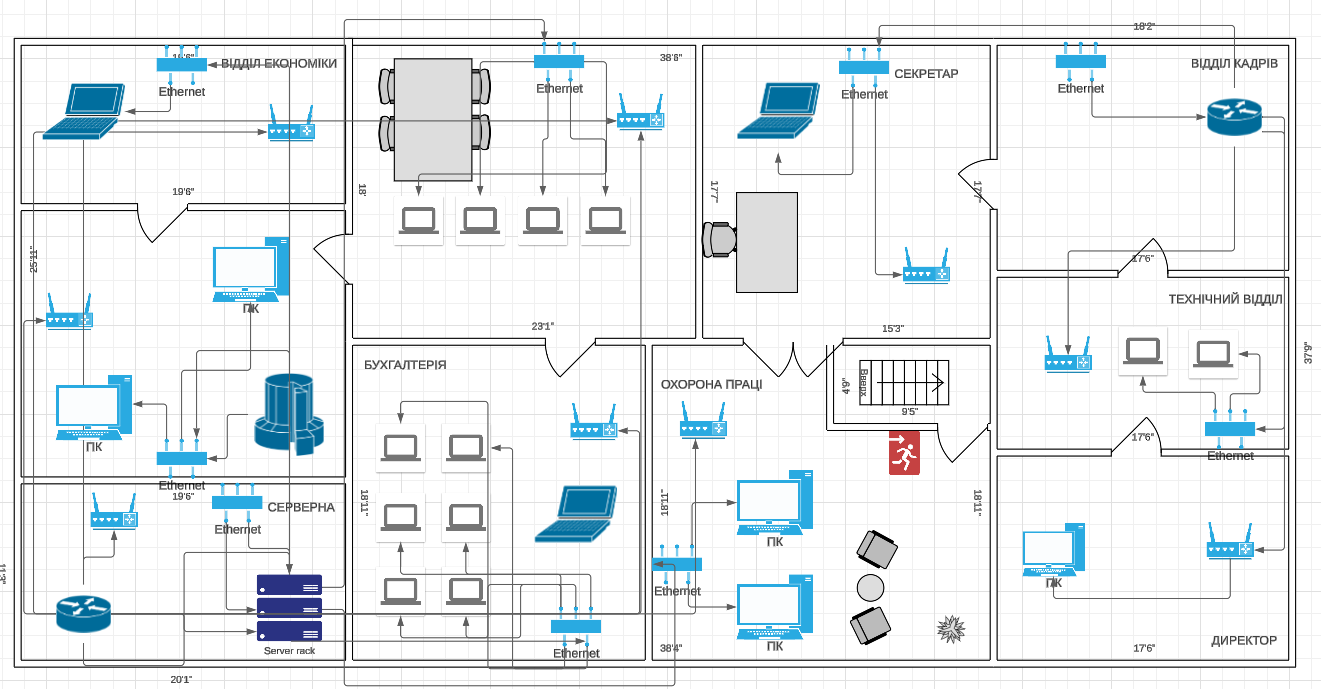


Рис. 3.1. Схематичне зображення будівлі ТОВ «Intellias»

Загальний перелік інформаційних ресурсів в інфраструктурі ТОВ "Intellias":

1. Комерційна таємниця:

- Заробітна плата співробітників.

- Контракти з постачальниками та покупцями.

- Технології виробництва.

2. Інформація з обмеженим доступом:

- Трудові договори.

- Особисті справи співробітників.

- Документація відділу складу.

- Особисті картки працівників.

- Бухгалтерська та внутрішня облікова інформація.

- Бухгалтерський та юридичний відділи.

- Інші розробки та документи для внутрішнього користування.

3. Публічна інформація:

- Статут та установчі документи.

- Прайс-лист товарів.

Наданий перелік відображає різноманітність типів інформації, що зберігаються та обробляються в інфраструктурі компанії "Intellias", а також підкреслює важливість правильного управління та захисту кожного з них [16].

Інфраструктура ТОВ "Intellias" є складною та ретельно налаштованою системою, яка об'єднує різноманітні компоненти для забезпечення надійності та ефективності роботи. Давайте розглянемо кожен з елементів інфраструктури детальніше [17].

