Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Розробка моделі оцінки захищеності інформаційних систем»

Виконавець: студент ІІ курсу, групи КБм-22

_____ **Павло ЛОВИГІН**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Тетяна БАБЕНКО	
Нормоконтроль	Лариса МИРУТЕНКО	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача КБм-22 (група) Ловигіна Павла Олександрович (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Розробка моделі оцінки захищеності інформаційних систем

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень Процес оцінки рівня захищеності інформаційних систем.

Предмет досліджень Моделі оцінки захищеності інформаційних систем на основі нейронних мереж.

Мета Розробка моделі оцінки захищеності інформаційних систем.

Вихідні дані для проведення роботи Методи та моделі оцінки захищеності інформаційних систем.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Покращення існуючих підходів до оцінки захищеності інформаційних систем.

Практична цінність Синтезована модель оцінки захищеності інформаційних систем різних типів, яка може бути використана для оцінки захищеності будь-якими організаціями.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	17.11.2023 – 29.01.2024
Аналіз літературних джерел	30.01.2024 – 12.02.2024
Аналіз методологій оцінки захищеності	13.02.2024 – 21.02.2024
Розгляд теоретичних аспектів оцінки захищеності	22.02.2024 – 26.02.2024
Аналіз методів побудови моделей загроз	27.02.2024 – 04.03.2024
Визначення індикаторів та метрик захищеності	05.03.2024 – 10.03.2024
Вибір методології оцінки захищеності	11.03.2024 – 17.03.2024
Розробкка моделі оцінки захищеності	18.03.2024 – 19.03.2024
Підготовка даних для моделювання	20.03.2024 – 17.04.2024
Моделювання та аналіз адекватності	18.04.2024 – 25.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 12.05.2024
Подача пакету документів на розгляд ЕК	13.05.2024 – 17.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	Зниження витрат на оцінку захищеності.
Соціальний ефект	Покращення забезпечення захисту інформаційних систем на підприємствах та інших організаціях.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Тетяна Бабенко
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Павло ЛОВИГІН
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Розробка моделі оцінки захищеності інформаційних систем»: 108 сторінки, 6 рисунків та 4 таблиці. 81 літературне джерело.

Метою роботи є розробка моделі оцінки захищеності інформаційних систем.

Для досягнення зазначеної мети поставлено наступні завдання:

- Аналіз підходів до оцінки рівня захищеності інформаційних систем.
- Аналіз індикаторів та метрик оцінки захищеності інформаційних систем.
- Створити структурований опис потенційних загроз для інформаційної системи.
- Розробка моделі оцінки захищеності інформаційних систем.
- Аналіз адекватності запропонованого рішення.

Об’єктом дослідження є процес оцінки рівня захищеності інформаційних систем.

Предметом дослідження механізми оцінки рівня захисту інформаційних систем.

Методи дослідження: аналіз відкритих джерел, порівняння методів оцінки захищеності, аналіз методів аналізу загроз, проектування штучної нейронної мережі.

Актуальність роботи полягає в тому, що оцінка захищеності інформаційних систем дозволяє вчасно виявляти «слабкі місця» системи під час проектування чи використання системи і полегшує процес покращення рівню захищеності. Всі існуючі підходи мають певні вади та недоліки і на меті роботи стоїть створення моделі, яка би поєднувала найкращі риси існуючих підходів, мінімізуючи вплив недоліків систем.

Практичною цінністю отриманих результатів є синтезована модель оцінки захищеності інформаційних систем різних типів. Розроблену модель можна використовувати для оцінки вже існуючих систем та при плануванні розгортання нових

систем різними приватними та державними організаціями, незалежно від розміру організацій, складності та розміру їх систем.

Наукова новизна роботи полягає в покращенні існуючих підходів до оцінки захищеності інформаційних систем шляхом розробки нової моделі, яка простіша у використанні і потребує меншої кількості ресурсів із збереженням точності оцінки.

Ключові слова: машинне навчання, STRIDE, DREAD, NIST, оцінка захищеності, індикатори захищеності, random forest.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

OWASP	–	Open Web Application Security Project
ISA	–	International Society of Automation
IEC	–	International Electrotechnical Commission
NIST	–	National Institute of Standards and Technology
ISO	–	International Organization for Standardization
ICS	–	Industrial Control Systems
VPN	–	Virtual Private Network
TLS	–	Transport Layer Security
IPS	–	Intrusion Prevention System
IDS	–	Intrusion Detection System
IC	–	Інформаційна система
GDPR	–	General Data Protection Regulation
HIPAA	–	Health Insurance Portability and Accountability Act
PCI DSS	–	Payment Card Industry Data Security Standard
АЗ	–	Апаратне забезпечення
ПЗ	–	Програмне забезпечення

ЗМІСТ

ВСТУП

У світі, де кількість кібератак, як і використання інформаційних систем, з кожним днем все збільшуються актуальність захисту даних стає дедалі вищою. Атаки на недостатньо захищені системи мають все більше і більше впливу на фізичний світ навколо – одна «вдала» реалізація загрози може призвести до втрати колосальних об’ємів даних, відключення промислових систем, керуючих базовими технологіями – генерацією електроенергії, наприклад [1,2]. Існує багато підходів до покращення інформаційних систем з точки зору безпеки, базовим з яких є оцінка захищеності.

Оцінка захищеності інформаційних систем допомагає виявити слабкі місця в системі та розробити план дій для зменшення ризиків. Цей план може включати застосування технічних, організаційних та процедурних заходів безпеки. Важливим аспектом є забезпечення відповідності системи вимогам безпеки, стандартам та регуляторним вимогам. Результати оцінки можуть використані як під час планування та проектування системи, так і під час використання.

Існуючі підходи оцінки захищеності дозволяють ефективно оцінити загальний рівень захищеності, кожен базуючись на своєму власному наборі метрик та оцінок. Проблема полягає в тому, що залежно від самої інформаційної системи, критичності даних, присутній у них, регуляторних чи інших вимог до захисту інформації оцінки можуть сильно різнитись.

Вибір лише однієї моделі чи методу оцінки суттєво звужує можливості організації у питаннях покращення захищеності. Оцінка системи за допомогою різних підходів – дуже складний з точки зору ресурсів процес, тому частіше використовується один основний метод оцінки, який зручніший для організації, яка проводить оцінку, а інші відкидаються.

Таким чином, актуальним науковим завданням є створення загальної моделі оцінки, яка здатна об’єднувати переваги декількох підходів і вирішити питання підвищеної складності використання дозволить суттєво зменшити необхідну для оцінки кількість ресурсів, що в свою чергу дозволить більшій кількості власників та операторів систем вчасно виявити недоліки у кібербезпеці та запобігти критичним для себе, й потенційно інших організацій, кібератакам.

РОЗДІЛ 1
ОГЛЯД ІСНУЮЧИХ МОДЕЛЕЙ ОЦІНКИ ЗАХИЩЕНОСТІ

1.1 Методології оцінки захищеності

1.1.1 NIST Cybersecurity Framework (CSF)

Це набір керівних принципів, практик та рекомендацій, розроблений Національним інститутом стандартів та технологій (NIST) США, який допомагає організаціям удосконалити стан своєї кібербезпеки. CSF допомагає організаціям виявляти, запобігати та відповідати на кіберзагрози шляхом визначення, впровадження та підтримки ефективних заходів забезпечення кібербезпеки [3].

CSF базується на керівних принципах, що включають основні функції кібербезпеки: захист, виявлення, реагування та відновлення.

Він складається з ряду категорій, підкатегорій та рекомендацій, які допомагають організаціям систематично вдосконалювати свої заходи з кібербезпеки.

Керівні принципи визначають основні цілі та принципи, які повинні керувати діяльністю з кібербезпеки в організації. Ці принципи включають в себе:

1. Керівництво.
2. Організацію та структуру.
3. Технологію.
4. Процеси.
5. Людський капітал.

Категорії описують основні аспекти, які потрібно враховувати для ефективного керування кібербезпекою. Вони включають:

1. Ідентифікацію.
2. Захист.

3. Виявлення.

4. Відповідь.

5. Відновлення.

Підкатегорії конкретизують кожну категорію, розширюючи її та вказуючи на конкретні завдання або заходи, які можна виконати для досягнення кожної з цих категорій.

Рекомендації містять в собі додаткові ресурси, які можуть допомогти організаціям реалізувати кожну з підкатегорій. Ці ресурси можуть включати стандарти, документацію, методи та інші корисні матеріали.

Ця структура надає систематичний підхід до керування СУІБ в організаціях та дозволяє їм ідентифікувати, захищати, виявляти, реагувати на загрози, а також відновлювати інформаційні системи у випадку реалізації загрози. Кожен компонент CSF взаємодіє з іншими, створюючи комплексний підхід до забезпечення кібербезпеки.

У лютому 2024 року вийшла нова редакція стандарту – NIST CSF 2.0, яка має велику кількість нововведень і переосмислень минулих версій стандарту. Організації в світі та в Україні починають впроваджувати нову редакцію стандарту, але цей процес тільки розпочався. В контексті цієї роботи доцільно більш детально розглянути нову версію стандарту [4, 5].

NIST CSF 2.0 складається з трьох основних частин:

- Ядро CSF – таксономія результатів кібербезпеки високого рівня, яка може допомогти будь-якій CSF управляти своїми ризиками кібербезпеки.
- Організаційні профілі CSF – Механізм опису поточного та/або цільового стану кібербезпеки організації та/або цільового стану кібербезпеки організації з точки зору результатів Ядра CSF.
- Рівні CSF – можуть бути застосовані до організаційних профілів CSF, щоб охарактеризувати суворість управління ризиками кібербезпеки в організації управління ризиками кібербезпеки в організації та практики управління ними.

NIST CSF 2.0 виділяє шість основних функцій.

Управління – стратегія управління ризиками кібербезпеки організації, очікування та політики – виділені, доведені до персоналу та контрольовані.

NIST надає наступні настанови відповідно до цієї функції:

Розробити стратегію управління ризиками кібербезпеки, що враховуватиме конкретні потреби та ризики організації.

Визначити унікальні вимоги та потреби організації у сфері кібербезпеки. Провести аналіз поточного та передбачуваного середовища ризиків та готовності організації до прийняття ризиків. Залучити всіх співробітників організації до обговорення ідей та пропозицій. Вивчити ініціативи, які були успішними або невдалими, і відкрито обговорити їх.

Розробити стратегію, яка враховуватиме конкретні цілі та специфіку ризиків організації, а також досвід інших організацій.

Постійно керувати та оновлювати стратегію на регулярних інтервалах. Чітко визначити ролі та обов'язки управління ризиками кібербезпеки.

Розробити політику управління ризиками, яка буде затверджена керівництвом, повторювана та відповідатиме поточним загрозам та цілям організації. Впровадити політику у корпоративну культуру для стимулювання обґрунтованого прийняття рішень. Врахувати юридичні, регуляторні та договірні зобов'язання.

Розробити та поширити організаційні практики кібербезпеки, які будуть зрозумілими та регулярно комунікуватися. Задокументувати практики та ділитися ними для зворотного зв'язку та гнучкості у виправленні курсу.

Впровадити та контролювати управління ризиками кібербезпеки в ланцюгу постачання, включаючи стратегію, політику, ролі та обов'язки. Залучити партнерів і постачальників до планування, реагування та відновлення.

Проводити постійний нагляд та контроль ризиків, а також їхнє постійне оновлення та аналіз.

Ідентифікація – ризики кібербезпеки мають бути зрозумілі.

Стандарт рекомендує наступні дії: визначити критичні бізнес-процеси та активи – які види діяльності організації неодмінно мають залишатися життєздатними. Наприклад, це може включати підтримку веб-сайту для отримання платежів, забезпечення безпеки інформації про клієнтів/пацієнтів або забезпечення доступності та точності критично важливої інформації. Провести інвентаризацію обладнання, програмного забезпечення, послуг та систем, включаючи власне обладнання, орендоване, персональні пристрої та додатки співробітників. Документувати інформаційні потоки та розташування даних, зокрема зберігання та використання даних у контрактах та зовнішніх партнерів. Виявити загрози, вразливості та ризики для активів організації. Задокументувати ідентифіковані ризики та розробити стратегії реагування на них. Переконатися, що реагування на ризики визначені, пріоритизовані та виконані, а результати моніторяться. Використовувати отриманий досвід для вдосконалення стратегій. Визначити можливості для підвищення продуктивності та кращого управління ризиками кібербезпеки. Підготувати звіт про дії після інциденту для документування самого інциденту, реакції, відновлення та отриманих уроків.

Захист – використання запобіжних заходів для управління кібербезпекою організації.

Керування доступом, шляхом створення унікальних облікових записів для співробітників та обмеженням їх доступу лише до необхідних ресурсів (принцип найнижчих привілеїв). Перед наданням користувачам доступу до інформації, комп'ютерів і додатків, рекомендується здійснювати їх автентифікацію.

Керуванням та відстеженням фізичного доступу до об'єктів та пристроїв слід займатися регулярно.

