НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Оцінка захищеності інформаційної системи

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-93
Жембровська Олена Сергіївна _____
(підпис)

Керівник: к. ек. н., доцент каф. ІБ ФТІ Ткач Володимир Миколайович _____
(підпис)

Рецензент доцент кафедри ММАД ФТІ Южакова Ганна Олексіївна _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2023 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Жембровська Олена Сергіївна
(прізвище, ім’я, по батькові)

1. Тема роботи Оцінка захищеності інформаційної системи,
керівник роботи Ткач Володимир Миколайович, кандидат економічних наук, доцент кафедри інформаційної безпеки,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «26» травня 2023 р. №2028-с

2. Термін подання здобувачем вищої освіти роботи 11 червня 2023 р.

3. Вихідні дані до роботи: роботи пов'язані з тематикою.

4. Зміст роботи: ознайомитися з існуючими методми оцінювання захищеності інформаційної системи, видлити найважливіші критерії для методів оцінювання, порівняти вибрані методи оцінювання, описати власну модель оцінювання.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

6. Дата видачі завдання: 25 січня 2023 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вибір теми дипломної роботи	02.01.2023 - 24.01.2023	виконано
2	Отримання завдання	25.01.2023	виконано
3	Пошук необхідної інформації в інформаційних джерелах	26.01.2023 - 25.02.2023	виконано
4	Робота над першим розділом роботи	26.02.2023 – 15.03.2023	виконано
5	Аналітичний огляд методів оцінювання, вибір найрозповсюдженіших.	16.03.2023 - 10.04.2023	виконано
6	Вибір критеріїв для порівняння методів оцінювання	11.04.2023 - 20.04.2023	виконано
7	Порівняння методів оцінювання за вибраними критеріями	21.04.2023 – 01.05.2023	виконано
8	Оформлення другого та третього розділів	02.05.2023 – 20.05.2023	виконано
9	Опис власного методу оцінювання захищеності інформаційної системи	20.05.2023 – 05.06.2023	виконано
10	Оформлення четверторо розділу	05.06.2023 – 10.06.2023	виконано

Здобувач вищої освіти _____ Олена ЖЕМБРОВСЬКА
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Володимир ТКАЧ
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Обсяг дипломної роботи склаадає 50 сторінок. Дипломна робота містить 3 рисунки, 2 таблиці, та 9 джерел посилань.

З розвитком технологій – збільшуєьться потреба в різного роду інформаційних системах, а разом з цим зростає і необхідність їх захищати. Тому оцінка захищеності інформаційної системи є запорукою належного функціонування будь-якого процесу пов’язаного з інформацією.

У даному дослідженні були визначені основні аспекти побудови методу оцінювання захищеності інформаційних систем (ІС). Вони включають етапи, причини та критерії оцінки захищеності. Додатково, розглянуті найпопулярніші фреймворки для оцінки захищеності ІС, які сприяють стандартизації та систематизації процесу оцінки, а також надають цінні рекомендації для поліпшення безпеки системи.

Також у роботі були описані найвідоміші методики, моделі та методи оцінювання захищеності інформаційної системи, і проведено їх аналіз згідно з вищезазначеними критеріями. Це дозволило встановити відповідність цих підходів до вимог оцінки захищеності.

Крім того, у роботі було описано метод оцінювання захищеності ІС, що базується на ідеї піраміди Маслоу. Цей метод дозволяє спеціалістам з кібербезпеки ефективно організовувати роботу з покращення інформаційних системам.

Ключові слова: інформаційна система, оцінка захищеності, критерії, піраміда Маслоу.

ABSTRACT

The volume of the thesis is 50 pages. The thesis contains 3 figures, 2 tables, and 9 references.

With the development of technology, the need for various types of information systems increases, and with it the need to protect them increases. Therefore, assessing the security of an information system is a prerequisite for the proper functioning of any information-related process.

This study identified the main aspects of building a method for assessing the security of information systems (IS). They include stages, reasons and criteria for assessing security. In addition, the most popular frameworks for assessing IS security are considered, which contribute to the standardization and systematization of the assessment process, as well as provide valuable recommendations for improving system security.

The paper also describes the most well-known techniques, models and methods for assessing the security of an information system and analyzes them according to the above criteria. This made it possible to establish the compliance of these approaches with the requirements of security assessment.

In addition, the paper describes a method for assessing the security of an IS based on the idea of Maslow's pyramid. This method allows cybersecurity professionals to effectively organize work to improve information systems.

Keywords: information system, security assessment, criteria, Maslow's pyramid.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 7
ВСТУП 8
1 АНАЛІЗ ДЖЕРЕЛ ІНФОРМАЦІЇ 11
1.1 Причини оцінювання захищеності ІС 11
1.2 Етапи дослідження захищеності інформаційної системи 13
1.3 Критерії при оцінці захищеності інформаційної системи 16
Висновки до розділу 1 19
2 ФРЕЙМВОРКИ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ 20
2.1 NIST Cybersecurity Framework 21
2.2 Open Source Cybersecurity Assessment and Validation Environment 24
Висновки до розділу 2 25
3 МЕТОДИ І МОДЕЛІ 27
3.1 Методика оцінки захищеності інформаційних систем 27
3.2 Operational Cybersecurity Assessment for Vulnerability Elimination 30
3.3 Security maturity model 32
3.4 Threat and Risk Assessment 36
3.5 Стандарти ISO 37
3.6 Порівняння методів оцінки захищеності інформаційної системи . 41
Висновки до розділу 3 43
4 ОПИС ВЛАСНОГО МЕТОДУ ОЦІНЮВАННЯ 44
Висновки до розділу 4 47
ВИСНОВКИ 49
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 50

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІС - інформаційна система

OSCAVE - Open Source Cybersecurity Assessment and Validation Environment

SMM - Security maturity model

TRA - Threat and Risk Assessment

NIST - National Institute of Standards and Technology

R – ранг

M – число функціональних класів

F_k^j – ваговий коефіцієнт к-сімейству j-класу

w_k – вагова функція к-сімейству

C_j – ваговий коефіцієнт важливості j-го класу

w_{kj} – підсумковий показник по всім сімействам j-го класу

ВСТУП

Актуальність роботи

Актуальність дипломної роботи полягає у необхідності забезпечення надійності та безпеки інформаційних систем у сучасному цифровому середовищі. Зростання кількості кібератак, витоків даних та інших загроз інформаційній безпеці ставить під загрозу конфіденційність, цілісність та доступність даних. Це має серйозні наслідки для організацій, урядових структур та інших суб'єктів, що працюють зі значною кількістю чутливої інформації.

Оцінка захищеності інформаційної системи стає критично важливою для виявлення потенційних слабких місць інформаційної безпеки та розроблення ефективних стратегій захисту. Така оцінка дозволяє виявити ризики та вразливості, пов'язані з конфігурацією системи, аутентифікацією, авторизацією, шифруванням даних, мережевою безпекою та іншими аспектами інформаційної безпеки.

Дослідження в галузі оцінки захищеності інформаційної системи допомагають виявляти нові загрози, розробляти ефективні технології та методи захисту, а також оцінювати ефективність існуючих заходів безпеки. У зв'язку зі стрімким розвитком технологій та постійними змінами загроз, ця тема дипломної роботи є актуальною і важливою для забезпечення інформаційної безпеки організацій та інших суб'єктів.