1. Сервери. У компанії використовуються сервери, які відповідають за обробку запитів від робочих станцій. Ці сервери забезпечують централізоване управління ресурсами та дозволяють робочим станціям отримувати доступ до необхідних даних і програм.

2. Мережеві комутатори. Некеровані комутатори TP-Link і DLink використовуються для підключення комп'ютерів і пристроїв в мережі. Вони автоматично розподіляють дані між підключеними пристроями, що спрощує мережеве підключення без необхідності складної конфігурації [18].

3. Маршрутизатори. Маршрутизатори TP-Link використовуються для забезпечення з'єднання між різними комп'ютерними мережами та керування обміном даними між ними. Вони грають важливу роль у забезпеченні безпеки мережі та оптимізації шляху передачі даних.

4. Брандмауер (Cisco ASA). Цей пристрій використовується для забезпечення безпеки мережі. Він фільтрує вхідні та вихідні пакети даних, контролює доступ до мережевих ресурсів та захищає мережу від зовнішніх загроз.

Заходи з захисту інформаційної системи ТОВ "Intellias" включають різні аспекти:

* **Автентифікація.** Визначення і перевірка ідентифікації користувачів перед наданням доступу до системи.
* **Авторизація.** Надання користувачам відповідних прав доступу після успішної автентифікації.
* **Зміна стандартного порту маршрутизатора для підключень RDP.** Захист системи від потенційних атак шляхом зміни стандартного порту, що знижує вразливість системи.

Навіть при вживаних заходах безпеки, зроблених у ТОВ "Intellias", комплексний аналіз показує, що існуючі заходи можуть бути недостатніми для повного забезпечення безпеки інформаційної системи. З огляду на постійне зростання загроз кібербезпеці, включаючи нові методи атак та вразливості програмного забезпечення, необхідно посилити заходи безпеки. Подальше вдосконалення системи захисту є критичним для забезпечення максимального рівня захисту конфіденційної інформації, уникнення втрат даних та запобігання можливим кібератакам [18, 19].

3.2 Створення та впровадження стратегій посилення кібербезпеки

При розробленні захищеного варіанта функціонування інформаційної мережі ТОВ "Intellias" враховувалася її здатність відповідати ростучим потребам підприємства у забезпеченні якості обслуговування, безпеки та продуктивності. Для цього було обрано обладнання від Cisco Systems, враховуючи його характеристики.

З фінансових і практичних міркувань, а також з урахуванням необхідності кіберзахисту мережі підприємства, було прийнято рішення встановити міжмережевий екран Cisco ASA 5506-X. Це обладнання забезпечує надзвичайний рівень захисту від мережевих загроз, включаючи глибоку перевірку мережі, аналіз окремих потоків даних та підтримку передачі голосових і відеоданих через VPN.

Міжмережевий екран Cisco ASA 5506-X (рис. 3.2) оснащений 8 портами 10/100/1000 BaseT Ethernet, 1 портом USB 2.0, серійними портами RJ-45 Console і Mini USB, а також блоком живлення AC, що відповідає потребам підприємства у забезпеченні безпеки та продуктивності в мережі [19].



Рис. 3.2 – Міжмережевий екран Cisco ASA 5506-X

***Таблиця 3.1*** Технічні характеристики Cisco ASA 5506-X [28]

|  |  |
| --- | --- |
| Тип пристрою | Міжмережевий екран |
| Порти доступу Ethernet | 8 x GE RJ-45 |
| Число IPSec VPN | 10 |
| Продуктивність FIREWALL | 750 Мбіт/с |
| VLAN 802.1q стандарт/макс | 5/30 |
| Габаритні розміри (ВхШхГ) | 4,45x20,04x17,45 |
| Пам’ять FLASH | 16 Гб |
| Об’єм ОЗУ | 4 Гб |
| Тип живлення | AC 100-240В |
| IPSec VPN 3DES/AES | 100 Мбіт/c |
| Нових сесій в секунду, макс | 5000 |
| Тип встановлення | Настільне |
| Продуктивність IPS | 125 Мбіт/с |
| Висока доступність | Ні |
| Кількість захищених вузлів | Не обмежено |

Для підприємства також обрано маршрутизатор Cisco 2811. Цей маршрутизатор відомий своєю надійністю та розширеними можливостями безпеки, які відповідають концепції самозахисту мережі Cisco Self-Defending Network. Він оснащений програмним забезпеченням Cisco IOS та підтримує функції IPSec VPN для забезпечення безпеки мережі.