Рекомендується регулярно навчати працівників щодо політики та процедур кібербезпеки, а також пояснювати, як розпізнавати типові атаки та повідомляти про підозрілу активність. Захист та контроль своїх пристроїв можна забезпечити шляхом

використання продуктів для захисту кінцевих точок (endpoint protection, endpoint detection and response – EDR) та встановлення єдиної конфігурації та журналізації.

Рекомендується захищати конфіденційні дані шляхом шифрування та періодичної перевірки цілісності, а також забезпечити безпечне видалення або знищення зайвої інформації.

Регулярне оновлення програмного забезпечення та створення резервних копій даних слід виконувати згідно з узгодженим розкладом, зберігаючи принаймні один набір даних в автономному режимі для захисту від програм-вимагачів. Рекомендується проводити тестування, щоб переконатися, що резервні копії можна успішно відновити до систем.

Виявлення – пошук та вивчення можливих загроз кібербезпеці і компрометації.

Слід постійно контролювати мережі, системи та обладнання для виявлення потенційно несприятливих подій. Рекомендується розробляти і тестувати процеси та процедури виявлення показників інцидентів кібербезпеки як у мережі, так і в фізичному середовищі. Здобуту інформацію журналу слід збирати з численних організаційних джерел для допомоги у виявленні несанкціонованої діяльності.

Важливим кроком є визначення та аналіз передбачуваного впливу і обсягу несприятливих подій. Якщо виявлено подію кібербезпеки, організація має швидко та ретельно зрозуміти вплив інциденту. Розуміння деталей будь-яких інцидентів кібербезпеки допомагатиме у формуванні відповіді. Рекомендується надавати інформацію про побічні явища уповноваженому персоналу та інструментам.

При виявленні інцидентів слід надавати інформацію про подію внутрішньому уповноваженому персоналу для забезпечення відповідних заходів реагування на інцидент.

Відповідь – виконання дій відносно інцидентів кібербезпеки.

Виконання плану реагування на інцидент після його оголошення повинно здійснюватися у координації з відповідними третіми сторонами. Для належного

виконання плану реагування на інцидент слід переконатися, що всі знають свої обов'язки; це включає розуміння будь-яких вимог, таких як регуляторні, юридичні звітності та обмін інформацією.

Рекомендується розподілити інциденти за категоріями та пріоритетами, а також підвищувати рівень критичності за необхідності. Після аналізу подій слід визначити першопричину інциденту та встановити пріоритети для тих проблем, які потребують першочергової уваги. Цю пріоритетність слід повідомити команді, а також переконатися, що всі члени команди розуміють кому слід повідомляти інформацію про пріоритетний інцидент при його виникненні.

Важливим є збір даних про інциденти та збереження їхньої цілісності та походження. Збір інформації повинен бути безпечним, щоб забезпечити реагування вашої організації на інцидент, а також для збереження репутації та довіри зацікавлених сторін. Безпечне зберігання цих даних допоможе в розробці оновлених та майбутніх планів реагування на інциденти, щоб вони були ще ефективнішими.

Повідомлення внутрішніх та зовнішніх зацікавлених сторін про будь-які інциденти та обмін з ними інформацією слід робити відповідно до політик, встановлених організацією. Безпечний обмін інформацією є важливим аспектом планів реагування та угод про обмін інформацією.

Локалізація та ліквідація наслідків інциденту залежить від виконання розробленого та протестованого плану реагування. Координація та ефективна комунікація з зацікавленими сторонами може сприяти більш ефективному реагуванню та пом'якшенню наслідків інциденту.

Відновлення – відновлення операцій та активів після інцидентів.

Розуміння ролей та обов'язків важливо для визначення того, хто у вашому бізнесі та за його межами несе відповідальність за відновлення. Важливо знати, хто має доступ і повноваження для прийняття рішень щодо здійснення заходів з реагування від імені бізнесу.

Після цього слід виконати план відновлення, забезпечивши операційну доступність постраждалих систем і сервісів, а також визначивши пріоритети та виконуючи завдання з відновлення.

Важливим етапом є перевірка виконаної роботи. Важливо забезпечити цілісність резервних копій та інших засобів відновлення, перш ніж використовувати їх для відновлення звичайних бізнес-операцій.

Під час спілкування з внутрішніми та зовнішніми зацікавленими сторонами необхідно ретельно продумати, якою інформацією, як і коли ви будете ділитися з різними зацікавленими сторонами. Важливо, щоб усі зацікавлені сторони отримали необхідну інформацію, але при цьому не поширювалася неналежна інформація.

Необхідно також повідомляти своїм співробітникам про будь-які отримані уроки та зміни в процесах, процедурах і технологіях згідно з політикою, вже встановленою організацією. Це може бути вдалий час для навчання або перепідготовки персоналу з питань кібербезпеки та кращих практик у цій сфері.

Використання NIST CSF найбільш доцільне для будь-яких організацій, від критичної інфраструктури та державних установ до приватних компаній різних розмірів, що робить цей стандарт універсальним [6,7].

1.1.2 OWASP Risk Rating

OWASP Risk Rating – це методологія для оцінки ризиків безпеки веб-додатків, розроблена організацією OWASP (Open Web Application Security Project).

OWASP – це некомерційна організація, яка займається покращенням безпеки програмного забезпечення. OWASP розробляє різноманітні матеріали, включаючи стандарти та інструменти, спрямовані на підвищення рівня безпеки веб-додатків [8].

OWASP Risk Rating дозволяє визначити й оцінити потенційні загрози та вразливості, які можуть вплинути на безпеку додатка, а також визначити його загальний

рівень ризику. Зазвичай оцінка ризику включає в себе аналіз потенційного впливу загроз та ймовірності їх виникнення, а також можливі наслідки для додатка та організації в цілому [9].

OWASP Risk Rating може бути корисним інструментом для розуміння та керування ризиками безпеки веб-додатків, що дозволяє організаціям приймати обґрунтовані рішення з покращення безпеки своїх програмних продуктів.

Процес оцінки можна розділити на наступні кроки:

Інвентаризація активів: перший крок – ідентифікація всіх активів, пов'язаних з веб-застосунком, таких як веб-сторінки, сервери, бази даних, інтегровані служби тощо.

Оцінка загроз: далі визначаються потенційні загрози, які можуть вплинути на ці активи. Це можуть бути атаки з використанням вразливостей, атаки на автентифікацію, витік конфіденційної інформації тощо.

Оцінка вразливостей: здійснюється оцінка існуючих вразливостей у веб-застосунку. Це може включати недостатню автентифікацію, незахищені точки входу, некоректну обробку введених даних тощо.

Визначення наслідків: оцінюються потенційні наслідки використання вразливостей при вразливості атаки. Це може бути втрата конфіденційності даних, порушення доступності або порушення цілісності веб-застосунку.

Визначення ймовірності: оцінюється ймовірність виникнення кожної загрози та вразливості. Вона може бути оцінена за шкалою від низької до високої.

Розрахунок ризику: на основі вищезгаданих кроків розраховується ризик для кожної з визначених загроз. Це робиться шляхом перемноження ймовірності та впливу загрози, щоб отримати числове значення ризику.

Визначення пріоритетів: на кінцевому етапі ризики ранжируються за їхнім рівнем серйозності, щоб визначити, які проблеми потребують негайного врегулювання, а які можуть бути вирішені в майбутньому.

Використання OWASP Risk Rating є найбільш доцільним у розробці веб-застосунків. Команди розробників можуть використовувати OWASP Risk Rating для оцінки потенційних загроз та вразливостей їхніх веб-застосунків ще на етапі розробки. Це дозволяє враховувати аспекти безпеки в процесі розробки і вже на початкових етапах уникати вразливостей, які можуть стати проблемою у майбутньому [10].

Команди з безпеки можуть використовувати OWASP Risk Rating для оцінки безпеки існуючих веб-застосунків у вже розгорнутому середовищі. Це допомагає виявити потенційні загрози та вразливості, які вже можуть існувати, і розробити плани для їхнього виправлення.

Найбільш ефективним буде використання підходу в усьому циклі SDLC і періодичне переоцінювання захищеності додатків [11].

1.1.3 ISA/IEC 62443

ISA/IEC 62443 – це серія міжнародних стандартів, розроблених Міжнародною організацією зі стандартизації (International Society of Automation, ISA) та Міжнародним електротехнічним комітетом (International Electrotechnical Commission, IEC), які стосуються кібербезпеки промислових автоматизованих систем. Ці стандарти призначені для захисту промислових систем керування від кіберзагроз, зокрема в промислових, енергетичних, транспортних і системах водопостачання [12].

Основні положення стандарту, релевантні в контексті оцінки захищеності інформаційних систем наступні:

Архітектура систем – стандарт визначає принципи та рекомендації щодо архітектури промислових систем керування з метою забезпечення їхньої кібербезпеки. Це охоплює визначення мережевої топології, сегментації мережі, зон безпеки та інші аспекти.

- Зональний підхід: одним з основних принципів архітектури систем за стандартом ISA/IEC 62443 є використання зонального підходу. Система розділяється на зони, кожна з яких має власні обмеження доступу та заходи безпеки. Це дозволяє контролювати та мінімізувати ризики для системи в цілому.
- Визначення зон безпеки: архітектура системи передбачає визначення різних зон безпеки залежно від рівня чутливості та важливості даних та функціональних областей. Наприклад, можуть бути визначені такі зони, як "зона керування", "зона виробництва", "зона підтримки" тощо.
- Сегментація мережі: одним із заходів для забезпечення безпеки є сегментація мережі. Це означає розділення мережі на логічні частини або сегменти, кожен з яких може мати власні правила доступу та заходи захисту.
- Захист мережевого трафіку: архітектура системи передбачає захист мережевого трафіку шляхом використання шифрування, мережевих брандмауерів, систем виявлення вторгнень та інших заходів. Це допомагає у запобіганні несанкціонованому доступу до мережі та даних.
- Ідентифікація та аутентифікація: для забезпечення безпеки важливо правильно ідентифікувати та аутентифікувати користувачів та пристрої. Це може включати використання паролів, біометричних даних, токенів або інших методів.
- Моніторинг та аналіз безпеки: архітектура системи передбачає наявність систем моніторингу та аналізу безпеки для виявлення потенційних загроз та вразливостей. Це допомагає оперативно реагувати на інциденти та запобігати їхньому виникненню.
- Загалом, архітектура систем за стандартом ISA/IEC 62443 спрямована на створення промислових систем керування, які мають високий рівень безпеки та стійкості до кіберзагроз. Це досягається за допомогою розділення системи на зони безпеки, застосування заходів контролю доступу та захисту мережі, а також моніторингу та аналізу безпеки.

Управління доступом – стандарт встановлює вимоги до управління доступом до систем та пристроїв. Це включає ідентифікацію та аутентифікацію користувачів, управління привілеями, контроль доступу до ресурсів і т.д.

- Ідентифікація користувачів і пристроїв: перший крок управління доступом – це ідентифікація користувачів та пристроїв. Кожен користувач і кожен пристрій повинні мати унікальний ідентифікатор, що дозволяє системі визначити їхню ідентичність при спробі доступу.
- Аутентифікація: після ідентифікації користувача або пристрою система повинна перевірити їхню аутентичність. Це може включати перевірку пароля, використання біометричних даних або інших методів, що підтверджують ідентичність.
- Авторизація: після успішної аутентифікації система повинна визначити, які ресурси або функції можуть бути доступні для користувача або пристрою. Це визначається на основі ролей, прав доступу та політик безпеки.
- Контроль доступу: управління доступом також включає контроль доступу до різних ресурсів і функцій. Це може включати налаштування прав доступу, встановлення обмежень на основі часу або місцезнаходження, а також застосування інших заходів захисту.
- Аудит доступу: ще одним важливим аспектом управління доступом є аудит доступу. Система повинна вести журнал усіх спроб доступу, успішних і неуспішних, щоб забезпечити можливість виявлення незвичайної або підозрілої активності.
- Моніторинг та аналіз: остаточним етапом управління доступом є постійний моніторинг та аналіз активності. Це допомагає виявляти аномальні патерни, загрози або вразливості в системі та негайно реагувати на них.

Мережева безпека: ISA/IEC 62443 містить вимоги та рекомендації щодо захисту мережевого середовища від кібератак, включаючи захист від несанкціонованого доступу, захист мережевого трафіку та інші заходи.

- Архітектура мережі: стандарт надає рекомендації щодо проектування безпечних архітектур мережі для промислових систем. Це включає розподілення мережевих сегментів, використання відокремлених мереж та впровадження заходів забезпечення захисту мережевого трафіку.
- Управління доступом: стандарт рекомендує застосування строгого управління доступом до промислових мереж, включаючи ідентифікацію, аутентифікацію, авторизацію і аудит доступу до систем та пристроїв.
- Шифрування даних: для захисту конфіденційності та цілісності даних, що передаються по мережі, рекомендується використання шифрування. Це може включати використання VPN, TLS або інших протоколів шифрування.
- Захист від атак: стандарт надає рекомендації щодо захисту мережі від різних типів кібератак, таких як вторгнення, віруси, шкідливі програми тощо. Це включає застосування вогнепроводів, систем виявлення вторгнень (IDS), систем запобігання вторгнень (IPS) та інших заходів безпеки.
- Моніторинг та аналіз безпеки: забезпечення постійного моніторингу та аналізу мережі для виявлення потенційних загроз та вразливостей. Це дозволяє вчасно реагувати на кіберзагрози та зменшує ризик інцидентів безпеки.
- Аварійне відновлення: стандарт також включає рекомендації щодо розробки планів аварійного відновлення для відновлення роботи мережі в разі кібератак або інших непередбачуваних подій.