Об’єкт дослідження

Об’єктом дослідження в даній роботі виступають інформаційні системи. Вони можуть бути як простими, там і складними і багаторівневими.

Предмет дослідження

Предметом дослідження є методи оцінки захищеності інформаційної системи.

Метою роботи

Нашою метою є аналіз та порівняння різних методів, їх переваг та недоліків, ефективності та застосування у контексті оцінки захищеності інформаційних систем. Аналітичний огляд, а також порівняння вибраних нами методів оцінки інформаційної системи за критеріями які ми виділили в ході роботи.

Методи дослідження

В цій роботі використовувалися такі методи дослідження: літературний аналіз, аналітичний огляд, експертні оцінки, статистичний аналіз.

Наукова новизна одержаних результатів

В нашій роботі ми виділили перелік найважливіших і найбільш вагомих критеріїв за якими проаналізували різні методи оцінки захищеності інформаційної системи, а також розробка власного методу заснованому на ідеї ієрархічності піраміди Маслоу.

Практичне значення одержаних результатів

В ході роботи ми порівняли різні методи оцінки захищеності інформаційної системи, що є практично важливим для визначення найкращих практик, розробки плану дій для покращення безпеки інформаційних систем та забезпечення відповідності вимогам безпеки. Також дана робота є основою для вдосконалення вже існуючих методів, та створення нових. А створений нами метод стає в перелік можливих для використання спеціалістами з кібербезпеки.

Апробація результатів роботи

Робота була представлена на Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS - 2023) (26 травня 2023, м. Київ)

1 АНАЛІЗ ДЖЕРЕЛ ІНФОРМАЦІЇ

Оцінка захищеності інформаційної системи - це процес визначення рівня безпеки інформаційної системи шляхом перевірки відповідності стандартам, ідентифікації потенційних вразливостей, оцінки ризиків та загроз, а також визначення ефективності застосовуваних заходів безпеки.

Оцінка захищеності інформаційної системи допомагає визначити, наскільки добре інформаційна система захищена від несанкціонованого доступу, втрати даних, порушення конфіденційності, цілісності та доступності інформації. Це важливий етап у процесі управління та розробки інформаційних систем.

1.1 Причини оцінювання захищеності ІС

Оцінка захищеності ІС є надзвичайно важливою задачею, оскільки забезпечення безпеки інформації є критичним аспектом для будь-якої організації чи підприємства. Інформаційні системи використовуються в різних сферах діяльності, таких як бізнес, урядові установи, освіта, наука, медицина та багато інших.

В ході роботи було виділено основні причини, чому оцінка захищеності інформаційної системи є важливою:

1. **Виявлення вразливостей**: Оцінка захищеності дозволяє ідентифікувати потенційні вразливості в інформаційній системі, такі як слабкі місця в програмному забезпеченні, недостатня конфігурація системи або вразливості мережевої інфраструктури. Це допомагає

виявити проблеми, які можуть бути використані зловмисниками для несанкціонованого доступу до системи або викрадення інформації.

2. **Захист від кібератак**: Оцінка захищеності допомагає виявити потенційні загрози та ризики, пов'язані з кібератаками. Це дозволяє прийняти необхідні заходи забезпечення безпеки, такі як налаштування фаєрволів, використання криптографічних методів або розробку стратегій реагування на інциденти.

3. **Захист конфіденційної інформації**: Оцінка захищеності допомагає визначити рівень захисту конфіденційної інформації, що зберігається в системі. Вона включає оцінку системи автентифікації, контролю доступу, шифрування даних та заходів щодо запобігання несанкціонованому доступу до інформації.

4. **Забезпечення неперервності процесу**: Оцінка захищеності інформаційної системи допомагає ідентифікувати проблемні місця, які можуть призвести до винекнення форс-мажорних ситуацій, що в свою чергу призводять до переривання процесу роботи.

5. **Виконання регуляторних вимог**: Багато галузей, таких як фінанси, охорона здоров'я та наукові дослідження, мають специфічні регуляторні вимоги щодо захисту інформації. Оцінка захищеності допомагає перевірити відповідність системи цим вимогам і прийняти необхідні заходи для виконання правил і стандартів.

6. **Захист репутації та довіри**: Уразливість або порушення безпеки може призвести до витоку чутливої інформації, пошкодити репутацію організації або спричинити фінансові втрати. Оцінка захищеності допомагає виявити потенційні ризики та прийняти заходи для їх

запобігання, що сприяє збереженню довіри клієнтів, партнерів і громадськості.

7. **Планування ресурсів і бюджетування**: Оцінка захищеності дозволяє оцінити потреби в ресурсах, які необхідні для забезпечення безпеки інформаційної системи. Це допомагає планувати витрати на обладнання, програмне забезпечення, навчання персоналу та інші аспекти, пов'язані з безпекою, для забезпечення ефективного бюджетування.

8. **Вимоги від клієнтів та партнерів**: Багато організацій повинні дотримуватися вимог щодо захисту інформації, встановлених їх клієнтами або партнерами. Оцінка захищеності допомагає переконатися, що організація відповідає цим вимогам і забезпечує належний рівень захисту для співпраці та партнерства.

Розуміння причин оцінювання захищеності допомагає організаціям та фахівцям з інформаційної безпеки усвідомити важливість і необхідність захищати інформаційні системи. Це стимулює розробку та впровадження ефективних заходів безпеки.

1.2 Етапи дослідження захищеності інформаційної системи

Виділення етапів роботи дозволяє належним чином спланувати процес оцінки захищеності ІС. Це включає визначення потрібних ресурсів, учасників проекту, встановлення мети та об'єктивів оцінки, а також розробку плану дій. Оцінка захищеності інформаційної системи включає такі етапи:

Дослідження захищеності системи можна розділити на кілька етапів, наприклад:

1. **Оцінка загальної конфігурації системи**: на цьому етапі необхідно виявити основні компоненти системи, що містять критичні дані, та оцінити рівень їх захисту.

2. **Виявлення потенційних вразливостей**: на цьому етапі необхідно виявити потенційні вразливості системи, які можуть бути використані зловмисниками для злому системи.

3. **Аналіз відповідності системи стандартам безпеки**: на цьому етапі необхідно оцінити відповідність системи стандартам безпеки, наприклад, ISO 27001, NIST, або іншим.

4. **Проведення тестування на проникнення**: на цьому етапі необхідно спробувати проникнути в систему, використовуючи різні методи атак.

5. **Оцінка ризиків**: Визначення ризиків, пов'язаних з виявленими вразливостями, та оцінка їх потенційного впливу на інформаційну систему та бізнес-процеси.

6. **Оцінка реалізованого захисту**: на цьому етапі необхідно оцінити ефективність реалізованого захисту, наприклад, ефективність захисту мережі, ефективність захисту від зловмисних програм тощо.

7. **Розробка плану покращення захисту**: на цьому етапі необхідно розробити план покращення захисту, який включає в себе рекомендації щодо покращення захисту системи, а також опис можливих ризиків та проблем, які можуть виникнути у разі недостатнього рівня захисту.

Кожен з цих етапів є важливим для виявлення слабких місць у системі та розробці плану покращення захисту. Однак, важливо враховувати, що ці етапи можуть бути дуже складними та вимагати значних зусиль, тому їх виконання потребує професійної.