Основні характеристики маршрутизатора Cisco 2811 включають високу продуктивність, модульну архітектуру та апаратну підтримку. Він також забезпечує можливості використання засобів безпеки, таких як запобігання вторгненням (IPS), контроль доступу (NAC) і фільтрація URL. Крім того, маршрутизатор підтримує технологію мережевої передачі живлення Power over Ethernet (PoE).

Маршрутизатор Cisco 2811 має наступні порти: 2 порти Fast Ethernet (10/100BASE-T), 2 порти USB 1.1, 4 слоти HWIC/WIC/VIC/VWIC, 1 слот NM/NME, 2 слоти PVDM2 і 2 слоти AIM. Ці характеристики роблять маршрутизатор Cisco 2811 ідеальним вибором для забезпечення безпеки та продуктивності в мережі підприємства (рис. 3.3) [19].



Рис. 3.3 – Маршрутизатор Cisco 2811

***Таблиця 3.2*** Технічні характеристики Cisco 2811

|  |  |
| --- | --- |
| Тип пристрою | Маршрутизатор |
| Вбудовані порти LAN | 2\*10/100 ТХ |
| Пам’ять Flash, Мб (станд./макс) | 64 / 128 |
| Пам’ять DRAM, Мб (станд./макс) | 256 / 768 |
| Інтегровані PVDM (DSP) слоти | 2 |
| Підтримка інтерфейсних карт | 4 слота (кожен слот підтримує любий HWIC, WIC, VIC и VWIC-модулі) |
| Наявність мережевих слотів | 1 |
| Порти USB 1.1 | 2 |
| Консольний порт (до 115.2 Кбіт/с) | 1 |
| Додатковий порт (AUX) (до 115.2Кбит/с) | 1 |
| Апаратне прискорення VPN | DES, 3DES, AES 128, AES 192, та AES 256 |
| AC-IP Maximum In-Line Power Distribution | 160W |

3.3 Оцінка ефективності застосування захисних можливостей Cisco ASA 5506-X

Забезпечення безпеки інформаційних систем стає все більш критичним завданням у сучасному цифровому середовищі, з урахуванням постійно зростаючих загроз та кількості кібератак. Для підприємства, такого як ТОВ «Intellias», вивчення та оцінка ефективності технологій захисту, зокрема Cisco ASA 5506-X, є необхідним для забезпечення стійкості інформаційної інфраструктури [20].

Cisco ASA 5506-X є міцним та багатофункціональним рішенням для захисту мережі. Він володіє рядом можливостей, включаючи фірмені фаєрволи, виявлення вторгнень та підтримку VPN-з'єднань [21].

Аналіз ефективності систем виявлення вторгнень та запобігання вторгненням, використання сигнатурних та аномалійних методів виявлення, а також систем аналізу поведінки є важливим для оцінки захисту мережі. Розгляд систем аутентифікації користувачів та пристроїв, включаючи використання сильних паролів та багаторівневу аутентифікацію, також є ключовим аспектом забезпечення безпеки.

Дослідження використання ACL для обмеження доступу до різних мережевих ресурсів та сервісів в залежності від користувацьких ролей, а також оцінка системи моніторингу для виявлення несанкціонованого доступу, також важливі для ефективного захисту мережі [23].

Подальше дослідження включає вивчення заходів, що застосовуються для захисту від DoS-атак та інших атак, спрямованих на вичерпання ресурсів, оцінку здатності систем виявлення вторгнень реагувати на виявлені загрози, та аналіз технологій, які виявляють аномальні патерни поведінки в мережі.

Глибокий аналіз рівня шифрування, використання тунельної архітектури та ефективності управління ключами для забезпечення безпеки VPN-з'єднань є ще одним важливим аспектом дослідження. Оцінка надійності використовуваних алгоритмів шифрування та ефективність систем управління ключами допомагає забезпечити безпеку передачі даних через VPN-з'єднання.

3.4 Пропозиції щодо використання захисної технології для критичної інфраструктури на прикладі Cisco ASA 5506-X

Для налаштування пристрою Cisco ASA 5506-X для забезпечення функцій захисту мережі використовуються основні команди, які дозволяють визначити тип обладнання, призначити імена інтерфейсів, встановити рівні безпеки, призначити IP-адреси та налаштувати маршрутизацію.