Захист від зловмисних програм – стандарт розглядає заходи щодо захисту від шкідливих програм, таких як віруси, троянці, черви тощо. Це включає антивірусний захист, контроль програм та інші заходи безпеки.

- Антивірусне програмне забезпечення: встановлення та постійне оновлення антивірусного програмного забезпечення на всіх комп'ютерах та серверах в мережі. Антивірусна програма повинна регулярно перевіряти системи на наявність потенційно шкідливих програм та вірусів.

- Виявлення та запобігання: використання систем виявлення та запобігання вторгнень (IDS/IPS), які можуть виявляти та блокувати спроби вторгнень з боку зловмисних програм.
- Оновлення програмного забезпечення: постійне оновлення програмного забезпечення та встановлення оновлень безпеки для закриття відомих вразливостей, які можуть бути використані зловмисниками для виконання атак.
- Обмеження привілеїв: обмеження прав доступу користувачів та програм до системних ресурсів може допомогти запобігти поширенню зловмисних програм та мінімізувати їхні наслідки.
- Шифрування даних: використання шифрування для захисту конфіденційних даних від несанкціонованого доступу з боку зловмисних програм.
- Навчання користувачів: проведення навчання користувачів щодо обізнаності з кібербезпекою та усвідомленням ризиків від відкриття ненадійних файлів чи посилань, що може призвести до введення зловмисних програм в систему.

Безпека проектування та розробки ПЗ: ISA/IEC 62443 надає вимоги щодо безпеки при проектуванні та розробці програмного забезпечення для промислових систем. Це включає аналіз вразливостей, захист від вразливостей та інші аспекти.

- Аналіз вимог до безпеки: забезпечення включення вимог до безпеки в початкові стадії проектування програмного забезпечення. Це може включати ідентифікацію потенційних загроз та вразливостей, а також встановлення відповідних заходів безпеки.
- Архітектурний дизайн безпеки: розробка безпечних архітектурних рішень, які враховують вимоги до безпеки та мінімізують ризики вразливостей. Це може включати використання принципів захищеного проектування, таких як принцип найменшого дозволення та принцип обмеження доступу.
- Тестування безпеки: проведення регулярного тестування безпеки програмного забезпечення для виявлення та виправлення вразливостей. Це може

включати проведення автоматизованих сканувань вразливостей, тестування на проникнення та аудит безпеки коду.

- Безпека в розробці програмного забезпечення: використання безпечних практик розробки програмного забезпечення, таких як безпека перевірки вводу даних, управління пам'яттю та захист конфіденційності даних.
- Освіта та навчання персоналу: навчання членів команди розробки щодо кращих практик безпеки програмного забезпечення та усвідомлення ризиків безпеки.
- Управління конфігурацією та змінами: забезпечення контролю над конфігурацією та змінами у програмному забезпеченні для мінімізації ризиків безпеки, пов'язаних із непередбаченими змінами.

Аудит та моніторинг – стандарт встановлює вимоги до проведення аудиту безпеки та моніторингу систем з метою виявлення потенційних загроз і вразливостей.

- Аудит безпеки системи: проведення регулярних аудитів безпеки системи для оцінки її відповідності вимогам безпеки та виявлення можливих проблем безпеки.
- Моніторинг подій інцидентів безпеки: встановлення систем моніторингу подій інцидентів безпеки для виявлення незвичайної активності або підозрілих подій, які можуть свідчити про можливі атаки або порушення безпеки.
- Аналіз журналів подій: аналіз журналів подій з метою виявлення та відстеження подій, які можуть вказувати на проблеми безпеки або аномальну активність.
- Оцінка ризиків: проведення регулярних оцінок ризиків для ідентифікації нових загроз та оцінки їхнього потенційного впливу на безпеку системи.
- Тривалість аудитів та моніторингу: забезпечення постійності та регулярності проведення аудитів та моніторингу для ефективного виявлення та вирішення проблем безпеки.
- Звітність і відстеження: підготовка звітів про результати аудитів та моніторингу, а також відстеження за рекомендаціями щодо виправлення виявлених проблем безпеки.

Управління ризиками: ISA/IEC 62443 визначає процес управління ризиками з метою ідентифікації, оцінки та контролю ризиків для промислових систем керування.

- Ідентифікація ризиків: визначення потенційних загроз та уразливостей, які можуть вплинути на безпеку системи. Це може включати виявлення технічних уразливостей, загроз з боку зловмисників, недоліки в процесах та інші фактори, які можуть призвести до виникнення ризиків.
- Оцінка ризиків: оцінка потенційного впливу загроз та уразливостей на безпеку системи, а також ймовірності виникнення цих загроз. Оцінка ризиків дозволяє визначити, які ризики є найбільш критичними та потребують найбільшого уваги.
- Управління ризиками: розробка стратегій та планів для управління виявленими ризиками. Це може включати прийняття заходів для зменшення або усунення ризиків, прийняття рішення щодо прийняття або передачі ризиків, а також встановлення контрольних механізмів для моніторингу та керування ризиками.
- Моніторинг і аналіз ризиків: постійне відстеження та аналіз ризиків для виявлення нових загроз та оцінки їхнього впливу на безпеку системи. Це дозволяє організації реагувати на зміни в загрозах та вразливостях та вчасно вживати заходів для їх усунення або зменшення.
- Звітність і відстеження: підготовка звітів про результати оцінки та управління ризиками, а також відстеження за рекомендаціями щодо керування та мінімізації ризиків. Це допомагає забезпечити ефективне управління ризиками та забезпечити безпеку системи на відповідному рівні [13].

Хоча стандарт ISA/IEC 62443 спрямований на забезпечення безпеки промислових автоматизованих систем, його принципи та практики можуть бути застосовані і в інших типах систем, не обмежуючись промисловістю [14].

1.1.4 NIST SP 800-82

Стандарт NIST SP 800-82 "Guide to Industrial Control Systems (ICS) Security" є документом, що надає рекомендації та керівництво забезпеченням безпеки систем промислового управління (ICS). Він розроблений Національним інститутом стандартів та технологій (NIST) Сполучених Штатів Америки та призначений для допомоги організаціям у розумінні, проектуванні, впровадженні та управлінні безпекою систем промислового управління [15].

Стандарт є важливим документом для організацій, які працюють з системами промислового управління, оскільки він надає детальні рекомендації та керівництво забезпеченням безпеки цих систем. Він є цінним ресурсом для розуміння та захисту від загроз, що виникають в контексті індустріальних середовищ [15].

Огляд систем промислового управління (ICS): документ містить огляд архітектури, типів та функцій систем промислового управління, включаючи системи контролю виробництва, автоматизовані системи будівель, системи контролю та автоматизації енергоспоживання та інші. Основні принципи відповідно до [16]:

- Архітектура систем промислового управління: важливою частиною огляду є розуміння архітектури систем промислового управління. Це включає складність мережевої топології, зв'язок між пристроями та системами, а також розподіленість управління та контролю.
- Типи систем: системи промислового управління можуть включати системи контролю виробництва (PLC), системи дистанційного моніторингу та керування (SCADA), системи управління будівлями (BMS), системи контролю доступу та багато інших. Кожен тип системи має свої унікальні особливості, які слід враховувати при оцінці їх безпеки.
- Функції та завдання: огляд також включає аналіз функцій та завдань, які виконуються системами промислового управління. Це може включати збір та обробку

даних про виробництво, керування процесами виробництва, моніторинг та діагностику пристроїв, інтеграцію з іншими системами та багато іншого.

- Загрози та вразливості: під час огляду важливо враховувати потенційні загрози та вразливості, які можуть впливати на системи промислового управління. Це можуть бути кібератаки, недбалість персоналу, технічні несправності, природні лиха та інші фактори.
- Рекомендації забезпечення безпеки: на основі огляду систем промислового управління розробляються рекомендації забезпечення їх безпеки. Це може включати рекомендації з контролю доступу, захисту мережі, моніторингу та журналювання, управління інцидентами та багато іншого.

Загрози та вразливості: стандарт надає огляд загроз та вразливостей, які можуть впливати на системи промислового управління, включаючи кібератаки, внутрішні загрози, природні лиха та інші. В стандарті можна виділити наступні принципи:

- Кібератаки: це можуть бути атаки з використанням шкідливих програм, таких як віруси, черви, троянці, шпигунське програмне забезпечення або вимагачі, спрямовані на порушення функціонування або викрадення конфіденційної інформації систем промислового управління.
- Фізична безпека: це може включати можливість фізичного доступу до обладнання та інфраструктури ICS, якщо пристрої не знаходяться в безпечному середовищі або не захищені від несанкціонованого доступу.
- Технічні вразливості: це може охоплювати програмні та апаратні вразливості, які можуть бути використані зловмисниками для зламу або маніпуляції системами промислового управління.
- Недостатність заходів безпеки: це може включати в себе недостатню аутентифікацію, авторизацію та аудит систем, відсутність мережевих меж та ізоляції, недостатню захист від витоку даних тощо.

- Недбалість персоналу: недостатні освіченість та навички персоналу можуть призвести до неправильного використання або налагодження систем, що може стати причиною безпекових проблем.

Захисні заходи та керівництво забезпеченням безпеки: Документ включає рекомендації з впровадження заходів забезпечення безпеки для захисту систем промислового управління від загроз. Це включає контроль доступу, захист мережі, моніторинг та журналювання, управління інцидентами та багато іншого.

- Аутентифікація та авторизація: встановлення механізмів аутентифікації користувачів та пристроїв, щоб переконатися у їхній ідентичності перед наданням доступу до систем. Авторизація визначає, які ресурси та функції можуть бути доступні після успішної аутентифікації.
- Шифрування даних: застосування шифрування для захисту конфіденційної інформації під час передачі через мережу або зберігання на пристроях.
- Мережеві заходи безпеки: встановлення брандмауерів, систем виявлення вторгнень (IDS), систем запобігання вторгненням (IPS) та інших засобів для моніторингу та захисту мережевого трафіку.
- Фізична безпека: забезпечення фізичного захисту інфраструктури ICS, такого як обладнання, серверні кімнати, комутаційні центри та інші важливі об'єкти.
- Аудит та моніторинг: проведення регулярного аудиту безпеки та моніторингу подій у системах промислового управління для виявлення аномальної активності та інцидентів безпеки.
- Управління життєвим циклом безпеки: використання стратегій та процесів управління життєвим циклом безпеки, таких як розробка, реалізація, управління змінами, оцінка ризиків та вдосконалення, щоб забезпечити безпеку на всіх етапах розвитку систем.

- Навчання та свідомість персоналу: навчання персоналу щодо безпекових практик та процедур, а також створення свідомості про кібербезпеку серед всього персоналу організації.

Планування та управління безпекою: NIST SP 800-82 рекомендує впровадити процеси планування, розробки політик та процедур, а також управління безпекою в рамках систем промислового управління.

- Оцінка ризиків: першим кроком у плануванні безпеки є визначення потенційних загроз та вразливостей, а також оцінка можливих наслідків цих загроз для системи промислового управління. Оцінка ризиків допомагає ідентифікувати ключові області, де необхідні заходи забезпечення безпеки.
- Розробка стратегії безпеки: на основі результатів оцінки ризиків створюється стратегія безпеки, яка визначає цілі, пріоритети та напрями дій для запобігання загрозам та зменшення вразливостей. Ця стратегія повинна відповідати конкретним потребам та характеристикам системи промислового управління.
- Впровадження та виконання заходів безпеки: після розробки стратегії безпеки необхідно впровадити та виконати конкретні заходи, спрямовані на запобігання загрозам та захист системи. Це може включати встановлення технічних засобів безпеки, впровадження політик та процедур безпеки, а також навчання персоналу.
- Моніторинг та аудит безпеки: план безпеки повинен включати механізми моніторингу та аудиту, які дозволяють вчасно виявляти аномальну активність та перевіряти відповідність заходів безпеки з встановленими стандартами та вимогами.
- Постійне удосконалення: план безпеки повинен бути динамічним і постійно адаптуватися до змін у загрозах та умовах довкілля. Це включає періодичну переоцінку ризиків, оновлення стратегій та заходів безпеки, а також навчання персоналу з нових та еволюціонуючих загроз.

Рекомендації щодо архітектури та конфігурації: стандарт також містить рекомендації щодо проектування та конфігурації систем промислового управління з урахуванням безпеки.