Також важливим моментом є те, що при оцінці захищеності ми враховуємо багато критеріїв і в тому числі оцінку ризиків. Зауважуємо на цьому, бо багато вже існуючих робіт в цій сфері зводять оцінку захищеності інформаційної системи, до оцінки ризиків, хоча це дві кардинально різні методики.

Оцінка ризиків і оцінка захищеності є двома різними аспектами оцінки в галузі кібербезпеки. Ось декілька ключових відмінностей між ними:

1. **Об'єкти оцінки**: Оцінка ризиків спрямована на виявлення потенційних загроз і визначення ризиків, пов'язаних з інформаційною системою. Вона оцінює ймовірність виникнення загроз та потенційні наслідки для системи та організації. З іншого боку, оцінка захищеності зосереджена на оцінці поточного стану захисту інформаційної системи, включаючи ідентифікацію слабких місць, вразливостей та недоліків у заходах безпеки.

2. **Цілі оцінки**: Оцінка ризиків має на меті визначити ризики і прийняти рішення щодо управління ними. Вона допомагає визначити пріоритети і визначити заходи з управління ризиками, такі як прийняття заходів з усунення ризиків, передача ризиків, зменшення ризиків або прийняття ризиків. Оцінка захищеності спрямована на виявлення потреб у покращенні захисту інформаційної системи. Вона надає уявлення про поточні недоліки та встановлює основи для розробки та реалізації політик, процедур та заходів безпеки.

3. **Підхід**: Оцінка ризиків зазвичай базується на ідентифікації загроз, оцінці їх впливу та імовірності виникнення, а також оцінці наслідків. Вона може використовувати кількісні або якісні методи для калькуляції ризиків. Оцінка захищеності, зі свого боку, зазвичай проводиться шляхом аналізу технічних, організаційних та процесних заходів безпеки, щоб визначити їх ефективність та встановити пропозиції щодо поліпшення.

4. **Часовий фрейм**: Оцінка ризиків зазвичай є процесом, який проводиться на постійній основі, оскільки ризики можуть змінюватися з часом через нові загрози або зміни у контексті. Оцінка захищеності може бути проведена на початковому етапі, щоб визначити поточний стан захисту, а також наступні етапи для контролю і поліпшення.

Враховуючи ці відмінності, оцінка ризиків та оцінка захищеності є взаємодоповнюючими процесами, які допомагають забезпечити ефективне управління кібербезпекою в організації.

Оцінка захищеності інформаційної системи допомагає організаціям зрозуміти їхні потреби в безпеці, виявити слабкі місця та прийняти відповідні заходи для покращення безпеки та запобігання інцидентам інформаційної безпеки.

1.3 Критерії при оцінці захищеності інформаційної системи

Оцінювання захищеності системи залежить від різних критеріїв, які враховують різні аспекти безпеки. Найбільш важливими критеріями для оцінки інформаційної системи вважають ті, що описані в трикутнику CIA,

який є концептуальною моделлю, що використовується для опису ключових аспектів інформаційної безпеки. Він визначає три основні складові, які мають бути для забезпечення безпеки інформації. CIA це абревіатура цих аспектів: Confidentiality - конфіденційність, Integrity - цілісність, Availability - доступність.

Рисунок 1.1 – Трикутник CIA

Проаналізувавши більше джерел інформації для розробки свого методу оцінювання було виділено ще декілька критеріїв. Ці основні положення є необхідними для забезпечення високого рівня захищеності інформаційної системи.

1. **Конфіденційність**: цей критерій вимірює рівень захищеності даних та інформації від несанкціонованого доступу.

2. **Цілісність**: цей критерій вимірює рівень захищеності даних та інформації від неправомірних змін або втручань.

3. **Доступність**: цей критерій вимірює рівень доступності системи та її функціональності в умовах атак або інших негативних впливів.

4. **Автентифікація**: цей критерій вимірює рівень захищеності системи від несанкціонованого доступу шляхом перевірки ідентифікації користувача.

5. **Авторизація**: цей критерій вимірює рівень захищеності системи від несанкціонованого доступу до ресурсів та функцій.

6. **Надійність**: цей критерій вимірює рівень захищеності системи від непередбачуваних помилок та збоїв. В цьому критерії варто також враховувати відмовостійкість - здатність інформаційної системи функціонувати безперебійно навіть при виникненні помилок, відмов апаратного і програмного забезпечення, атак або інших небезпечних ситуацій. Вона включає механізми резервування, резервне копіювання даних.

7. **Відновлюваність**: цей критерій вимірює рівень захищеності системи від негативних впливів та її здатність до відновлення та відновлення даних після непередбачуваних подій.

8. **Спостережуваність**: визначає, наскільки легко можна отримати інформацію про стан системи за допомогою доступних спостережень або вимірювань.

Проте застосування цих критеріїв в системі повинно бути проаналізоване з точки зору її потреб та вимог до безпеки. Також, варто врахувати специфіку конкретної системи та її інфраструктури, щоб визначити, які заходи безпеки найбільш доцільно застосовувати.

Висновки до розділу 1

В цьому розділі ми ознайомилися з основними моментами в побудові методу оцінювання захищеності ІС, як етапи, причини та критерії.

Оцінка захищеності інформаційних систем має велике значення з кількох причин. Вона допомагає виявити вразливості, захистити систему від кібератак, зберегти конфіденційну інформацію, забезпечити неперервність процесу, виконати регуляторні вимоги, зберегти репутацію та довіру, планувати ресурси та бюджетування, а також відповідати вимогам клієнтів та партнерів.

Розуміння етапів роботи при оцінці захищеності дозволяє належно спланувати та провести процес оцінки безпеки інформаційних систем. Це включає планування, аналіз, виявлення вразливостей, розробку заходів безпеки та оцінку відповідності регуляторним вимогам.

1 ФРЕЙМВОРКИ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ

Фреймворки для оцінки захищеності інформаційних систем мають декілька важливих цілей і призначень:

Фреймворки встановлюють стандарти та рекомендації щодо оцінки захищеності інформаційних систем. Вони надають загальний набір принципів, методів та процедур, які допомагають оцінити рівень захищеності системи і визначити недоліки.

Фреймворки надають набір критеріїв, за допомогою яких можна оцінити рівень захищеності інформаційних систем. Ці критерії враховують різні аспекти безпеки, такі як фізична безпека, технічна безпека, соціальна безпека, процеси управління ризиками тощо.

Фреймворки допомагають систематично підходити до оцінки захищеності інформаційних систем. Вони надають методики, процедури та інструменти для збору необхідної інформації, аналізу ризиків, визначення пріоритетів та формування рекомендацій щодо підвищення захисту.

Фреймворки допомагають виявити недоліки в захисті інформаційних систем і визначити слабкі місця. Вони допомагають ідентифікувати потенційні загрози, вразливості та ризики, що можуть вплинути на безпеку системи.

Фреймворки надають рекомендації та керівні принципи щодо підвищення рівня захищеності інформаційних систем. Вони допомагають ідентифікувати пріоритетні області для вдосконалення та визначають набір кроків і заходів, які можна вжити для зменшення ризиків.