Команда "*interface*" використовується для встановлення параметрів продуктивності та ініціалізації інтерфейсів пристрою. "Nameif" призначає імена інтерфейсам ASA, що спрощує їхню ідентифікацію. Рівень безпеки для кожного інтерфейсу визначається за допомогою команди "security-level", де значення за замовчуванням встановлені для зовнішнього та внутрішнього інтерфейсів.

За допомогою команди "ip-адреса" призначаються IP-адреси кожному інтерфейсу, а "*маршрутизація*" використовується для встановлення статичних маршрутів для інтерфейсів, що дозволяє пристрою визначати кращий шлях до пункту призначення [25, 26].

Наприклад, при налаштуванні двох інтерфейсів, які відповідають за зовнішню та внутрішню мережі, встановлюються відповідні параметри за допомогою вищезгаданих команд. Результати налаштування представлені на відповідному рис. 3.4.

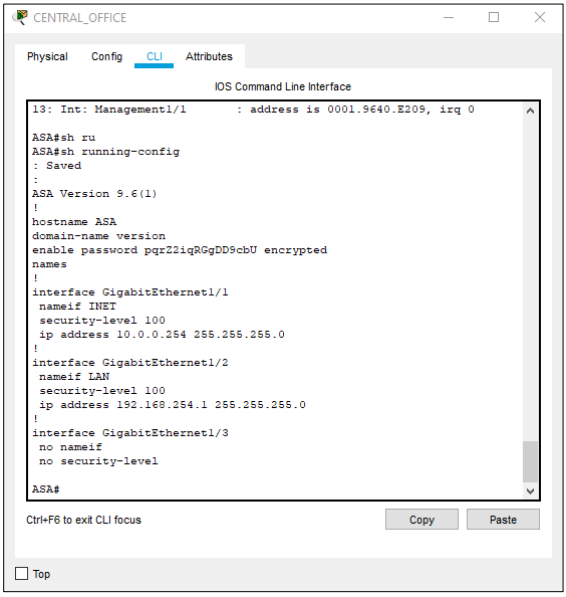
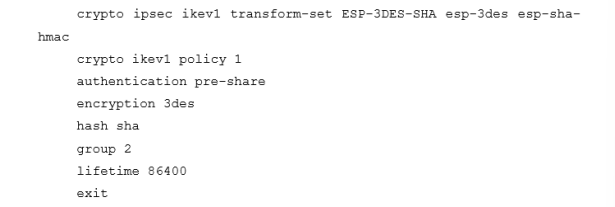


Рис. 3.4 – Налаштування інтерфейсів

Далі налаштовуємо параметри шифрування за допомогою протоколу IPSec, який забезпечує захист передачі даних через Інтернет-протокол IP. Це дозволяє забезпечити конфіденційність, цілісність та аутентифікацію даних під час їхньої передачі (рис. 3.5).

Для налаштування використовуються відповідні команди, які вказані в лістингу 3.1. За допомогою цих команд встановлюються параметри шифрування, аутентифікації та інші параметри, які визначають політику безпеки IPSec. Коли дві політики збігаються, IPSec встановлюється для забезпечення консистентності та безпеки даних між вузлами мережі.

Лістинг 3.1 – налаштування параметрів шифрування IPSec показані на відповідному рисунку, де враховані всі вимоги щодо конфігурації політики безпеки.



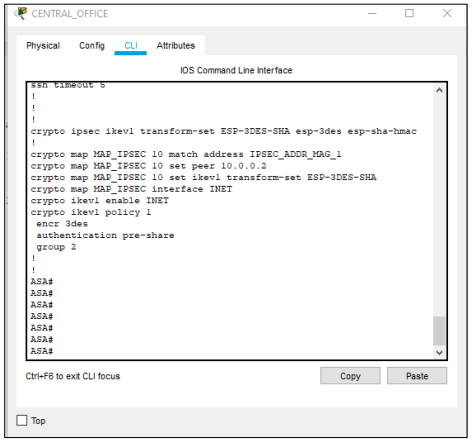


Рис. 3.5 – Налаштування параметрів шифрування за допомогою набору протоколів IPSec

Для встановлення правил контролю доступу для потрібного VPN-трафіку необхідно використовувати розширений або іменований список контролю доступу, який визначає специфічний трафік, що має бути захищений за допомогою шифрування. На основі цих списків визначаються параметри фільтрації, які вказують, який трафік має бути дозволений або заборонений через VPN-з'єднання.