- Сегментація мережі: системи промислового управління повинні бути розділені на логічні сегменти або зони з мінімальним рівнем взаємодії між ними. Це допомагає уникнути поширення атак та мінімізувати вплив потенційних інцидентів безпеки.
- Захист доступу до мережі: рекомендується встановлення ефективних механізмів аутентифікації та авторизації для обмеження доступу до мережі та ресурсів промислового управління. Це включає використання сильних паролів, багаторівневих систем авторизації та ідентифікації, а також мережевих файерволів та інших захисних пристроїв.
- Захист передачі даних: рекомендується використання шифрування та інших методів захисту для забезпечення конфіденційності та цілісності даних, що передаються по мережі.
- Конфігураційний контроль: організації повинні встановити процеси для управління конфігураціями систем промислового управління, включаючи регулярне оновлення програмного забезпечення та встановлення захисних налаштувань.
- Моніторинг та аудит безпеки: рекомендується використання систем моніторингу та аудиту, що дозволяють виявляти ненормальну активність, ідентифікувати потенційні загрози та реагувати на них.
- Резервне копіювання та відновлення: для запобігання втрати даних та недоступності систем промислового управління від потенційних інцидентів рекомендується регулярне створення резервних копій та встановлення процедур відновлення.

- Фізична безпека: крім захисту від кіберзагроз, важливо також забезпечити фізичну безпеку систем промислового управління, включаючи захист від несанкціонованого доступу до обладнання та інфраструктури.

Захист інформаційних систем в промисловості має свої специфічні особливості через унікальні вимоги і потреби цього сектору. Деякі з найбільш важливих вимог щодо захисту інформаційних систем в промисловості [17]:

1) Стійкість до фізичних впливів: індустріальні системи зазвичай працюють в середовищах з підвищеним ризиком фізичних впливів, таких як висока вологість, пил, вібрації тощо. Вимоги до захисту інформаційних систем включають установку відповідного обладнання, яке може працювати в таких умовах, та забезпечення надійного захисту від фізичних пошкоджень.

2) Захист від кіберзагроз: промислові системи, зокрема системи управління, стають все більш піддаються кіберзагрозам через збільшену кількість підключених пристроїв та застосування відкритих мереж. Вимоги щодо захисту включають в себе використання захисту від відомих вразливостей, мережевого моніторингу, регулярне оновлення програмного забезпечення та впровадження механізмів виявлення та реагування на інциденти безпеки.

3) Забезпечення безпеки даних: у промисловості часто використовуються важливі та конфіденційні дані, такі як дані про виробництво, плани виробництва, конструкторські рішення тощо. Вимоги до захисту даних включають в себе шифрування даних під час зберігання, обмеження доступу до конфіденційної інформації, а також регулярні резервні копії даних.

4) Забезпечення надійності та доступності: у промисловості доступність систем має критичне значення, оскільки будь-який переривання в роботі може призвести до серйозних фінансових втрат та ризиків для безпеки. Вимоги до захисту включають в себе застосування механізмів резервного копіювання та відновлення, моніторингу доступності систем та швидкого відновлення після інцидентів.

5) Відповідність нормативно-правовим вимогам: багато секторів промисловості мають строгі вимоги щодо безпеки та захисту інформації, які встановлені регуляторними органами або стандартами галузі. Вимоги до захисту включають в себе виконання цих нормативних вимог та регулярне аудитування для підтримки відповідності.

Стандарт ISA/IEC 62443 розроблений спеціально для промислових систем, проте багато з його принципів та підходів можна застосувати для оцінки захищеності інших типів систем. Багато основних принципів та методів, використаних у стандарті, такі як ідентифікація загроз, визначення вразливостей, оцінка ризиків, розробка стратегій захисту та реагування на інциденти, можна успішно застосовувати в інших сферах. Оцінка та управління ризиками є ключовими складовими стандарту, і цей підхід може бути застосований для будь-якого типу системи, де потрібно визначити та зменшити ризики безпеки [18, 19].

1.1.5 C2M2

Стандарт C2M2 (Cybersecurity Capability Maturity Model) – це модель оцінки зрілості кібербезпеки, розроблена для допомоги організаціям у визначенні та вдосконаленні своїх кібербезпекових можливостей. Основна мета C2M2 полягає в тому, щоб допомогти організаціям зрозуміти, наскільки ефективно вони використовують свої ресурси і процеси кібербезпеки, та надати їм методологію для поетапного вдосконалення [20].

Основні складові стандарту C2M2 включають наступне:

- Домени кібербезпеки: C2M2 визначає набір доменів кібербезпеки, які охоплюють широкий спектр кібербезпечних аспектів, таких як управління доступом, захист інформації, моніторинг, реагування на інциденти тощо.

- Рівні зрілості: для кожного домену кібербезпеки визначається шкала зрілості, що дозволяє оцінити, на якому рівні знаходиться організація у відповідному аспекті кібербезпеки. Зазвичай ця шкала включає п'ять рівнів, від базового до оптимального.
- Компоненти зрілості: для кожного рівня зрілості визначаються конкретні компоненти або характеристики, які характеризують організацію на цьому рівні. Це допомагає зрозуміти, що саме потрібно покращити для переходу на вищий рівень зрілості.
- Модель оцінки: C2M2 надає методику для проведення оцінки зрілості кібербезпеки, яка включає в себе опис процесу оцінки, методи збору даних і визначення рівнів зрілості.

Загальна ідея C2M2 полягає в тому, щоб організація могла визначити свій поточний рівень зрілості в галузі кібербезпеки, ідентифікувати області для покращення та розробити план дій для досягнення більш високих рівнів кібербезпеки. Це дає змогу організаціям систематично вдосконалювати свої можливості кібербезпеки і забезпечувати ефективний захист від кіберзагроз [21-22].

1.1.6 ITIL

Стандарт ITIL (Information Technology Infrastructure Library) у контексті кібербезпеки надає фреймворк для ефективного управління IT-сервісами та інфраструктурою, включаючи аспекти кібербезпеки [23]. Основна мета ITIL – це забезпечити надійне функціонування IT-сервісів та захист від потенційних загроз безпеці.

У контексті кібербезпеки ITIL може включати наступні аспекти [24]:

- Управління ризиками: ITIL надає рамки для ідентифікації, аналізу та управління ризиками, пов'язаними з IT-сервісами, включаючи потенційні кіберзагрози.

- Інцидентний менеджмент: ITIL надає процеси для ефективного виявлення, відповіді та відновлення від кіберінцидентів, включаючи аналіз подій та реагування на них.
- Проактивне моніторинг і захист: ITIL рекомендує встановлення механізмів моніторингу та захисту, які дозволяють виявляти та запобігати кіберзагрозам на ранніх стадіях.
- Управління змінами: ITIL включає процеси для керування змінами в IT-інфраструктурі з метою запобігання можливим кіберінцидентам та забезпечення безпеки під час внесення змін.
- Управління доступом: ITIL рекомендує встановлення правильних процедур та контролів доступу до систем та даних для забезпечення конфіденційності та цілісності інформації.

Загалом, ITIL допомагає організаціям ефективно впоратися з кіберзагрозами та забезпечити безпеку IT-сервісів шляхом впровадження стандартизованих процесів та практик управління [25, 26].

1.1.7 ISO 27001

ISO 27001 – це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою у організації. Його основна мета – забезпечити ефективний управлінський підхід до захисту конфіденційної інформації, такої як клієнтська інформація, власні дані компанії, технічна інформація тощо [27].

Методологія оцінки захищеності за ISO 27001 ґрунтується на наступних етапах [28]:

1. Розуміння потреб із захисту інформації: цей етап включає в себе ідентифікацію всіх видів конфіденційної інформації, яка обробляється, зберігається та передається в

організації. Також проводиться оцінка ризиків, що означає визначення потенційних загроз безпеці, вразливостей та потенційних наслідків їх реалізації.

2. Розробка політики інформаційної безпеки: на цьому етапі формулюються загальні принципи, цілі та вимоги щодо захисту інформації. Визначається відповідальність за реалізацію політики та механізми забезпечення її виконання.

3. Визначення області застосування: цей етап визначає, на якій частині організації буде застосовуватися система управління інформаційною безпекою. Встановлюються межі, що визначають обсяг і відповідальність за інформаційну безпеку.

4. Здійснення ризик-аналізу і створення плану керування ризиками: на цьому етапі відбувається виявлення і оцінка ризиків для інформації та інформаційних систем. Розробляється план керування ризиками, який включає в себе вибір і реалізацію відповідних контролів безпеки.

5. Вибір відповідних контролів і заходів безпеки: на цьому етапі обираються конкретні технічні, організаційні та адміністративні заходи безпеки для зменшення ризиків до прийнятного рівня. Розробляються та впроваджуються процедури та політики із захисту інформації.

6. Впровадження заходів безпеки і створення системи управління інформаційною безпекою: на цьому етапі відбувається реалізація обраних контролів безпеки та створення необхідних структур і процедур для управління інформаційною безпекою.

7. Моніторинг, аудит і постійне вдосконалення: цей етап передбачає проведення систематичних оцінок ефективності системи управління інформаційною безпекою, а також внутрішніх і зовнішніх аудитів для перевірки відповідності вимогам ISO 27001. На основі результатів оцінок і аудитів система постійно вдосконалюється.

Впровадження ISO 27001 може принести організації ряд переваг, таких як:

- Підвищення рівня захисту інформаційних активів;
- Підвищення довіри клієнтів та партнерів;
- Ефективне управління ризиками;

- Покращення загальної продуктивності.

Важливо зазначити, що ISO 27001 – це не жорсткий набір правил, а гнучкий стандарт, який можна адаптувати до потреб будь-якої організації. Впровадження ISO 27001 може потребувати значних ресурсів та часу, але воно може допомогти організаціям значно покращити свій рівень кібербезпеки та захистити свої інформаційні активи [29, 30].

1.2 Теоретичні аспекти оцінки захищеності інформаційних систем

1.2.1 Підходи та методи

Існує багато різних підходів та ще більше різноманітних методів оцінки захищеності ІС. Можна виділити чотири основних, найбільш поширених підходи [33].

1.2.1.1 Системний підхід

Системний підхід до оцінки захищеності інформаційних систем базується на розгляді інформаційної системи як цілісної системи, що складається з взаємопов'язаних компонентів. Цей підхід передбачає кілька ключових етапів:

1. Визначення цілей оцінки: ця стадія передбачає чітке сформулювання цілей та завдань оцінки. Наприклад, цілі можуть включати в себе виявлення та оцінку ризиків інформаційної безпеки, перевірку відповідності стандартам та нормам, а також визначення пріоритетів для покращення захищеності.

2. Визначення об'єкта оцінки: об'єктом оцінки може бути вся інформаційна система або її окремі компоненти, такі як апаратне та програмне забезпечення, мережева інфраструктура, системи зберігання та обробки даних, а також персонал та його обізнаність у питаннях кібербезпеки.

3. Структуризація об'єкта оцінки: на цьому етапі об'єкт оцінки розбивається на менші, більш керовані підсистеми та компоненти. Створюється ієрархічна структура, яка відображає взаємозв'язки між компонентами.

4. Вибір методів оцінки: для кожного компонента обираються відповідні методи оцінки, залежно від його специфіки та цілей оцінки. Можливі методи включають аналіз документації, сканування вразливостей, тестування проникнення, аналіз журналів, опитування персоналу, моделювання загроз та аналіз ризиків.

5. Проведення оцінки: застосування обраних методів до кожного компонента інформаційної системи і ретельне документування результатів оцінки та виявлених проблем.

6. Аналіз результатів: проведення комплексної оцінки результатів, виявлення закономірностей та тенденцій, визначення критичних ризиків та вразливостей.

7. Розробка рекомендацій: на основі результатів оцінки розробляється план дій щодо покращення захищеності інформаційної системи. План включає конкретні рекомендації щодо усунення виявлених проблем та вдосконалення системи кібербезпеки.

1.2.1.2 Комплексний підхід

Комплексний підхід до оцінки захищеності інформаційних систем передбачає використання різних методів та інструментів для отримання максимально повної картини стану захищеності. Ось деякі з них:

Аналіз документації: цей метод полягає у вивченні документації, що описує інформаційну систему, її компоненти та політики безпеки. Це може включати перегляд технічної документації, процедур безпеки, архітектури системи та інших важливих документів.

Сканування вразливостей: цей метод включає автоматизоване виявлення вразливостей в інформаційній системі, таких як слабкі точки у програмному забезпеченні, налаштування мережевих пристроїв тощо.

Тестування проникнення: цей метод передбачає спробу проникнути в інформаційну систему з метою виявлення несанкціонованого доступу. Тестування може включати в себе спроби зламати паролі, отримати несанкціонований доступ до системи або витягнути конфіденційну інформацію.

Аналіз журналів: цей метод полягає у вивченні журналів інформаційної системи для виявлення підозрілих дій або подій, які можуть вказувати на потенційні загрози безпеці.

Опитування персоналу: цей метод включає опитування співробітників, які використовують інформаційну систему, щодо їхніх знань та дотримання правил безпеки. Це дозволяє отримати інформацію про поведінку персоналу та їхню усвідомленість щодо кібербезпеки.

Комбінація цих методів дозволяє отримати більш глибоке та всебічне розуміння стану захищеності інформаційної системи. Наприклад, можна скористатися аналізом документації разом із скануванням вразливостей та тестуванням проникнення для отримання комплексної оцінки рівня безпеки системи.