2.1 NIST Cybersecurity Framework

Національний інститут стандартів і технологій (NIST) є агентством Сполучених Штатів, яке розробляє стандарти та рекомендації щодо кібербезпеки. Один з найбільш відомих продуктів NIST в цій сфері - Цифровий фреймворк кібербезпеки NIST (NIST Cybersecurity Framework).

NIST Cybersecurity Framework є розширеним підходом до керування кібербезпекою, призначеним для підприємств, урядових установ та інших організацій. Він пропонує методику для розуміння, оцінки та зменшення ризиків кібербезпеки шляхом визначення і застосування ефективних заходів забезпечення безпеки.

Основні складові NIST Cybersecurity Framework:

1. Керівництво (Framework Core): Це набір керівних принципів, керівних заходів та практик, які сприяють зміцненню кібербезпеки. Він включає п'ять фундаментальних елементів:
    - Identify (Визначення): Виявлення та ідентифікація активів, вразливостей та загроз.
    - Protect (Захист): Розробка та реалізація заходів захисту для запобігання атакам та вразливостям.
    - Detect (Виявлення): Виявлення кіберінцидентів та швидка реакція на них.
    - Respond (Реагування): Швидке реагування та відновлення після кіберінцидентів.
    - Recover (Відновлення): Відновлення нормального функціонування та попередження майбутніх інцидентів.

2. Розробка процесів (Framework Profile): Організації можуть створювати "профілі" фреймворку, встановлюючи власні цілі та рекомендації забезпечення безпеки, які відповідають їх потребам та ризикам. Це дозволяє визначати пріоритети та пристосовувати заходи безпеки до конкретної ситуації.
3. Оцінка (Framework Implementation Tiers): Цей елемент визначає рівень зрілості організації в галузі кібербезпеки. Він включає чотири рівні:
    - Partial (Частковий): Організація виконує лише базові заходи безпеки.
    - Risk Informed (Інформований ризиком): Організація має процеси управління ризиками та ефективні заходи безпеки.
    - Repeatable (Повторюваний): Організація виконує систематичні процеси та заходи безпеки.
    - Adaptive (Адаптивний): Організація виявляється, аналізує та адаптує свої заходи безпеки.

NIST Cybersecurity Framework надає організаціям гнучкість у визначенні та виконанні заходів безпеки залежно від їх потреб. Він сприяє покращенню кібербезпеки, зниженню ризиків та підвищенню здатності реагувати на кібератаки.

NIST Cybersecurity Framework є корисним для оцінки захищеності інформаційної системи з кількох причин:

1. **Стандарти та рекомендації**: Фреймворк надає широкий набір стандартів та рекомендацій, які допомагають організаціям визначити ефективні заходи безпеки. Він заснований на кращих практиках та галузевих стандартах, розроблених експертами в галузі кібербезпеки.

2. **Гнучкість**: Фреймворк дозволяє організаціям адаптувати його до своїх потреб. Вони можуть створювати власні профілі, встановлюючи цілі та рекомендації забезпечення безпеки, що відповідають їх контексту та ризикам. Це дозволяє зосередитися на конкретних аспектах захищеності інформаційної системи.

3. **Ідентифікація ризиків**: Фреймворк допомагає організаціям ідентифікувати потенційні загрози та вразливості своєї інформаційної системи. Це включає процеси визначення та класифікації активів, оцінку ризиків і визначення пріоритетів для впровадження заходів безпеки.

4. **Цикл управління**: Фреймворк надає цикл управління кібербезпекою, який включає визначення, захист, виявлення, реагування та відновлення. Це допомагає організаціям планувати, впроваджувати та покращувати свої заходи безпеки відповідно до змінюючихся загроз та вимог.

5. **Загальноприйнятість**: NIST Cybersecurity Framework став широко визнаним і використовується як референсний пункт у галузі кібербезпеки. Багато організацій, включаючи урядові установи, використовують цей фреймворк як основу для оцінки та вдосконалення своєї захищеності.

Загалом, NIST Cybersecurity Framework надає структурований підхід до оцінки та покращення захищеності інформаційних систем. Він допомагає організаціям ідентифікувати ризики, встановлювати ефективні заходи безпеки та розробляти стратегії управління кібербезпекою.

2.2 Open Source Cybersecurity Assessment and Validation Environment

OSCAVE - це відкрите програмне забезпечення для автоматизованої оцінки та перевірки захищеності інформаційно-комунікаційних систем (ІКС).

Основна мета OSCAVE - допомогти організаціям здійснювати автоматизовану перевірку безпеки своїх інформаційних систем та інфраструктури, що використовується для забезпечення захисту цих систем. OSCAVE складається з набору інструментів та методологій, які дозволяють виявити потенційні вразливості системи та забезпечити захист від можливих загроз.

OSCAVE має такі основні функції:

1. **Автоматизована перевірка захищеності системи**: OSCAVE дозволяє проводити автоматизовану перевірку захищеності системи з використанням різних методологій та інструментів. Це дозволяє виявити потенційні вразливості та інші загрози для системи.
2. **Підтримка стандартів безпеки**: OSCAVE забезпечує підтримку різних стандартів безпеки, таких як ISO 27001, NIST та інших. Це дозволяє використовувати OSCAVE для оцінки відповідності системи вимогам стандартів безпеки.
3. **Аналіз результатів**: OSCAVE дозволяє аналізувати результати перевірки захищеності системи та створювати звіти з рекомендаціями щодо забезпечення захисту від можливих загроз.

4. **Інтеграція з іншими інструментами**: OSCAVE може бути інтегрований з іншими інструментами, такими як системи моніторингу, системи логування та інші. Це дозволяє забезпечити комплексний підхід до захисту системи.

5. **Відкрите програмне забезпечення**: OSCAVE є відкритим програмним забезпеченням, що дозволяє розробникам, експертам з безпеки та користувачам вносити свої внески в проект, вносити покращення та доповнення, що робить його дуже гнучким та адаптованим до різних потреб та вимог користувачів.

У загальному, використання OSCAVE дозволяє забезпечити високий рівень захищеності ІКС та знизити ризики їхньої критичності. Крім того, використання цієї платформи дозволяє забезпечити відповідність ІКС стандартам безпеки та регуляторним вимогам.

Одним з недоліків OSCAVE є складність його налаштування та використання. Для того, щоб дійсно використовувати цю платформу для оцінки захищеності системи, потрібно мати відповідний досвід та знання з області кібербезпеки. Також, OSCAVE не є універсальним рішенням і може не підходити для оцінки захищеності деяких систем, особливо тих, які використовують нестандартні архітектури та технології.

Висновки до розділу 2

Загалом, фреймворки для оцінки захищеності інформаційних систем допомагають стандартизувати та систематизувати процес оцінки, а також надають цінні рекомендації для покращення безпеки системи. Вони є

корисними інструментами для організацій, що прагнуть забезпечити високий рівень захищеності своїх інформаційних ресурсів.

3 МЕТОДИ І МОДЕЛІ

3.1 Методика оцінки захищеності інформаційних систем

В 2021 році С.В. Батечко, О.Ю. Лебедєва, В.В. Зоріло описали свою методику для оцінки захищеності інформаційних систем. Вона була основана на стандарті ISO 15408. І складається ця методика з наступних етапів:

1. Визначення класів: Визначаються класи, які будуть брати участь у процесі оцінки захищеності інформаційних систем.