Результати налаштування правил контролю доступу показані на (рис. 3.6), де враховані всі вимоги до забезпечення безпеки та обмеження доступу до мережевих ресурсів через VPN.

Лістинг 3.2 – Налаштування списку контролю доступу





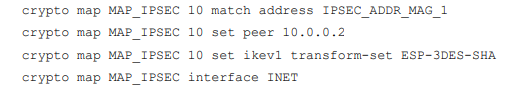
Рис. 3.6 – Налаштування списку контролю доступу

Налаштування шифрування та його застосування до інтерфейсу INET представлено в лістингу 3.3. Результати цих коригувань показані на рисунку 3.7.

Схема шифрування визначає політику IPsec, яка узгоджується в IPSEC SA. Ця політика включає в себе:

* Використання списків контролю доступу для визначення, які пакети дозволені та захищені за допомогою з'єднань IPSec.
* Ідентифікацію тимчасових вузлів.
* Визначення локальної адреси трафіку IPSec.
* Встановлення набору трансформацій для протоколу IKEv1.

Лістинг 3.3 – Налаштування кріптосхеми



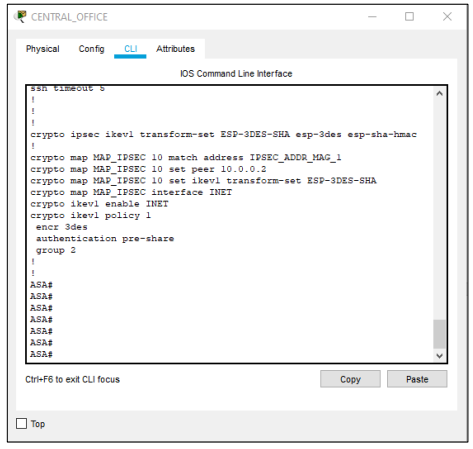
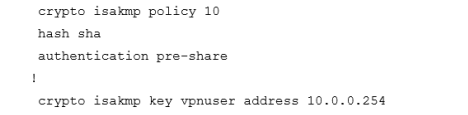


Рис. 3.7 – Налаштування кріптосхеми

Для підприємства ТОВ «Intellias» рекомендовано використовувати маршрутизатор Cisco 2811. Почнемо з налаштування ISAKMP - протоколу обхіду асоціації безпеки Інтернету та керування ключами. ISAKMP надає основу для обміну ключами, необхідних для встановлення захищеного з'єднання. Зазвичай для цього використовується протокол IKE - стандартний механізм, який використовується для налаштування і керування з'єднаннями IPSec в VPN.

Створимо політику ISAKMP з типом тунелю L2L (лістинг 3.4).

Лістинг 3.4 – Створення політики ISAKMP



Команда «***crypto isakmp policy***» використовується для налаштування політики IKE та визначення алгоритмів і параметрів, що необхідні для створення захищеного каналу. У наведеному списку створюється політика IKE з пріоритетом 10. Результат виконання цієї команди показано на рис. 3.8.

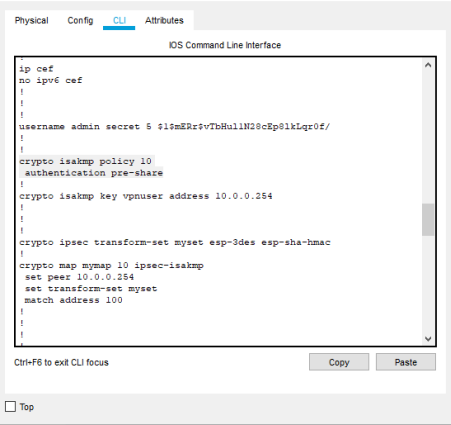


Рис. 3.8 – Створення політики ISAKMP

Давайте створимо політику для ефективного шифрування даних. Це можна зробити за допомогою вказаних у лістингу 3.5 команд. Створення політик показано на рисунку 3.9.