Переваги такого комплексного підходу включають більш глибоке та всебічне розуміння стану захищеності інформаційної системи, можливість виявлення проблем, які можуть бути пропущені при використанні лише одного методу, а також підвищення надійності та достовірності результатів оцінки.

1.2.1.3 Кількісний підхід

Кількісний підхід до оцінки захищеності інформаційних систем базується на використанні математичних методів для об'єктивної оцінки ризиків та визначення рівня

захищеності. Цей підхід дозволяє виявляти потенційні загрози, оцінювати їхні наслідки та визначати ефективні заходи для зменшення ризиків.

Методи кількісної оцінки:

1. Моделювання загроз.

Цей метод передбачає створення моделей, які описують можливі загрози для інформаційної системи та їхню ймовірність. Важливо враховувати різноманітність потенційних загроз, їхні наслідки та ймовірність виникнення.

2. Аналіз ризиків.

Проводиться оцінка ймовірності виникнення кожної загрози та її впливу на інформаційну систему. Використовуються різноманітні методи аналізу, включаючи статистичні дані, експертні оцінки та історичні дані про інциденти.

3. Розрахунок рівня захищеності.

На основі оцінки ризиків визначається загальний рівень захищеності інформаційної системи. Цей рівень може відображати ймовірність вразливості системи, ступінь ефективності захисних заходів та загальний ризик для організації.

4. Метод оцінки впливу (Impact Assessment).

Цей метод фокусується на оцінці потенційних збитків, які може завдати інформаційна система певна загроза. Для визначення впливу загрози можуть використовуватися різні методи, такі як аналітичні моделі, експертні оцінки та сценарії "що якби". Цей метод дозволяє ідентифікувати критичні активи інформаційної системи та встановлювати пріоритети для їхнього захисту.

5. Метод аналізу витрат-вигод (Cost-Benefit Analysis).

Цей метод оцінює економічну доцільність інвестицій у заходи з кібербезпеки. Він порівнює витрати на реалізацію цих заходів з очікуваними вигодами, такими як запобігання збиткам від кібератак. Цей аналіз дозволяє приймати обґрунтовані рішення щодо розподілу ресурсів для кібербезпеки та визначення оптимальних стратегій інвестування.

6. Метод моделювання ризиків (Risk Modeling).

Цей метод використовує математичні моделі для прогнозування ймовірності та наслідків кібератак. Він дозволяє оцінити загальний рівень ризику для інформаційної системи та визначити критичні ризики, що можуть призвести до серйозних наслідків для організації. Моделювання ризиків також може використовуватися для розробки стратегій та планів реагування на кіберінциденти.

7. Метод оцінки зрілості (Maturity Assessment).

Цей метод оцінює рівень зрілості системи кібербезпеки організації. Він використовує моделі або еталонні моделі для оцінки ефективності політик, процедур та практик кібербезпеки. Оцінка зрілості дозволяє визначити сильні та слабкі сторони системи кібербезпеки та намітити шляхи її вдосконалення.

8. Метод бенчмаркінгу (Benchmarking).

Цей метод порівнює рівень захищеності інформаційної системи з іншими системами або галузевими стандартами. Він дозволяє визначити, наскільки добре інформаційна система захищена порівняно з іншими.

1.2.1.4 Якісний підхід

Якісний підхід до оцінки захищеності ІС використовує описові методи для оцінки рівня захищеності ІС. Цей підхід може включати наступні методи:

1. Експертна оцінка.

Експертна оцінка передбачає залучення фахівців в галузі кібербезпеки для проведення оцінки захищеності інформаційної системи. Ці експерти можуть мати значний досвід у виявленні потенційних загроз, аналізі вразливостей та розробці стратегій захисту. Вони використовують свої знання та досвід для ідентифікації потенційних проблем та ризиків, що можуть виникнути в інформаційній системі, та рекомендують заходи для їх запобігання або пом'якшення.

2. Аналіз політик безпеки.

Аналіз політик безпеки полягає у вивченні існуючих політик безпеки інформаційної системи та їх порівнянні з кращими практиками в галузі кібербезпеки. Цей процес допомагає виявити прогалини або недоліки в політиках безпеки, такі як відсутність або недостатня чіткість вимог щодо паролів, доступу до даних чи застосування шифрування. На основі результатів аналізу можуть бути запропоновані рекомендації з покращення політик безпеки для забезпечення вищого рівня захищеності інформаційної системи.

3. Оцінка культури безпеки.

Оцінка культури безпеки визначає наскільки свідомі працівники організації ризики кібербезпеки та наскільки дотримуються вони правил безпеки. Цей процес може включати проведення анкетування співробітників щодо їхніх знань про потенційні загрози, проведення навчань з кібербезпеки та аналіз внутрішньої культури організації щодо безпеки даних. Результати оцінки дозволяють виявити слабкі місця в культурі безпеки та розробити стратегії для їх вдосконалення, що сприятиме підвищенню рівня захищеності інформаційної системи.

1.2.2 Індикатори та метрики захищеності

Індикатори захищеності – це метрики, які використовуються для оцінки рівня захищеності інформаційної системи від кіберзагроз. Їх можна класифікувати за різними критеріями, щоб чітко структурувати та систематизувати індикатори.

1.2.2.1 Класифікація індикаторів захищеності

Класифікація за типом:

Індикатори, пов'язані з аутентифікацією оцінюють ефективність методів аутентифікації, які використовуються для доступу до ІС, наприклад, складність паролів,

використання багатофакторної аутентифікації, наявність блокування облікових записів після кількох невдалих спроб входу.

Індикатори, пов'язані з доступом оцінюють контроль доступу до ІС, наприклад, наявність матриці дозволів, використання принципів найменшого привілею, моніторинг активності користувачів.

Індикатори, пов'язані з конфіденційністю оцінюють захист конфіденційних даних, наприклад, шифрування даних у стані спокою та під час передачі, контроль доступу до даних, навчання персоналу щодо захисту даних.

Індикатори, пов'язані з цілісністю оцінюють захист даних від несанкціонованого змінення або видалення, наприклад, використання контрольних сум, резервне копіювання даних, моніторинг змін даних.

Індикатори, пов'язані з доступністю оцінюють стійкість ІС до збоїв та відмов, наприклад, резервування обладнання та програмного забезпечення, план відновлення після аварій, тестування на стійкість до відмов.

Індикатори, пов'язані з управлінням ризиками оцінюють процес управління ризиками кібербезпеки в організації, наприклад, наявність політики управління ризиками, проведення оцінки ризиків, впровадження заходів з пом'якшення ризиків.

Індикатори, пов'язані з реагуванням на інциденти оцінюють здатність організації реагувати на кіберінциденти, наприклад, наявність плану реагування на інциденти, час виявлення та реагування на інциденти, навчання персоналу щодо реагування на інциденти.

Індикатори, пов'язані з відповідністю (комплаєнсом) оцінюють відповідність ІС стандартам та нормативним актам з кібербезпеки, наприклад, ISO 27001, PCI DSS, GDPR [34-36].

Індикатори, пов'язані з моніторингом оцінюють ефективність моніторингу ІС на наявність кіберзагроз, наприклад, наявність системи моніторингу безпеки, аналіз журналів, тестування на проникнення.

1.2.2.2 Огляд та узагальнення індикаторів захищеності

В результаті аналізу вищенаведених джерел можна виділити наступні загальні індикатори захищеності:

Архітектура системи – оцінка структури системи, конфігурації та розподілу компонентів, включаючи сервери, мережеві пристрої, бази даних та клієнтське програмне забезпечення.

Управління ідентифікацією та автентифікацією – оцінка механізмів контролю доступу, використання сильних паролів, багаторівневої аутентифікації та інших методів ідентифікації користувачів.

Шифрування даних – оцінка використання шифрування для захисту конфіденційності даних в спокої та під час транзиту через мережу.

Заходи захисту мережі – оцінка використання брандмауерів, виявлення вторгнень, VPN та інших технологій для захисту мережевої інфраструктури.

Моніторинг та аналіз безпеки – оцінка систем моніторингу безпеки, виявлення вторгнень, аналізу журналів подій та інших засобів для виявлення та реагування на загрози.

Захист даних від програмних вразливостей – оцінка заходів для запобігання використанню програмних вразливостей, таких як SQL-ін'єкції, переповнення буфера, кросс-сайтові скрипти тощо.

Резервне копіювання та відновлення даних – оцінка наявності та ефективності процесів резервного копіювання та відновлення для забезпечення надійності та доступності даних.

Аудит та відповідність – оцінка виконання аудиту безпеки, забезпечення відповідності нормативним вимогам, таким як GDPR, HIPAA, PCI DSS тощо.

Стійкість до відмови – оцінка механізмів та процедур для запобігання, виявлення та відновлення від інцидентів відмови в системі.

Управління кризовими ситуаціями – оцінка наявності та ефективності процедур для керування кризовими ситуаціями та відновлення бізнес-процесів після інцидентів.

Рівень актуалізації та патчів програмного забезпечення та операційних систем – оцінка регулярності та ефективності процесів оновлення програмного забезпечення та операційних систем для виправлення відомих вразливостей.

Наявність та ефективність застосованих заходів безпеки – оцінка використання та ефективності антивірусного програмного забезпечення, фаєрволів, систем виявлення вторгнень та інших заходів для захисту інформаційних систем.

Рівень контролю доступу та ідентифікації користувачів – оцінка рівня контролю доступу до ресурсів інформаційної системи, використання багаторівневих методів аутентифікації та ідентифікації користувачів для забезпечення конфіденційності та цілісності даних.

Реагування на інциденти та відновлення – оцінка наявності та ефективності процедур управління інцидентами та відновлення після порушень безпеки, включаючи швидкість реагування та відновлення.

Захист від внутрішніх загроз – оцінка заходів для запобігання та виявлення внутрішніх загроз, таких як несанкціонований доступ співробітників або зловживання привілеями.

Управління конфігураціями – оцінка системи управління конфігураціями для контролю над змінами в інформаційній системі та забезпечення стабільності та безпеки.

Надійність інфраструктури – оцінка надійності та стійкості апаратної та програмної інфраструктури для запобігання відмов та забезпечення безперебійної роботи.

Управління життєвим циклом безпеки – оцінка процесів управління безпекою протягом усього життєвого циклу системи, включаючи планування, розробку, впровадження, експлуатацію та відновлення.

Культура безпеки – оцінка наявності та ефективності програм та ініціатив з підвищення культури безпеки серед персоналу, включаючи навчання та свідомість про безпеку.

Партнерські відносини та постачальники – оцінка заходів для забезпечення безпеки у взаємодії з постачальниками, партнерами та зовнішніми сторонами, які мають доступ до системи або даних.

Постійне вдосконалення – оцінка процесів вдосконалення системи безпеки на основі аналізу інцидентів, вразливостей та навчальних заходів.

Планування кризових ситуацій та управління ризиками – оцінка планів кризового реагування та процесів управління ризиками для ідентифікації та зменшення потенційних загроз.

1.2.3 Оцінка ризиків в інформаційній безпеці та їх вплив на оцінку захищеності

Оцінка ризиків – це невід'ємна частина процесу оцінки захищеності інформаційних систем. Вона дозволяє:

- Виявити та ідентифікувати потенційні загрози для ІС.
- Оцінити ймовірність та наслідки реалізації цих загроз.
- Прийняти обґрунтовані рішення щодо пріоритетності заходів з кібербезпеки.
- Розробити план дій з покращення захищеності ІС.

Оцінка ризиків в інформаційній безпеці є ключовим етапом у процесі забезпечення безпеки даних. Для проведення оцінки ризиків в інформаційній безпеці використовуються різні методи та підходи. Один із найпоширеніших підходів – це аналіз ризиків, що базується на ідентифікації потенційних загроз, вразливостей і наслідків

інцидентів. Цей підхід дозволяє приділити увагу найбільш значущим ризикам та прийняти обґрунтовані рішення щодо їх управління.

Оцінка ризиків також передбачає визначення заходів та стратегій для мінімізації чи усунення виявлених ризиків. Це може включати в себе розробку політик безпеки, впровадження технічних заходів захисту, навчання персоналу та створення планів реагування на інциденти [37].

Загальна оцінка ризиків в інформаційній безпеці значно впливає на оцінку захищеності інформаційної системи. Чим вищий рівень ризику, тим більші заходи необхідно прийняти для забезпечення адекватного рівня захисту. Таким чином, ретельний аналіз ризиків дозволяє ефективно керувати безпекою інформації та запобігати можливим загрозам для організації.

Оцінка ризиків не лише дає чітке розуміння рівня загроз, але й стає потужним інструментом для прийняття обґрунтованих рішень, оптимізації ресурсів, покращення комунікації та досягнення загальної стійкості ІС до кібернетичних загроз.

Завдяки оцінці ризиків стає можливим чітко виділити ті загрози, які становлять найбільшу небезпеку для інформаційної системи. Це дозволяє сфокусувати ресурси та зусилля на нейтралізації саме цих критичних ризиків, максимально підвищуючи загальний рівень захищеності. На основі оцінки ризиків можна чітко ранжувати необхідні заходи з кібербезпеки за їхньою важливістю та ефективністю. Це дозволяє оптимізувати розподіл ресурсів, спрямовуючи їх на ті заходи, які дають найкращу віддачу від інвестицій і гарантують максимальний захист від найімовірніших та найнебезпечніших загроз [39].