   Вагові коефіцієнти C_i для кожного і-го класу безпеки розраховуються за такою формулою:

$$C_i = 1 - \frac{R_i - 1}{M} \tag{3.1}$$

2. Ранжування класів та розрахунок вагових коефіцієнтів: Класи ранжуються за важливістю, а потім обчислюються вагові коефіцієнти для кожного класу.

   Для нормування коефіцієнтів використовується наступна формула:

$$C_k = \frac{C_i}{\sum_{i=1}^{M} C_i}. \tag{3.2}$$

де R – ранг, а M – число функціональних класів.

3. Ранжування сімейств кожного класу та розрахунок вагових коефіцієнтів сімейств: Для кожного класу ранжуються сімейства, що входять до нього, і обчислюються вагові коефіцієнти для кожного сімейства.

Ранжування сімейств класів та обчислення вагового коефіцієнту для кожного сімейства здійснюється з використанням наступних формул:

$$F_i = 1 - \frac{R_i - 1}{M}. \tag{3.3}$$

$$F_k = \frac{F_i}{\sum_{i=1}^{M} F_i}. \tag{3.4}$$

4. Відмітка про виконання дій: Проводиться відмітка про виконання дій, зазначених у компонентах кожного сімейства для класів, що беруть участь в оцінці.

5. Формування матриці вагової функції: Створюється матриця вагової функції на основі відміток про виконання.

На етапі анкетування, експерт проставляє значення вагової функції для кожного компонента, яка має три різні поведінки: "-1" - якщо компонент не виконано, "0" - якщо він не використовується, і "1" - якщо компонент виконано.

Ці значення заносяться до вагової функції для кожного сімейства. В результаті анкетування компонентів кожного сімейства обчислюється оцінка для цього сімейства.

$$W_{kj} = \sum_{k=1}^{n} F_k^j w_k \ , \tag{3.5}$$

Де F_k^j – ваговий коефіцієнт к-сімейству j-класу;

w_k – вагова функція к-сімейству

6. Розрахунок залежностей: Якщо стандарт передбачає залежності між компонентами сімейств, розраховуються відповідні залежності для кожної компоненти сімейства.

7. Розрахунок узагальнюючих показників: Обчислюються узагальнені показники для кожного класу на основі вагових коефіцієнтів і відміток про виконання.

$$X_j = \sum_{k=1}^{n} C_j w_{kj} \ , \tag{3.6}$$

де C_j – ваговий коефіцієнт важливості j-го класу;

w_{kj} – підсумковий показник по всім сімействам j-го класу

8. Розрахунок підсумкової оцінки: Проводиться розрахунок підсумкової оцінки захищеності інформаційної системи.

$$Y = \sum_{j} X_j \tag{3.7}$$

9. Розрахунок залежностей, узагальнених показників та підсумкової оцінки для класів з усіма позитивними відмітками: Здійснюється розрахунок залежностей, узагальнених показників та підсумкової оцінки для класів, якщо всі компоненти сімейств мають позитивні відмітки про виконання дій.

10. Порівняння результатів та формування рекомендацій: Порівнюються результати, отримані в пункті 8 та 9, і формуються рекомендації щодо підвищення захищеності оцінювання інформаційної системи.

Ці кроки допомагають оцінити захищеність інформаційної системи та надають основу для розробки рекомендацій з покращення безпеки.

Проте, так як, ця методика була розроблена на основі стандарту ISO 15408, вона має такі самі недоліки і перевоги, тому в подальшому аналізі ми оцінюємо саме стандарт ISO 15408.

3.2 Operational Cybersecurity Assessment for Vulnerability Elimination

Operational Cybersecurity Assessment for Vulnerability Elimination (Операційна оцінка кібербезпеки для усунення вразливостей) - це підхід до оцінки та усунення вразливостей в інформаційних системах з метою забезпечення їхньої безпеки. Цей процес дозволяє виявляти ідентифікувати потенційні слабкі місця в системі, а також визначати та впроваджувати заходи для усунення цих вразливостей.

Детальний процес Operational Cybersecurity Assessment for Vulnerability Elimination може включати наступні етапи:

1. **Інвентаризація активів**: Цей етап передбачає ідентифікацію та класифікацію всіх активів інформаційної системи, таких як сервери, мережеві пристрої, додатки, дані тощо. Це допомагає усвідомити обсяг та склад системи, які підлягають оцінці.

2. **Виявлення вразливостей**: На цьому етапі проводять сканування та аналіз інформаційної системи з використанням спеціальних інструментів, які допомагають виявити потенційні вразливості. Це можуть бути слабкі паролі, застарілі програмні компоненти, недостатні налаштування безпеки тощо.

3. **Оцінка ризиків**: На основі виявлених вразливостей проводиться оцінка ризиків. Це включає аналіз потенційного впливу вразливостей на безпеку системи та оцінку ймовірності їхньої експлуатації з боку зловмисників. Результатом є визначення пріоритету вразливостей та ризикових областей, які вимагають найбільшої уваги.

4. **Розробка заходів безпеки**: На цьому етапі розробляються та визначаються конкретні заходи для усунення виявлених вразливостей. Це можуть бути технічні заходи, такі як оновлення програмного забезпечення, встановлення патчів, зміна конфігурацій тощо, або організаційні заходи, такі як підвищення свідомості користувачів, зміна політик безпеки тощо.

5. **Впровадження та тестування**: Розроблені заходи безпеки впроваджуються в інформаційну систему. Після впровадження проводиться тестування ефективності цих заходів для перевірки їхньої працездатності та забезпечення відповідності вимогам безпеки.

6. **Моніторинг та підтримка**: Після впровадження заходів безпеки необхідно забезпечувати постійний моніторинг системи для

виявлення нових вразливостей та реагування на змінюючіся загрози. Також важлива регулярна підтримка та оновлення заходів безпеки для забезпечення високого рівня захищеності.

Цей підхід до оцінки та усунення вразливостей допомагає організаціям підвищити безпеку своїх інформаційних систем, знизити ризики кібератак та забезпечити захищеність даних та інфраструктури. Він спрямований на постійне вдосконалення та впровадження заходів безпеки для ефективного управління кібербезпекою.

3.3 Security maturity model

Security maturity model - це модель, яка допомагає компаніям оцінити та покращити рівень зрілості їхньої інформаційної безпеки. Ця модель визначає кілька рівнів зрілості, на яких компанії можуть знаходитися, починаючи від найменш зрілого і закінчуючи найбільш зрілим.

Зазвичай, security maturity model включає 5 рівнів:

1. **Неформальний рівень безпеки**: на цьому рівні, компанії не мають ніяких процедур безпеки та не звертають належної уваги на можливі загрози.

2. **Рівень реакції**: на цьому рівні, компанії мають деякі процедури безпеки, але вони ще не є структурованими. Компанії звертають увагу на загрози лише тоді, коли вони стають очевидними.

3. **Рівень запобігання**: на цьому рівні, компанії починають більш систематично працювати над безпекою та впроваджувати процедури та політики, які спрямовані на запобігання можливим загрозам.

4. **Рівень управління ризиками**: на цьому рівні, компанії вже мають добре структуровані політики безпеки, які дозволяють їм ефективно управляти ризиками та виявляти можливі загрози.