Лістинг 3.5 – Створення політики



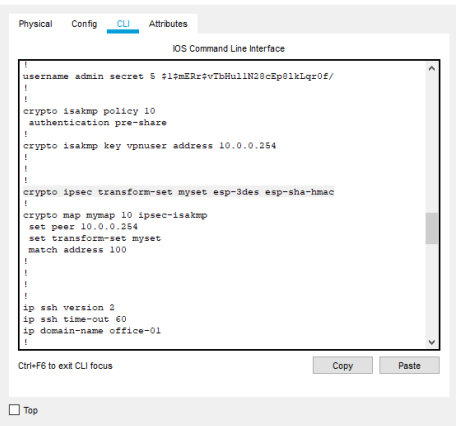
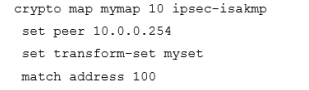


Рис. 3.9 – Створення політики

Створимо актуальну криптографічну карту, використовуючи наведені в лістингу 3.6 команди.

Лістинг 3.6 – Створення криптографічної карти



Результат виконання команди наведено на рисунку 3.10

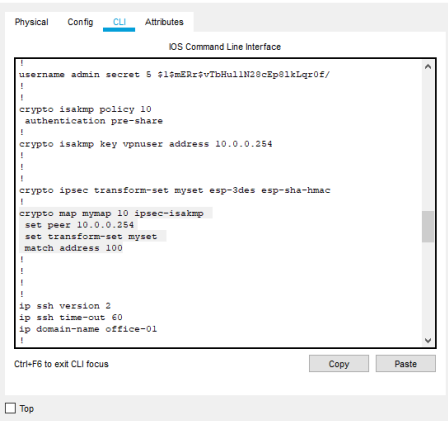
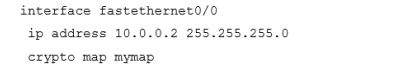


Рис. 3.10 – Створення криптографічної карти

Використаємо криптографічну карту на зовнішньому інтерфейсі, використовуючи наведені в лістингу 3.7 команди. Застосування криптографічної карти на зовнішній інтерфейс показано на рисунку 3.11.

Лістинг 3.7 – Застосування криптографічної карти на зовнішній інтерфейс



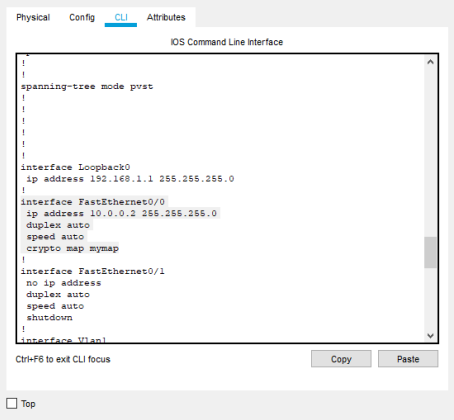
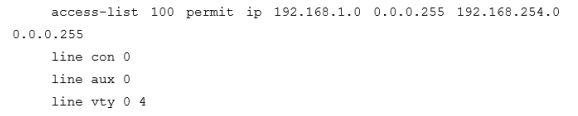


Рис. 3.11 – Застосування криптографічної карти на зовнішній інтерфейс

Створюємо ACL (Список Контролю Доступу) для зашифрованого трафіку (рис. 3.12).

Лістинг 3.8 – Створення ACL (Access Control List) для зашифрованого трафіку



Трафік з 192.168.1.0 до 192.168.254.0 зашифровано. Трафік, який не відповідає списку доступу, незашифрований для Інтернету.

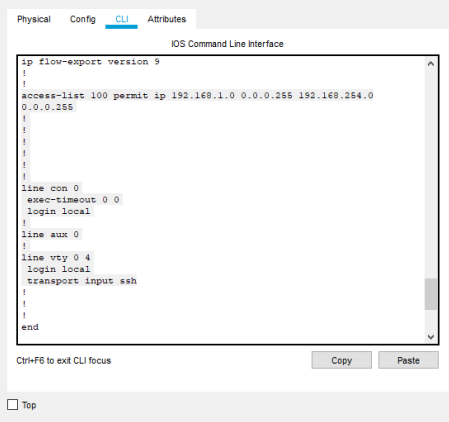


Рис. 3.12 – Створення АСL для зашифрованого трафіку

Висновки до розділу 3

Розроблено рекомендації технології для забезпечення безпечного функціонування критичної інфраструктури підприємства виявлено ряд ключових аспектів, які потребують уваги. Огляд існуючої інформаційної системи підприємства виявив ідентифікацію критичних точок з уразливістю, які потребують негайного усунення. Зокрема, було виявлено недостатність заходів кібербезпеки та потребу у посиленні існуючих стратегій для запобігання можливим загрозам.