Оцінка ризиків забезпечує чітку та обґрунтовану базу для прийняття рішень щодо кібербезпеки. Це дозволяє керівництву та відповідальним особам чітко пояснювати та аргументувати свої дії, ґрунтуючись на даних та аналітиці, а не на інтуїції чи особистих думках. Оцінка ризиків – це не статичний процес. Вона повинна проводитися регулярно, щоб враховувати зміни в ІС, появу нових загроз та вдосконалення методів

кіберзлочинності. Це дозволяє динамічно адаптувати систему кібербезпеки до мінливих умов та підтримувати її стійкість на належному рівні.

Завдяки чіткій картині ризиків та пріоритетів стає можливим економно витрачати ресурси, спрямовуючи їх на ті заходи, які дійсно дають результат. Це запобігає неефективному розподілу коштів та зусиль, максимізуючи віддачу від інвестицій у кібербезпеку. Оцінка ризиків створює спільну мову для всіх учасників процесу кібербезпеки, даючи чітке розуміння рівня загроз та пріоритетних завдань. Це покращує комунікацію між різними відділами та рівнями управління, гарантуючи скоординовану та ефективну роботу всієї команди з кібербезпеки. Прозорість та обґрунтованість оцінки ризиків сприяє підвищенню довіри до системи кібербезпеки з боку керівництва, співробітників та клієнтів. Це створює атмосферу впевненості та спокою, що позитивно впливає на загальну продуктивність та репутацію організації. Оцінка ризиків є важливим елементом для досягнення відповідності стандартам та нормам кібербезпеки. Вона надає чітке уявлення про те, наскільки ІС відповідає встановленим вимогам, та допомагає виявити та усунути недоліки, які можуть призвести до штрафів або інших санкцій.

Висновки за розділом 1

В першому розділі роботи детально проаналізовано існуючі методи та підходи до оцінки захищеності різних типів інформаційних систем, включаючи NIST CSF, NISF SP 800-82, C2M2, ITIL, ISO 27001, ISA/IEC 62443, ISO 15408. Було розглянуто існуючі дослідження в цій галузі, як міжнародні, так і українські. За результатами аналізу можна виділити наступні висновки: не існує універсального підходу до оцінки захищеності ІС, який би підходив всім організаціям. Організаціям слід вибирати підхід до оцінки захищеності, який відповідає їхнім потребам, ресурсам та рівню ризиків. Використання індикаторів захищеності може допомогти організаціям чітко структурувати та систематизувати інформацію про рівень захищеності ІС.

Також в розділі розглянуто індикатори захищеності інформаційних систем – метрики, які використовуються для оцінки рівня захищеності інформаційної системи від кіберзагроз. Було запропоновано категоризацію індикаторів, виділено та узагальнено конкретні загальні індикатори.

Поставлено наступні задачі дослідження:

1. Аналіз індикаторів та метрик оцінки захищеності інформаційних систем
2. Створити структурований опис потенційних загроз для інформаційної системи.
3. Розробка моделі оцінки захищеності інформаційних систем.
4. Аналіз адекватності запропонованого рішення.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛЕЙ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Модель загроз — це інструмент, який використовується для ідентифікації, класифікації та аналізу потенційних загроз інформаційним системам або даним. Вона допомагає зрозуміти, які загрози можуть вплинути на інформаційні ресурси та якими шляхами вони можуть використовуватися для атак [43].

2.1 Методи побудови моделей загроз

Моделювання загроз – це процес, що охоплює широкий спектр систем організації, включаючи бізнес-процеси, інформаційні системи, мережеву інфраструктуру, розподілені підсистеми, додатки, сервіси, програмний код та інше. Цей процес може бути виконаний на будь-якій стадії розробки, але переважно проводиться на ранній стадії, щоб його результати могли допомогти при розробці проекту і зменшити витрати.

Моделювання загроз – це не лише виявлення потенційних загроз, але й розробка моделі шляхом ітеративної оцінки вразливостей в системі. Ця модель допомагає виявляти, повідомляти і розуміти загрози та заходи щодо їх зниження в контексті захисту критичних ресурсів. Під час моделювання загроз важливо враховувати різноманітні сценарії та методи нападу, щоб отримати повний образ потенційних загроз і їх впливу на систему.

Один з ключових аспектів моделювання загроз – це визначення і аналіз вразливостей в системі. Це дозволяє ідентифікувати слабкі місця в системі, які можуть бути використані зловмисниками для атаки. Додатково, моделювання загроз допомагає встановити пріоритети щодо захисту цих вразливостей, визначити потенційні втрати та ризики для організації та розробити стратегії для їх зменшення.

Застосування моделювання загроз включає в себе різноманітні методи та інструменти, такі як аналіз вразливостей, сканування безпеки, тестування на проникнення, аналіз шляхів нападу та інші. Ці методи допомагають створити повну картину загроз для системи і розробити ефективні заходи для її захисту.

Існує багато методів модулювання, але варто сфокусуватись на основних, найбільш поширених.

2.1.1 STRIDE

STRIDE – модель визначення загроз комп’ютерній безпеці, розроблена компанією Microsoft у 1999 році. Цей метод ґрунтується на шести категоріях загроз, які охоплюють широкий спектр можливих атак [44]:

1. Spoofing (підміна): це загроза, пов'язана з можливістю атакуючого незаконно представлятися іншою особою або системою. Наприклад, атака типу "підробка логіна" (spoofing attack) може дозволити зловмиснику неавторизовано отримати доступ до системи, підміняючи свій ідентифікатор.

2. Tampering (фальсифікація): ця категорія відноситься до можливості атакуючого модифікувати дані або програмне забезпечення в системі. Наприклад, атака, спрямована на фальсифікацію даних у базі даних або зміну вихідного коду програми, щоб внести уразливості.

3. Repudiation (відмова від відповідальності): ця категорія описує ситуації, коли атакувач може виконувати дії в системі, а потім заперечувати свою причетність до них. Наприклад, атака, яка дозволяє зловмиснику здійснити фінансові операції, а потім заперечувати, що вони були вчинені або приховати неавторизовані дії.

4. Information Disclosure (розголошення інформації): такі загрози стосуються можливості незаконного доступу до конфіденційної інформації. Наприклад, атака, яка

призводить до розголошення особистих даних користувачів або конфіденційної корпоративної інформації.

5. Denial of Service (відмова в обслуговуванні): ця категорія відноситься до атак, спрямованих на знищення або обмеження доступності ресурсів системи. Наприклад, атака, яка перевантажує сервер або мережу, щоб запобігти законному доступу користувачів.

6. Elevation of Privilege (підняття привілеїв): ця категорія відноситься до загроз, пов'язаних зі спробами атакуючих отримати більші привілеї, ніж вони мають у системі, щоб отримати доступ до обмежених ресурсів або функцій.

Модель STRIDE має наступні переваги [45]:

- Простота: STRIDE ґрунтується на шести простих та зрозумілих категоріях загроз, що робить його доступним для користувачів з різним рівнем технічної підготовки.
- Всебічність: STRIDE охоплює широкий спектр можливих атак, що дозволяє виявити та оцінити широкий спектр ризиків.
- Ефективність: STRIDE можна використовувати для швидкого та ефективного аналізу загроз, що робить його цінним інструментом для команд з кібербезпеки.

Найбільшим недоліком цього методу є суб’єктивність оцінки – моделювання загроз повністю покладено на експертну думку.

2.1.2 Дерева атак

Дерева атак (Attack Trees) – це метод побудови моделей загроз, який використовує деревоподібну структуру для представлення потенційних атак на систему. Цей метод був розроблений в рамках теорії ігор та криптографії та знаходить широке застосування в області інформаційної безпеки [46].

Основна ідея дерев атак полягає в тому, щоб візуалізувати всі можливі шляхи атаки, які можуть використовувати зловмисники для проникнення в систему. Дерево складається з вузлів та ребер. Кожен вузол представляє певну атаку або етап атаки, а ребро показує зв'язок між різними етапами атаки [47].

В цілому, структура дерева атак виглядає наступним чином:

- Корінь: корінь дерева представляє загальну мету атаки, наприклад, отримання несанкціонованого доступу до системи або витік конфіденційної інформації.
- Вузли: кожен вузол дерева представляє окрему атаку або етап атаки, який може бути виконаний для досягнення загальної мети. Наприклад, вузол може представляти фазу атаки, таку як перехоплення паролів або використання вразливості в програмному забезпеченні.
- Ребра: ребра вказують на зв'язок між різними етапами атаки. Вони показують логічну послідовність дій, необхідних для виконання атаки. Наприклад, ребро може показувати, що успішне виконання одного етапу атаки дозволяє зловмисникові перейти до наступного етапу.
- Листя: листя дерева відображає кінцеві результати атаки, такі як отримання доступу до конфіденційних даних або виконання певної функції зловмисника.

Під час аналізу дерева атак проводиться оцінка ризику кожного вузла. Це дозволяє визначити найбільш критичні етапи атаки та приділити їм пріоритет у плануванні заходів захисту.

Фактори, які беруться до уваги при оцінці ризик це потенційний збиток, ймовірність успіху, легкість реалізації атаки та наявність ресурсів для атаки.

На основі оцінки ризику кожного вузла розробляються заходи щодо пом’якшення ризику.

Цей метод має низку переваг: візуалізація загроз, систематичність аналізу, оцінка ризику на кожному етапі атаки.

2.1.3 MITRE ATT&CK

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – це фреймворк, який розвивається MITRE Corporation і використовується для моделювання тактик, технік та загальних знань про зловмисні дії [50]. Його ціль – надати відкритий набір знань про те, як зловмисники атакують системи та мережі, щоб організації могли краще розуміти, виявляти та захищатися від цих загроз.

Застосування фреймворка ATT&CK допомагає ідентифікувати різноманітні тактики та техніки, які можуть бути використані зловмисниками для атаки на систему. Це включає тактики, як витіснення (перехід), поширення, виконання, обман та інші, а також конкретні техніки, які використовуються для реалізації цих тактик.

Після ідентифікації тактик та технік за допомогою ATT&CK можна детально проаналізувати, які конкретні вразливості або слабкі місця в системі можуть бути використані зловмисниками для виконання цих атак.

Після ідентифікації загроз та оцінки вразливостей проводиться оцінка ймовірності того, що ці атаки будуть здійснені. Це може включати аналіз історичних даних про подібні інциденти, здатність зловмисників та їх мотивацію, а також оцінку ефективності заходів захисту, які вже впроваджені.

Для кожної ідентифікованої загрози можна провести оцінку потенційного впливу на організацію. Це включає аналіз можливих наслідків в разі вдалого виконання атаки, таких як втрата конфіденційності, цілісності або доступності даних, фінансові втрати, порушення репутації та інші.

На основі оцінок загроз, вразливостей, ймовірності та впливу розробляється стратегія захисту. Це може включати впровадження технологічних та організаційних заходів безпеки, які зменшують ймовірність та вплив атак, а також здатність виявляти, відбивати та відновлюватися від інцидентів.

Інтеграція фреймворка ATT&CK в процес побудови моделі ризику допомагає організаціям краще розуміти загрози, що стикаються з їх системами, та розробляти ефективні стратегії захисту для запобігання та виявлення кібератак.

На додачу до ATT&CK компанією MITRE було розроблено DEF3ND [51] – це ініціатива, яка спрямована на розробку та розгортання моделі захисту мереж та систем. DEFEND є спробою збільшити ефективність захисту мереж та систем, реагуючи на зростаючі загрози кібербезпеки та еволюцію кібератак [52].

DEF3ND надає можливі рішення для пом’якшення та запобігання ризику для кожної тактіки та техніки, які розглядаються в ATT&CK. Поєднання двох підходів дозволяє одночасно визначити ризики та загрози і зрозуміти, які саме методи захисту допоможуть з ними впоратись.

2.2. Визначення та обґрунтування індикаторів та метрик оцінки захищеності

Вибір індикаторів є першим за важливістю елементів моделювання. Невдалий вибір індикаторів унеможливлює отримання якісних та об’єктивних результатів моделювання, оскільки елементи системи будуть не оцінені взагалі або оцінені некоректно.

2.2.1. Обґрунтування вибору індикаторів, що будуть використовуватися в моделюванні

Індикатори повинні бути чітко визначені, вимірювані, об'єктивні та практичні, щоб забезпечити точну та корисну інформацію про рівень ризику.

Вибір індикаторів має базуватись на наступних принципах:

- Цілі оцінки: Які цілі переслідує оцінка? Чи йдеться про визначення загального рівня ризику, виявлення конкретних загроз або порівняння ІС з іншими?