5. **Рівень оптимізації**: на цьому рівні, компанії володіють високим рівнем зрілості безпеки та постійно вдосконалюють свої політики та процедури, щоб забезпечити максимальний рівень захисту.

Security maturity model може бути корисною для компаній, що прагнуть поліпшити своє відношення до інформаційної безпеки. Ця модель може допомогти компаніям визначити, на якому рівні вони знаходяться. Загалом будь-який тип моделі зрілості – це набір практик або процесів, які зображують рівні прогресу на основі можливостей організації. Багато моделей зрілості випливають із пропозицій або вимог відповідності. Модель зрілості безпеки зосереджена на розвитку процесів безпеки та засобів контролю для досягнення ефективної та оптимізованої безпеки.

Модель зрілості безпеки можна використовувати як інструмент для визначення областей, які потребують пріоритетності для вдосконалення, і порівняння прогресу під час шляху організації до створення свого середовища контролю безпеки. Прикладом моделі зрілості безпеки, адаптованої до галузі, є C2M2 (Модель зрілості можливостей кібербезпеки), розроблена Міністерством енергетики США (DoE) та галузевими експертами. C2M2 може використовуватися організаціями в процесі отримання Міністерством оборони (DoD) сертифікації моделі зрілості кібербезпеки (CMMC). Ось додаткові вказівки щодо CMMC.

Хоча можуть існувати різні варіанти моделей зрілості безпеки, що відрізняються певним ступенем деталізації та рівнем оцінки, існують спільні теми та цілі прогресу, які, здається, є в кожній моделі зрілості.

Модель зрілості кібербезпеки (C2M2) дозволяє організаціям оцінити свої можливості кібербезпеки та оптимізувати інвестиції в безпеку. Він використовує набір перевірених галуззю практик кібербезпеки, зосереджених на активах і середовищах як інформаційних технологій (IT), так і операційних технологій (OT). Типовий документ C2M2 версії 2.1 містить ключові концепції та практики C2M2.

Для вимірювання прогресу моделі зрілості зазвичай мають шкалу, що визначає рівні зрілості. C2M2 використовує шкалу рівнів індикатора зрілості (MIL) 0–3. Набір атрибутів визначає кожен рівень. Якщо організація демонструє ці атрибути,
він досяг як цього рівня, так і можливостей, які цей рівень представляє. мати вимірні перехідні стани між рівнями дозволяють організації використовувати шкалу для:

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

Рисунок 3.1 - Підсумок характеристик рівня індикатора зрілості

Характеристики рівня

MIL0 • Практики не виконуються

MIL1 • Початкові вправи виконуються, але можуть бути випадковими

MIL2 Характеристики управління:

• Практики задокументовані

• Для підтримки процесу надаються відповідні ресурси

Характеристика підходу:

• Практики є більш повними або просунутими, ніж на MIL1

MIL3 Характеристики управління**:**

• Діяльність керується політикою (або іншими організаційними директивами)

• Відповідальність, підзвітність і повноваження щодо виконання практик

призначений

• Персонал, який виконує практику, має відповідні навички та знання

• Оцінюється та відстежується ефективність діяльності

Характеристика підходу:

• Практики є більш повними або просунутими, ніж у MIL2

Модель зрілості безпеки є корисним інструментом для оцінки рівня захищеності інформаційної системи. Вона надає рамки та критерії, за допомогою яких можна оцінити і порівняти ефективність заходів забезпечення безпеки в організації.

Ось деякі конкретні переваги використання Security Maturity Model для оцінки захищеності інформаційної системи: оцінка поточного стану,

порівняння з найкращими практиками, створення стратегії безпеки, планування та призначення ресурсів, відстеження прогресу.

3.4 Threat and Risk Assessment

Threat and Risk Assessment (TRA) - це процес оцінки потенційних загроз та ризиків для системи, її інфраструктури та даних. Мета TRA - виявлення можливих загроз та ризиків, що можуть вплинути на систему, та розробка заходів для зменшення цих ризиків.
Процес TRA складається з наступних етапів:

1. Ідентифікація активів: цей етап включає визначення активів, що потребують захисту. Активи можуть включати інфраструктуру, додатки, дані та інші елементи системи.

2. Визначення потенційних загроз: цей етап включає визначення загроз, які можуть спричинити порушення безпеки системи. Загрози можуть включати хакерські атаки, віруси, зловмисники, природні катастрофи та інші.

3. Оцінка вразливостей: цей етап включає визначення вразливостей системи, які можуть бути використані зловмисниками для атаки на систему.

4. Оцінка наслідків: цей етап включає оцінку наслідків порушення безпеки системи. Наслідки можуть включати втрату даних, порушення конфіденційності та цілісності даних, втрату репутації компанії та інші.

5. Оцінка ризиків: цей етап включає оцінку ризиків, пов'язаних з потенційними загрозами та вразливостями системи. Оцінка ризиків дозволяє визначити прийнятний рівень ризику та розробити стратегію зменшення цих ризиків.

6. Розробка плану захисту: цей етап включає розробку плану захисту системи, який містить рекомендації та заходи для зменшення ризиків порушення безпеки системи.

Отже, хоча SMM та TRA мають різний підхід до оцінки безпеки інформаційної системи, обидва підходи можуть бути корисними при плануванні та забезпеченні високого рівня безпеки. SMM допомагає зосередитися на розвитку та підвищенні рівня безпеки системи, тоді як TRA зосереджується на ідентифікації та зменшенні ризиків, пов'язаних з безпекою системи.

3.5 Стандарти ISO

Окрім вищезгаданих методів, проаналізувати захищеність інформаційної системи можна за допомогою стандірів, тобто перевіривши сисему на відповідність їм.

3.5.1 ISO 27001

Стандарт ISO 27001 (Системи управління інформаційною безпекою) включає в себе широкий спектр критеріїв безпеки, але деякі з перерахованих критеріїв можуть не бути прямо перевіреними самим

стандартом. Варто відзначити, що хоча ISO 27001 надає загальний фреймворк для управління інформаційною безпекою, вона не визначає конкретні методи перевірки кожного окремого критерію.

Ось які критерї не зможуть бути перевіреними самим стандартом ISO 27001:

1. **Надійність**: ISO 27001 не включає специфічні вимоги щодо надійності системи. Проте, за допомогою інших документів, таких як ISO 27002 (Практики безпеки інформації), можна знайти рекомендації та керівництва щодо забезпечення надійності.

2. **Відновлюваність**: ISO 27001 не надає конкретних вимог щодо планування та відновлення після інцидентів. Проте, вимоги щодо бізнес-континуїтету та відновлення можна знайти в інших стандартах, наприклад, ISO 22301 (Системи управління бізнес-континуїтетом).

3. **Спостережуваність**: ISO 27001 не визначає конкретні вимоги щодо спостережуваності системи. Однак, цей аспект безпеки може бути охоплений іншими положеннями стандарту, такими як вимоги до журналів подій та моніторингу.

Важливо відзначити, що хоча ISO 27001 не включає пряму перевірку цих критеріїв, вона стимулює організації до впровадження ризик-орієнтованого підходу до управління інформаційною безпекою.