Виокремлено стратегії посилення кібербезпеки, які включають в себе розроблення та впровадження нових заходів безпеки. Ці стратегії мають на меті забезпечення більш ефективного контролю над доступом до інформації, виявлення та реагування на потенційні загрози та забезпечення безперебійного функціонування системи в умовах постійно зростаючого рівня кіберзлочинності.

Розроблено пропозиції щодо використання захисної технології для критичної інфраструктури на прикладі Cisco ASA 5506-X. Ці пропозиції включають у себе рекомендації щодо оптимального конфігурування та впровадження інструменту з метою максимізації ефективності та безпеки інформаційної системи підприємства.

**ВИСНОВКИ**

Під час аналізу та оцінки потенційних загроз було виявлено, що безпека інформаційної системи підприємства ТОВ "Intellias" безпосередньо впливає на його фінансовий стан, репутацію та дотримання законодавства. Для запобігання можливим втратам необхідний комплексний підхід та управління ризиками на всіх рівнях.

На основі аналізу сучасних методів інформаційної безпеки зроблено висновок про важливість дослідження технологій захисту інформаційних систем. Виділено ключові аспекти, що сприяють створенню комплексної системи захисту.

Використання технічних засобів, таких як антивірусне програмне забезпечення, брандмауери та системи IDS/IPS, визначено як вирішально важливе для ефективного захисту інформаційної інфраструктури. Проаналізовано їх взаємодію та роль у забезпеченні безпеки.

В процесі створення технології забезпечення захищеного функціонування інформаційної системи підприємства проведено основні налаштування пристроїв забезпечення безпеки Cisco ASA, зокрема налаштування інтерфейсів, параметрів шифрування, списків контролю доступу та криптосхем. Для забезпечення шифрування даних по мережевому протоколу IP налаштовано засіб IPsec.

Усе це веде до висновку про створення варіанту технології забезпечення захищеного функціонування інформаційної системи підприємства ТОВ "Intellias".