- Специфіка ІС: Які характеристики ІС роблять її унікальною? Які дані та активи потребують захисту?
- Наявні джерела інформації: Які дані доступні для збору та аналізу? Які методи збору даних можна використовувати?
- Вплив на ризик: Індикатори повинні вимірювати фактори, які мають значний вплив на рівень ризику ІС.
- Зв'язок з загрозами: Індикатори повинні бути пов'язані з конкретними загрозами, які були виявлені в процесі моделювання.
- Вимірюваність: Індикатори повинні бути чітко визначені та вимірювані, щоб дані могли бути зібрані та проаналізовані.
- Об'єктивність: Індикатори повинні бути об'єктивними та неупередженими, щоб забезпечити точну оцінку рівня ризику.
- Практичність: Чи можна легко збирати та аналізувати дані для вибраних індикаторів? Чи є це економічно вигідним?
- Важливість ІС: Наскільки важлива ІС для роботи організації? Який вплив матиме збій або витік даних на бізнес?
- Галузеві ризики: Які кіберзагрози є найактуальнішими для галузі, в якій працює організація?
- Нормативні вимоги: Чи існують якісь нормативні вимоги, яким повинна відповідати ІС?
- Ресурси: Які ресурси доступні для моделювання загроз та реалізації заходів з кібербезпеки?
- Апетит до ризику: Який рівень ризику готова прийняти організація?

2.2.2. Визначення цілей

Відповідно до існуючих методів моделювання загроз, найкращих практик галузі та підходів до оцінки захищеності, які були розглянуті у першому розділі роботи, можна виділити наступні цілі моделювання:

- Підвищення стійкості ІС до кіберзагроз: Ця мета може включати зменшення кількості кіберінцидентів, скорочення часу відновлення після інцидентів та покращення здатності ІС протистояти новим та невідомим загрозам.
- Зниження ризику витоку даних: Ця мета може включати захист конфіденційних даних від несанкціонованого доступу, розкриття або використання.
- Забезпечення безперебійної роботи ІС: Ця мета може включати мінімізацію простоїв ІС, захист від відмов в обслуговуванні та забезпечення доступності ІС для користувачів.
- Відповідність нормативним вимогам: Ця мета може включати забезпечення відповідності ІС стандартам та нормам кібербезпеки, встановленими регулятивними органами або галузевими організаціями.
- Підтримка конкурентної переваги: Ця мета може включати захист інтелектуальної власності та комерційної таємниці від кіберзлочинців.

Модель оцінки захищеності інформаційних систем, запропонована в цій роботі ставить на меті всі вищенаведені цілі.

2.2.3 Перелік активів

Активи – це будь-які цінні ресурси, які потрібно захищати в рамках системи або процесу. Визначення переліку активів допомагає ідентифікувати ключові складові системи та їх значення для бізнесу або організації і зменшує ймовірність пропустити деякі складові системи під час моделювання загроз або оцінки захищеності.

В загальному випадку, до переліку активів слід включати:

- Апаратне забезпечення: Сервери, робочі станції, мережеві пристрої, мобільні пристрої тощо.
- Програмне забезпечення: Операційні системи, прикладні програми, бази даних, веб-сайти тощо.
- Дані: Конфіденційна інформація, фінансові дані, особисті дані тощо.
- Інформаційні ресурси: Інформаційні системи, мережі, веб-сайти тощо.

Перелік активів визначається самостійно організацією, яка бажає оцінити рівень захищеності власної системи. Більш точний перелік активів, який має бути врахований у моделі матиме наступний вигляд:

1. Апаратні активи:

- Сервери (фізичні та віртуальні)
- Мережеві пристрої (маршрутизатори, комутатори, брандмауери тощо)
- Робочі станції
- Мобільні пристрої
- Пристрої зберігання даних (HDD, SSD, NAS тощо)
- Інші апаратні компоненти ІС

2. Програмні активи:

- Операційні системи
- Системне програмне забезпечення
- Прикладне програмне забезпечення
- Бази даних
- Веб-сайти та веб-програми
- Інструменти та утиліти

3. Дані:

- Конфіденційні дані (персональні дані, фінансові дані, інтелектуальна власність тощо)

- Неконфіденційні дані (загальнодоступні дані, оперативні дані тощо)
- Структуровані дані (дані в базах даних, таблицях тощо)
- Неструктуровані дані (тексти, зображення, відео тощо)

4. Інформаційні ресурси:

- Веб-сайти
- Мережі
- Системи електронної пошти
- Системи обміну повідомленнями
- Системи дистанційного доступу
- Інші інформаційні ресурси.

2.2.4 Аналіз загроз

Мета аналізу загроз – визначити список потенційних загроз для інформаційних систем. Найбільш практичним способом визначення загроз є детальний розгляд наявних інформаційних активів та виділення всіх можливих загроз для кожного з них. Почнемо з апаратних активів:

1. Фізичні втрати:

Втрата або крадіжка серверів, робочих станцій, мобільних пристроїв та інших апаратних компонентів.

Пошкодження або втрата апаратних пристроїв внаслідок пожежі, повені, землетрусу тощо.

2. Несправність обладнання:

Відмови серверів, мережевих пристроїв або інших апаратних компонентів через неправильну експлуатацію, низьку якість обладнання або технічні проблеми. Перевантаження або перегрів обладнання, що може призвести до відмови.

3. Фізичне пошкодження:

Пошкодження обладнання внаслідок ударів, падінь, впливу вологи, пилу, високої температури тощо.

4. Віруси та шкідливе програмне забезпечення:

Зараження серверів, робочих станцій або мобільних пристроїв вірусами, троянами або іншим шкідливим програмним забезпеченням, що може призвести до втрати даних або недоступності системи.

5. Неавторизований фізичний доступ:

Несанкціонований фізичний доступ до серверних приміщень, дата-центрів або інших місць розташування апаратного обладнання.

6. Проблеми зі зберіганням даних:

Втрата або пошкодження даних на пристроях зберігання, таких як жорсткі диски (HDD), твердотільні накопичувачі (SSD), мережеві пристрої для зберігання (NAS) тощо.

7. Неавторизоване використання:

Використання апаратного обладнання для несанкціонованих цілей, наприклад, для зламу або атак на інші системи або мережі.

Загрози програмним активам:

1. Вразливості програмного забезпечення:

Використання вразливостей в операційних системах, системному програмному забезпеченні або прикладних програмах для здійснення атак на системи.

2. Віруси, черв'яки та троянські коні:

Зараження операційних систем, системного програмного забезпечення або прикладних програм шкідливими програмами, що можуть викликати витік чутливої інформації або втрату контролю над системою.

3. Маніпуляція даними:

Несанкціонований доступ до баз даних або веб-сайтів з метою модифікації, видалення або крадіжки даних.

4. Дефекти в програмному забезпеченні:

Помилки, недоліки або дефекти в операційних системах, системному програмному забезпеченні або прикладних програмах, що можуть призвести до неправильної роботи або витоку інформації.

5. Несанкціонований доступ:

Отримання несанкціонованого доступу до системних адміністративних інструментів або привілегій.

6. Неавторизовані зміни в програмному забезпеченні:

Маніпуляція або зміна програмного забезпечення без відповідних дозволів або авторизації, що може призвести до втрати даних або недоступності сервісів.

7. Втрата доступності веб-сайту:

Атаки на веб-сайти або веб-додатки з метою перешкодити їх роботі або знизити їх доступність для користувачів.

8. Недостатні заходи захисту:

Відсутність або недостатньо ефективні заходи захисту, такі як антивіруси, файрволи, захист від SQL-ін'єкцій, що може призвести до вразливості систем.

9. Використання небезпечних сторонніх компонентів:

Використання сторонніх бібліотек або модулів з відомими вразливостями, що можуть бути використані для атак на систему.

10. Проблеми з конфіденційністю:

Витік конфіденційної інформації через недоліки в системах або додатках, які призводять до незаконного доступу до даних користувачів або конфіденційних даних компанії.

11. Компрометація інфраструктури хмарних сервісів:

Компрометація обчислювальних ресурсів або послуг хмарних сервісів, що призводить до втрати контролю над даними або відмови у послугах.

12. Атаки на віртуальні середовища:

Атаки на віртуальні машини або контейнери, що призводять до втрати конфіденційності, цілісності або доступності даних.

13. Викрадення ідентифікаційних даних:

Викрадення або втрата ідентифікаційних даних, таких як паролі, ключі API або сертифікати, що може призвести до несанкціонованого доступу до систем або послуг.

14. Недостатні заходи моніторингу та аудиту:

Відсутність або недостатньо ефективні засоби моніторингу та аудиту, що може призвести до неспроможності виявлення атак або інцидентів безпеки.

15. DDoS-атаки (Distributed Denial of Service):

Атаки, які спрямовані на перевантаження веб-сайтів або веб-додатків шляхом відправлення великої кількості запитів, що призводить до відмови у послугах для законних користувачів.

16. Недостатні заходи шифрування:

Відсутність або недостатньо ефективні заходи шифрування даних, що може призвести до незаконного доступу до конфіденційної інформації або витоку даних.

17. Небезпечне керування сесіями (Session Management):

Використання недоліків в керуванні сесіями для здійснення атак на ідентифікацію та аутентифікацію користувачів.

18. Недостатнє оновлення програмного забезпечення:

Незабезпечення оновлення або встановлення важливих патчів безпеки, що може призвести до експлуатації відомих вразливостей.

Загрози для даних:

1. Незаконне використання даних:

Використання даних в недозволених цілях, таких як шахрайство, шпигунство або шантаж.

2. Атаки на конфіденційність даних:

Атаки, спрямовані на отримання доступу та / або шифрування конфіденційної інформації для отримання викуп.

3. Неавторизований доступ:

Несанкціонований доступ до даних через порушення прав доступу або використання слабких паролів.

4. Втрата доступності даних:

Атаки на системи зберігання даних, такі як DDoS-атаки або фізичні пошкодження, що можуть призвести до відмови у доступі до даних.

5. Несанкціоноване видалення або зміна даних:

Видалення або модифікація даних без дозволу власника або адміністратора.

6. Соціальна інженерія:

Використання маніпуляційних технік для отримання конфіденційної інформації від користувачів, таких як відправлення фішингових листів або телефонних дзвінків.

7. Використання засобів перехоплення даних:

Використання шпигунського програмного забезпечення або апаратних пристроїв для перехоплення конфіденційної інформації під час її передачі по мережі.

8. Витік даних через недоліки в захисті:

Використання недоліків у заходах захисту, таких як витік даних через недостатньо захищені мережі або незашифровані комунікації.

9. Атаки на шифрування даних:

Атаки на захищені канали зв'язку або алгоритми шифрування з метою розкриття конфіденційної інформації.

10. Втрата даних через випадкові відмови:

Втрата даних через технічні або апаратні несправності, такі як сбої жорстких дисків або відмови систем зберігання.

11. Втрата даних через випадкове видалення:

Видалення або втрата даних через помилкові дії користувачів або адміністраторів системи.

12. Зміна контрольної інформації:

Зміна або підробка контрольної інформації, такої як хеш-суми або цифрові підписи, для приховування змін в даних.

Інформаційні ресурси, як і інші активи, мають свої специфічні загрози:

1. Вразливості веб-додатків:

Веб-сайти можуть мати вразливості, які можуть бути використані зловмисниками для отримання доступу до систем або даних.

2. Крос-сайтові скрипти (XSS):

XSS-атаки можуть бути використані для введення шкідливого коду на веб-сайти.

3. Відмова в обслуговуванні (DoS):

DoS-атаки можуть бути використані для того, щоб зробити веб-сайти недоступними для законних користувачів.

4. Викрадення сеансу:

Зловмисники можуть викрасти сеанси користувачів, щоб отримати доступ до веб-сайтів.

5. Фішинг:

Фішингові атаки можуть бути використані для того, щоб обдурити користувачів, змусивши їх розкрити свої особисті дані або паролі.

6. Несанкціонований доступ:

Зловмисники можуть отримати несанкціонований доступ до мереж, щоб вкрасти дані, пошкодити системи або шпигувати за користувачами.

7. Атаки типу "людина в середині":

Атаки типу "людина в середині" можуть бути використані для перехоплення трафіку між користувачами.

8. Шкідливе програмне забезпечення:

Шкідливе програмне забезпечення може бути встановлено на мережеві пристрої, щоб пошкодити системи або вкрасти дані.

9. Відмова в обслуговуванні (DoS):

DoS-атаки можуть бути використані для того, щоб зробити мережі недоступними для законних користувачів.

10. Шкідливе програмне забезпечення:

Шкідливе програмне забезпечення може бути надіслано електронною поштою, щоб пошкодити системи або вкрасти дані.

11. Спам:

Спам може захаращувати поштові скриньки користувачів і ускладнювати їм пошук важливих повідомлень.

12. Витік даних:

Дані з систем обміну повідомленнями можуть бути викрадені або випадково оприлюднені.

13. Слабкі паролі:

Слабкі паролі можуть бути легко вгадані або зламані зловмисниками, що дозволяє їм отримати доступ до систем через системи дистанційного доступу.

2.2.5 Методи аналізу загроз

2.2.5.1 DREAD

DREAD – це абревіатура від Damage**,** Reproducibility**,** Exploitability**,** Affected Users**,** Discovery Probability**,** які є п'ятьма факторами, що використовуються для оцінки ризику кожної загрози в цій моделі [58]. Найбільшу користь ця модель представляє в контексті визначення пріоритетності реагування на ризики. Кожен ризик аналізується за п’ятьма метриками:

1. Damage (збитки): Яка шкода може бути завдана системі внаслідок атаки? Це може включати втрату конфіденційності, цілісності або доступності даних, втрати фінансів, порушення репутації тощо. Чим більші можливі збитки, тим вищий рівень загрози.