3.5.2 ISO 15408

ISO/IEC 15408, відомий також як стандарт Common Criteria (CC), є міжнародним стандартом для оцінки захищеності інформаційних систем. Він надає загальні принципи та методику оцінки безпеки, що дозволяє організаціям оцінювати безпеку продуктів, систем або рішень IT та встановлювати їхню відповідність до конкретних безпечних вимог.

Ось деякі способи, якими ISO/IEC 15408 може бути корисний для оцінки захищеності інформаційної системи:

Стандарт ISO/IEC 15408 надає об'єктивну методологію для оцінки безпеки. Він встановлює систематичний підхід до оцінки, що дозволяє здійснювати оцінку на основі специфічних безпечних вимог. Це допомагає організаціям отримати об'єктивну оцінку захищеності своїх інформаційних систем та ідентифікувати можливі недоліки чи слабкі місця.

ISO/IEC 15408 є міжнародним стандартом, що має велику вагу і визнання у галузі кібербезпеки. Використання цього стандарту для оцінки захищеності дозволяє організаціям довести свою відповідність встановленим міжнародним стандартам і нормативам безпеки.

ISO/IEC 15408 визначає стандартизований процес оцінки безпеки, що включає визначення вимог, виконання оцінки, проведення тестування безпеки та документування результатів. Це допомагає організаціям проводити систематичну та повноцінну оцінку безпеки своїх інформаційних систем.

ISO/IEC 15408 забезпечує оцінку безпеки на основі встановлених критеріїв та рівнів впливу безпеки. Це надає організаціям достатньо

інформації для прийняття обгрунтованих рішень щодо безпеки, включаючи вибір відповідних контрольних заходів та визначення необхідності додаткових заходів безпеки.

Використання ISO/IEC 15408 для оцінки захищеності дозволяє організаціям незалежно оцінювати безпеку продуктів або рішень від різних постачальників. Вони можуть встановлювати спільні критерії безпеки та порівнювати різні варіанти, що допомагає вибрати найбільш підходящі рішення з точки зору безпеки.

Загалом, ISO/IEC 15408 є цінним інструментом для оцінки захищеності інформаційної системи, який допомагає забезпечити об'єктивну оцінку безпеки, відповідність міжнародним стандартам та прийняття обгрунтованих рішень щодо безпеки.

ISO/IEC 15408 встановлює загальні вимоги та процедури для оцінки та сертифікації безпеки інформаційних систем. В рамках цього стандарту визначаються терміни, процеси та методології, які можна використовувати для оцінки та сертифікації систем з урахуванням конкретних критеріїв безпеки. Однак, самі критерії безпеки не деталізуються або не перераховуються як окремі елементи в стандарті ISO/IEC 15408.

Отже, стандарт ISO/IEC 15408 не надає вичерпного опису кожного з перерахованих критеріїв безпеки, але може використовуватись як основа для розробки та оцінки систем з урахуванням цих критеріїв. Для більш детального опису кожного з критеріїв безпеки можуть використовуватися інші стандарти, розширення або методології.

3.6 Порівняння методів оцінки захищеності інформаційної системи

Вибір методу оцінки захищеності системи, такого як SMM, TRA або OCAVE, залежить від конкретних потреб організації, характеристик системи та доступних ресурсів. Кожен з цих методів має свої особливості та переваги, і важливо врахувати контекст і конкретні вимоги при виборі.

SMM (Security Maturity Model): Цей метод оцінки зосереджений на оцінці рівня зрілості безпеки організації, її процесів та практик. SMM вимагає виконання аналізу поточного стану безпеки та порівняння з набором критеріїв, що визначають рівні зрілості. Цей метод особливо корисний для організацій, які бажають розробити довготривалу стратегію безпеки та поетапно підвищувати свій рівень безпеки.

TRA (Threat and Risk Assessment): Цей метод оцінки зосереджений на виявленні потенційних загроз і ризиків, які можуть впливати на безпеку інформаційної системи. TRA вимагає ідентифікації загроз, оцінки ризиків та розробки стратегій мінімізації ризиків. Цей метод корисний для виявлення конкретних загроз та ризиків і розробки конкретних заходів забезпечення безпеки.

OCAVE (Operational Cybersecurity Assessment for Vulnerability Elimination): Цей метод оцінки зосереджений на виявленні вразливостей в системі та розробці планів їх виправлення. OCAVE вимагає систематичного сканування, аналізу та оцінки вразливостей, а також розробки конкретних заходів з попередження та виправлення вразливостей. Цей метод корисний для організацій, які бажають активно виявляти та виправляти вразливості в своїй системі.

При виборі методу оцінки важливо враховувати свої потреби, доступні ресурси, специфіку системи та контекст організації. Іноді комбінування різних методів може бути найкращим підходом для забезпечення повної оцінки захищеності системи.

Для порівняння різних методів використовуємо критерії виокремлені вище:

Де 0 – метод оцінювання не може перевірити необхідний критерій.

1 – метод може перевірити відповідність, але для оцінки необхідно залучити інші інструменти.

2 – цим методом можна оцінити систему на відповідність критерію без залученнядодаткових інструментів.

Таблиця 3.1 – Відповідність методів оцінювання до критеріїв

	Конфіденційність	Цілісність	Доступність	Аутентифікація	Авторизація	Надійність	Відновлюваність	Спостережуваність
OCAVE	1	1	1	1	1	1	1	1
SMM	2	2	2	2	2	2	2	0
TRA	1	1	1	1	1	1	1	1
ISO 27001	2	2	2	2	2	0	0	0
ISO 15408	1	1	1	1	1	1	1	0

Висновки до розділу 3

В цьому розділі ми аналітично оглянути та проаналізували, відповідно до виділених нами критеріїв, різні методи оцінювання захищеності інформаційної системи. Розглянули та проаналіхували також стандарти ISO 27001 та ISO 15408, які можуть стати основою для побудови захищеної інформаційної системи. Завдяки дослідженню відповідності методів оцінювання до критеріїв,ми систематизували методи, що в подальшому дозволить з легкістю вибрати необхідний з них відповідно до потреб.

4 ОПИС ВЛАСНОГО МЕТОДУ ОЦІНЮВАННЯ

Ідея реалізації власного методу оцінювання була створена на основі піраміди Маслоу.

Піраміда Маслоу, відома також як ієрархія потреб Маслоу, була розроблена американським психологом Абрахамом Маслоу у 1940-50-х роках. Ця теорія відображає ієрархічну структуру потреб людини, де кожен рівень потреб має свою важливість і впливає на мотивацію та поведінку особистості. Піраміда Маслоу складається з п'яти рівнів потреб, які розташовані від найбільш базових до більш високих.

Тобто, якщо в піраміді Маслоу людські потреби можна представити у вигляді ієрархічної структури, де більш базові потреби повинні бути задоволені перед тим, як можна перейти до вищих рівнів, то в нашій піраміді аналогічно відбувається з потребами інформаційної системи для її захищеності.

Задоволення потреб нижчого рівня стає основою для прагнення до задоволення потреб вищого рівня. Потреби на нижніх рівнях мають пріоритет перед потребами на вищих рівнях.

Піраміду Маслоу доречно використовувати в оцінці захищеності інформаційних систем, оскільки захист інформації також має ієрархічну структуру потреб. Нижчі рівні піраміди Маслоу відображають базові потреби в безпеці та фізичній захищеності інформаційної системи, такі як фізичний доступ до приміщень, контроль доступу до системи, захист від зловмисних вторгнень та вірусів.