# **ПЕРЕЛІК ПОСИЛАНЬ**

1. Глоба Л.С. Розробка інформаційних ресурсів та систем: підручник. Київ: Політехніка, 2013. 380 с.
2. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с
3. Технології захисту інформації. Лекція 4. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>. (дата звернення: 02.03.2024 р.).
4. Asamba, M. Running head: BEST PRACTICES OF NETWORK SECURITY 1 Best Practices of Network Security Student’s Name Institutional Affiliation BEST PRACTICES OF NETWORK SECURITY 2. Technology 23, 14–23 (2020).
5. Дослідження основних тенденцій сучасної розробки вебсайтів / А. М. Десятко, Н. О. Котенко, Т. О. Жирова та ін. // Кібербезпека: освіта, наука, техніка = Cybersecurity: Education, Science, Technique. Київський університет ім. Бориса Грінченка. 2019. С.
6. Сучасні технології тестування та захисту веб-сторінок / М. І. Цюцюра, О. В. Криворучко, Т. О. Жирова та ін. // Управління розвитком складних систем. Випуск № 39, 2019. С. 100–10
7. Аналіз стану захищеності інформаційно-телекомунікаційних систем / О. В. Криворучко, О. М. Сунічук, Д. В. Швець та ін. // Управління розвитком складних систем. 2020. № 42. С. 56–62; dx.doi.org\10.32347/2412-9933.2020.42.56-62.
8. Trofymenko, O.H., Dubovoy, Ya.V. (2018) Concerning the legal capacity of cyberspace safe operation. Cybersecurity in Ukraine: legal and organizational issues: materials of the III AllUkrainian scientific-practical conference (November 30, 2018). Odessa. pp. 5–7.
9. European Cybersecurity Implementation: Overview – ISACA (2014). Retrieved from: <https://informationsecurity.report/Resources/Whitepapers/3251dc92-c468-4f99-bd2bc4203ce81af3_European-Cybersecurity-Implementation-Overview_res_Eng_0814.pdf> (дата звернення: 02.03.2024 р.).
10. Tereikovskyi I. A., Chernyshev D. O., Tereikovska L. A., Mussiraliyeva S. Z. and Akhmed G. Z., 2018. The procedure for the determination of structural parameters of a convolutional neural network to fingerprint recognition. Journal of Theoretical and Applied Information Technology, vol. 97, no. 8, pp. 2381–2392.
11. Tereikovskyi I., Mussiraliyeva S., Kosyuk Y., Bolatbek M. and Tereikovska L., 2018. An experimental investigation of infrasound influence hard drives of a computer system. International Journal of Civil Engineering and Technology, vol. 9, no. 6, pp. 1558–1566.
12. Tereikovskiy I., Parkhomenko I., Toliupa S. and Tereikovska L., 2018. Markov model of normal conduct template of computer systems network objects. In: 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 20–24 Feb. 2018. Slavske, pp. 498–501.
13. Олещук О. В., Попель О. Є., Копитчук М. Б. Моделювання повнозв’язної нейронної мережі з використанням технології CUDA // Вісник Національного університету «Львівська політехніка». 2012. № 747. С. 131–139.
14. Бакін Д.С. Проблеми захисту інформації в комп’ютерних мережах: матеріали всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С. 79-80. URL: http://dspace.kntu.kr.ua/jspui/ bitstream/123456789/5101/1/AUConferenceCyberSecurity\_November2016\_p79.pdf
15. Jozef Janitor, Karol Kniewald. Visual Learning Tools for Teaching / Learning Computer Networks: Sixth International Conference on Networking and Services, 2010. Р. 351-355.
16. Maximum Security: A Hacker’s Guide to Protecting Your Internet Site and Network. URL: http://index-of.es/EBooks/German/Hacking/maximum\_security.pdf.
17. Болехівський Н. Полотай О. Класифікація мережевих атак та методи протидії і ззахисту. URL: https://sci.ldubgd.edu.ua/bitstream/handle/123456789/6737/ 1.pdf?sequence=1&isAllowed=y (дата звернення: 15.03.2024 р.).
18. Cisco. URL: https://www.cisco.com/c/en/us/index.html (дата звернення: 10.04.2024 р.).
19. Cisco Systems, Inc. The Zone-Based Policy Firewall Design URL: [http://www.cisco.com/en/US/product s/sw/secursw/ps1018/products\_tech\_note09186a0](http://www.cisco.com/en/US/product%20s/sw/secursw/ps1018/products_tech_note09186a0) [0808bc994.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml) (дата звернення: 10.04.2023 р.).
20. Cisco Systems, Inc. Cisco Secure Access Control Server for Windows: ReleaseNotes. URL: [http://www.cisco.com/en/US/produ cts/sw/secursw/ps2086/prod\_ release\_notes\_list.html](http://www.cisco.com/en/US/produ%20cts/sw/secursw/ps2086/prod_%20release_notes_list.html) (дата звернення: 10.04.2024 р.).
21. Campus LAN and Vireless LAN Solution Design Design Good [Електронний ресурс], Режим доступу: URL: – [https://www.cisco.com/c/en/us/td /docs/solutions/CVD/Campus/cisco-campus-lan-wlan-](https://www.cisco.com/c/en/us/td%20/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-) [design-guide.html](https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html) (дата звернення: 11.04.2024 р.).
22. Cisco Systems, Inc. Cisco Router and Security Device Manager 2.4 User’s Guide. URL: [http://www.cisco.com/en/US/product s/sw/secursw/p s5318/products\_user\_guide\_list.ht](http://www.cisco.com/en/US/product%20s/sw/secursw/p%20s5318/products_user_guide_list.ht)[ml](http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_list.html) (дата звернення: 14.04.2024 р.).
23. Cisco Systems, Nz. The Zone-Based Shelves Firewall Design Signe Gude. URL: [http://vvv.cisco.chom/en/US/produtsss/sv /setsursv/ps1018/produtsss\_te ch\_note09186a0](http://vvv.cisco.chom/en/US/produtsss/sv%20/setsursv/ps1018/produtsss_te%20ch_note09186a0) [0808b994.shtml](http://vvv.cisco.chom/en/US/produtsss/sv/setsursv/ps1018/produtsss_tech_note09186a00808b994.shtml) (дата звернення: 22.04.2024 р.).

# **ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**