На наступних рівнях враховані потреби в технічній безпеці, такі як шифрування даних, забезпечення цілісності та конфіденційності інформації. Також враховуються потреби в соціальній безпеці, які включають управління доступом до даних інших користувачів, аутентифікацію та авторизацію.

На вищих рівнях піраміди враховані потреби в плануванні реагування на інциденти, виявленні та відновленні після кібератаки, а також потреби в постійному вдосконаленні системи захисту, щоб забезпечити її ефективність та відповідність сучасним загрозам.

Застосування піраміди Маслоу в оцінці захищеності інформаційних систем допомагає систематично аналізувати та оцінювати різні аспекти безпеки, починаючи з базових потреб і переходячи до вищих рівнів. Це дозволяє розуміти загальну структуру ієрархії захисту інформаційних систем і приймати обґрунтовані рішення щодо підвищення їх захищеності.

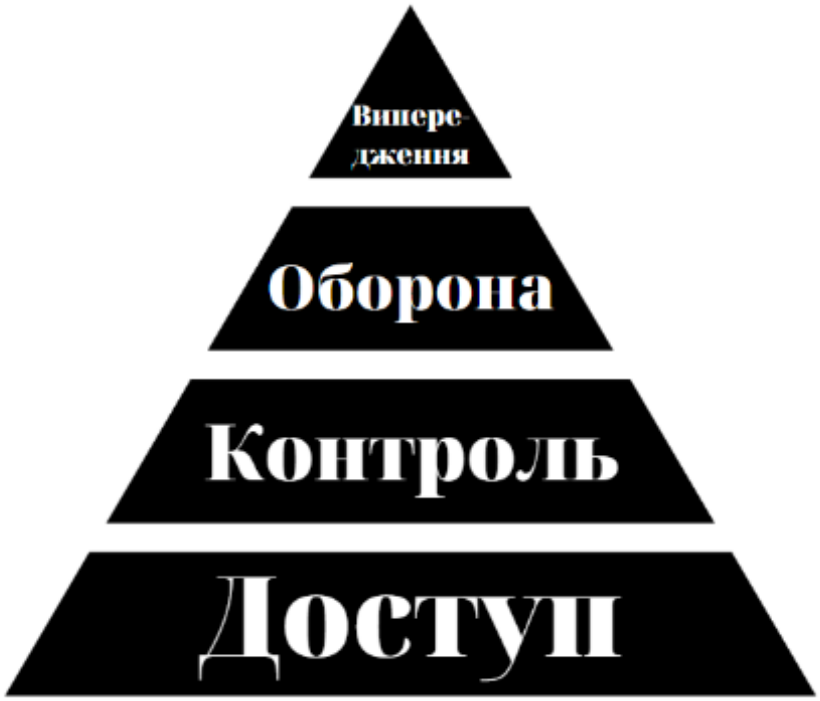

Рисунок 4.1 – Піраміда оцінки захищеності інформаційної системи

Далі описані рівні піраміди захищеності системи:

1. **Рівень доступу**: Система має базові заходи безпеки, такі як встановлення паролів і обмеження доступу до конфіденційної інформації.

2. **Рівень контролю**: Система має розширені заходи безпеки, які включають в себе регулярне оновлення програмного забезпечення, встановлення антивірусного програмного забезпечення, аутентифікацію користувачів і контроль доступу до конфіденційної інформації.

3. **Рівень оборони**: Система має високий рівень захисту, що включає в себе захист від відомих та невідомих загроз, в тому числі захист від атак з використанням соціальної інженерії, а також захист від

внутрішніх загроз, таких як зловживання даними або крадіжки інформації. Крім того, така система може мати складну інфраструктуру з високим рівнем автоматизації процесів забезпечення безпеки.

4. **Рівень випередження**: Система має найвищий рівень захисту, що включає в себе захист від невідомих загроз, захист від атак з використанням передових технологій та захист від внутрішніх загроз з боку найбільш привілейованих користувачів. Вона може мати складну інфраструктуру з високим рівнем автоматизації процесів забезпечення безпеки.

І тим самим при створенні інформаційної системи необхідно йти послідовно, задовольняючи рівень за рівнем. Особливість цього методу в тому, що система залишається на найменшому рівні поки повністю не задовільнить всі його вимоги. Тобто маючи антивірусне програмне забезпечення, але при цьому не маючи обмеження доступу до конфіденційної інформації, система залишається на рівні доступу.

Висновки до розділу 4

В цьому розділі роботи описаний метод оцінювання захищеності інформаційної системи, який заснований на ідеї піраміди Маслоу, за допомогою якого спеціалісти кібербезпеки з легкістю зможуть передавати роботу один одному, адже зазначивши на якому рівні зараз знаходиться система, інший спеціаліст одразу зрозуміє обсяг роботи який йому необхідно впровадити задля забезпечення найвищого рівня захищеності системи.

Проаналізувавши цей метод на відповідність вище виділеним критеріям можна побачити, що він задовільняє їх всі, а отже є універсальним. Також, розробка цього методу дає можливість науковцям і дослідникам використовувати його як основу для інших, більш розширених робіт.

ВИСНОВКИ

В ході роботи було виділено основні аспекти побудови методу оцінювання захищеності ІС, включаючи його етапи, причини та критерії.

В роботі також описано найпопулярніші фреймворки для оцінки захищеності інформаційних систем, які сприяють стандартизації та систематизації процесу оцінки, а також надають цінні рекомендації для покращення безпеки системи. Вони є цінними інструментами для організацій, які мають на меті забезпечити високий рівень захищеності своїх інформаційних ресурсів.

Було описано найвідоміші методики, моделі та методи оцінювання захищеност інформацйної системи та проаналізовано їх відповідно до виділених вище критеріїв.

Також було описано метод оцінювання захищеності інформаційної системи, заснований на ідеї піраміди Маслоу, дозволяє спеціалістам з кібербезпеки легко передавати роботу один одному, використовуючи структурований підхід. Вказавши поточний рівень захищеності системи на піраміді, інший спеціаліст може швидко зрозуміти обсяг роботи, який необхідно виконати для досягнення найвищого рівня захищеності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 Жембровська О.С., Ткач В. М. Оцінка захищеності інформаційної системи // Всеукраїнська науково-практична конференція Theoretical and Applied Cybersecurity (TACS - 2023) (26 травня 2023, м. Київ)

2 О. Ю. Юдін, В. М. Сидоренко , С. О. Гнатюк , О. С. Верховець ”Модель розрахунку кількісного критерію оцінювання захищеності інформаційно-телекомунікаційних систем критичної інфраструктури держави”

3 [Ел. ресурс] – https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/

4 НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

5 Cybersecurity Capability Maturity Model (C2M2) Version 2.1 June 2022, U.S. Department of energy

6 Україна. Закони. «Про основні засади забезпечення кібербезпеки України» : офіц. текст : [прийнятий Верховною Радою 5 жовтня 2017 р.]. К.: Відомості Верховної Ради України, 2017, № 45, ст.403.

7 ISO 27001:2022 - «Information technology — Security techniques — Information security management systems — Requirements».

8 Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації № 745 від 02.12.2022

9 ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.