2. Reproducibility (повторюваність): Як ймовірно, що атака буде успішно повторена? Якщо атака легко відтворюється або може бути виконана знову в майбутньому, загроза вважається більш серйозною.

3. Exploitability (експлуатованість): Яка ймовірність успішної експлуатації цієї загрози зловмисниками? Це враховує вразливості в системі, які можуть бути використані для реалізації атаки.

4. Affected Users (користувачі, на яких впливає ризик): Скільки користувачів або систем можуть бути пошкоджені цією загрозою? Чим більше користувачів або систем можуть бути зачеплені, тим більша загроза.

5. Discoverability (ймовірніссть виявлення): Яка ймовірність того, що ця загроза буде виявлена до виконання атаки або після неї? Якщо загрозу важко виявити до чи після її реалізації, це може збільшити її потенційний вплив.

Після оцінки кожного критерію за шкалою від 0 до 10, загальний рейтинг загрози може бути обчислений як добуток множення значень кожного критерію. Далі організація може використовувати цей рейтинг для прийняття рішень щодо пріоритизації заходів безпеки та розробки стратегій захисту [59].

Наприклад, загроза з Damage=5, Reproducibility=7, Exploitability=8, Affected Users=4, Discovery Probability=3 матиме загальне значення 840. Стандартна інтерпретація загального ризику:

- Ризик 1-399: Низький, потребує базових заходів захисту.
- Ризик 400-699: Середній, потребує більш детального аналізу та заходів захисту.
- Ризик 700-1000: Високий, потребує негайних заходів захисту.

2.2.5.2 PASTA

Модель PASTA (Process for Attack Simulation and Threat Analysis) – це методологія для аналізу загроз та планування заходів забезпечення інформаційної безпеки [60]. Ця модель допомагає інженерам безпеки розуміти, які загрози можуть бути спрямовані на їхні інформаційні системи, та розробляти стратегії для їх запобігання або мінімізації наслідків. Модель PASTA надає структурований підхід до аналізу загроз та розробки планів безпеки, допомагаючи організаціям ефективно захищати свої інформаційні системи [61].

Основні кроки моделі PASTA [62]:

1. Підготовка (Preparation): На цьому етапі визначаються мета та область дослідження. Формується команда для аналізу безпеки, визначаються ресурси та інструменти, які будуть використовуватися під час аналізу.

2. Аналіз загроз (Threat Analysis): Команда проводить аналіз загроз, ідентифікуючи потенційні атаки та уразливості, які можуть бути використані атакуючими. Це може включати розгляд сценаріїв загроз, оцінку вразливостей, а також аналіз відомих загроз та атак.

3. Аналіз атак (Attack Analysis): На цьому етапі команда аналізує потенційні атаки більш детально, визначаючи, як саме атаки можуть бути виконані та які можуть бути їхні наслідки. Це допомагає краще зрозуміти потенційні загрози та визначити стратегії захисту.

4. Визначення цілей безпеки (Security Objectives Definition): На цьому етапі визначаються конкретні цілі безпеки, які мають бути досягнуті. Ці цілі можуть включати захист конфіденційності, цілісності та доступності даних, а також захист від певних типів атак.

5. Розроблення плану безпеки (Security Architecture Development): Команда розробляє стратегію безпеки, яка включає в себе заходи для досягнення визначених

цілей безпеки. Це може включати в себе впровадження технологічних рішень, політик безпеки, процедур та навчання персоналу.

6. Валідація (Validation): На цьому етапі проводиться оцінка та перевірка ефективності розробленого плану безпеки. Команда перевіряє, чи відповідає план безпеки визначеним цілям та чи здатний він захистити систему від потенційних атак.

7. Звіт (Reporting): Останній етап включає підготовку звіту про результати аналізу загроз та розробку плану безпеки. Цей звіт може використовуватися для інформування зацікавлених сторін про виявлені загрози та запропоновані заходи безпеки.

Переваги:

1. Комплексний підхід: PASTA забезпечує комплексний підхід до аналізу загроз та розробки стратегій безпеки, що дозволяє виявляти ризики та розробляти ефективні заходи захисту.

2. Фокус на атаках: цей метод зосереджений на аналізі потенційних атак і розумінні їхніх наслідків, що дозволяє більш ефективно захищати систему, реагуючи на конкретні загрози.

3. Врахування контексту: PASTA дозволяє аналізувати загрози та ризики з урахуванням контексту конкретної організації та її інформаційної інфраструктури.

4. Структурований процес: модель використовує структурований процес аналізу та розробки плану безпеки, що сприяє організованості та системності при виконанні завдань.

5. Підвищення освідомленості: PASTA допомагає підвищити рівень осведомленості персоналу про потенційні загрози та вразливості, що може покращити загальну безпеку організації.

Недоліки:

1. Складність використання: деякі організації можуть зіткнутися зі складнощами під час впровадження та використання моделі PASTA через її деталізацію та потребу в експертних знаннях з області безпеки.

2. Час та ресурси: проведення аналізу загроз та розробка плану безпеки за допомогою PASTA може вимагати значних часових та фінансових ресурсів, особливо для великих організацій.

3. Необхідність постійного оновлення: загрози та вразливості в інформаційних системах постійно змінюються, тому необхідно постійно оновлювати аналіз та стратегії безпеки з використанням моделі PASTA.

4. Залежність від якості аналізу: ефективність моделі PASTA залежить від якості проведеного аналізу загроз та вразливостей, а також від правильності розробленого плану безпеки.

2.2.5.3 VAST

Модель VAST (Visual, Agile, and Simple Threat modeling) – це методологія для аналізу загроз та вирішення проблем безпеки в інформаційних системах [64]. Вона була розроблена з метою забезпечення простого та швидкого процесу моделювання загроз, який може бути легко впроваджений в агільних проектах.

Основні принципи моделі VAST [64]:

1. Візуальність (Visual): модель VAST ставить акцент на використанні візуальних засобів для представлення архітектури системи та ідентифікації потенційних загроз. Вона використовує графічні зображення та діаграми для обліку аспектів безпеки системи, що дозволяє краще зрозуміти потенційні ризики.

2. Гнучкість (Agile): модель VAST адаптована для використання в сучасних проектах, де швидкість та гнучкість є ключовими. Вона дозволяє проводити швидкі сесії аналізу загроз під час коротких ітерацій розробки, що сприяє оперативному виявленню та вирішенню проблем безпеки.

3. Простота (Simple): модель VAST ставить на простоту та доступність. Вона використовує прості техніки та інструменти для аналізу загроз, що дозволяє залучати до

процесу моделювання загроз не лише спеціалістів з безпеки, а й інших учасників проекту.

Процес моделювання загроз за методологією VAST включає наступні кроки:

1. Ідентифікація активів: визначення ключових активів системи, які можуть бути вразливими до загроз.

2. Розуміння архітектури: аналіз архітектури системи з метою з'ясування потенційних шляхів атак та вразливостей.

3. Ідентифікація загроз: виявлення потенційних загроз та визначення їх впливу на систему.

4. Оцінка ризиків: оцінка потенційних наслідків загроз та визначення стратегій для їх зменшення або усунення.

5. Розробка заходів безпеки: оозробка конкретних заходів та стратегій для запобігання атак та зменшення ризиків.

Модель VAST може бути корисною для швидкої і ефективної ідентифікації загроз та розробки стратегій безпеки. Вона дозволяє залучити до процесу моделювання загроз різних учасників проекту та швидко реагувати на потенційні ризики [65].

2.2.5.4 CVSS

CVSS (Common Vulnerability Scoring System) – це стандартний метод оцінки вразливостей, який використовується для кваліфікації та кількісної оцінки потенційних ризиків безпеки [68]. CVSS надає можливість однозначно оцінити серйозність вразливостей на основі ряду критеріїв, таких як потенційні наслідки, вразливі компоненти та інші фактори.

Основні складові CVSS [69]:

1. Базовий рівень (Base Score): це числова оцінка вразливості, яка враховує серйозність вразливості без урахування контексту використання. Base Score визначається за допомогою ряду метрик, включаючи:

- Експлуатація – включає в себе вектор атаки, складність атаки, вимоги до привілеїв, необхідність дій з боку користувача, масштаб.
- Вплив – вплив на конфіденційність, цілісність та доступність системи або інформації в ній.

2. Часовий рівень (temporal score): це допоміжні оцінки, які дозволяють уточнити значення базового рівня залежно від можливостей для експлуатації (наявність загальнодоступних засобів для експлуатації), можливостей захисту (наявність методу виправлення вразливості) та точності інформації про саму вразливість.

3. Рівень середи (environmental score): уточнює загальне значення залежно від вимог конкретної системи. Наприклад, у інформаційних системах які обробляють медичні дані зазвичай набагато вищі вимоги до конфіденційності інформації, відповідно вразливості, які впливають на конфіденційність є більш пріоритетними для виправлення.

В результаті оцінки отримується числове значення від 1.0 до 10.0 та відповідні їм якісні показники критичності (низька, середня, висока та критична). Чим вище оцінка – тим більш важливою буде загроза.

2.2.6 Вибір індикаторів

Вибір індикаторів для моделі базується на зазначених у попередніх розділах роботи концепціях та принципах. Кожній загрозі протиставляється певний набір контролів – методів захисту, які пом’якшують або унеможливлюють реалізацію загрози. Кожен з підходів оцінки захищеності систем, розглянутий в першому розділі роботі, визначає свій власний набір контролів, за якими проводиться оцінювання. Використання

одного підходу до оцінки захищеності конкретної системи дає результати і можливість розробки планів дій для підвищення захищеності систем, але має критичний недолік – залежно від вибору підходу результати будуть різними для кожної системи.

Найкращим підходом до вибору індикаторів є опрацювання якомога більшої кількості контролів, визначених в різних підходах до оцінки захищеності. Такий підхід буде надмірним, оскільки окремі контролі або навіть цілі категорії в різних підходах перетинаються. З іншого боку – такий підхід надає якомога ширше покриття контролів, і, відповідно, найближчі до реальності результати.

В контексті моделі, яка пропонується в цій роботі, індикатором захищеності є оцінка конкретного контролю, який відповідає певній загрозі. Оцінка контролів – доволі складна тема, тому варто визначити один загальний підхід до визначення адекватності контролю. Для вирішення цієї задачі в роботі пропонується використовувати єдиний підхід у вигляді визначення кількісного або якісного показника.

Використання кількісних показників, як було зазначено у першому розділі роботи, надає практичність, в той час як якісні метрики дозволяють легше описувати, і відповідно розуміти деякі складні аспекти захищеності ІС.

Враховуючи що загальна кількість унікальних контролів, визначених у найпоширеніших підходах (NIST SP 800-82, ISO 27000, NIST CSF) сягає більше тисячі, для полегшення оцінки і підвищення практичності використання такого підходу варто для кінцевого розрахунку використати меншу кількість індикаторів. Найкращим, на мою думку, вирішенням буде використання інтегральних індикаторів – один більш «загальний» індикатор, який враховуватиме декілька «менших», більш конкретних оцінок.

Оскільки для використання у моделі оцінки захищеності пропонується підхід орієнтований на загрози – визначення індикаторів захищеності напряму залежить від наявних загроз та їх критичності – в першу чергу необхідно проаналізувати загрози інформаційної системи. З аналізу загроз вже органічно випливає набір індикаторів для

кожної з них. В таблиці 2.1 наведено декілька прикладів загроз та відповідних їм інтегральних індикаторів для системи, яка складається з фізичного серверу та декількох програмних систем (FTP та Web сервіси).

Таблиця 2.1 – Інтегральні індикатори захищеності

Компонент системи	Загроза	Індикатор
АЗ	Невторизований доступ	Фізичне обмеження доступу до серверного приміщення
	Фізичне пошкодження внаслідок стихійних лих	Використання автоматизованих вогнегасників, захищеність приміщення від повені, тощо
	Несправність обладнання	Наявність технічного обслуговування, запасних компонентів, можливість швидкої заміни несправних компонентів
FTP	Неавторизований доступ	Контролі доступу, аутентифікація та авторизація
	Використання відомих вразливостей	Контроль версіювання, встановлення оновлень, виявлення та виправлення вразливостей
	DDoS-атаки	Використання фаєрволів, інших методів захисту від DDoS-атак
	Використання zero-day вразливостей	Threat Intelligence, проведення оцінки вразливостей ПЗ
	Використання слабких паролів	Використання багатофакторної аутентифікації, політики паролів
Web	Використання відомих вразливостей	Контроль версіювання, встановлення оновлень, виявлення та виправлення вразливостей
	Неавторизований доступ	Контролі доступу, аутентифікація та авторизація

	Використання zero-day вразливостей	Проведення оцінки вразливостей ПЗ, використання засобів захисту (IDN, WAF)
	Вразливості скриптингу	Використання технологій, орієнтованих на безпеку ПЗ (безпечні фреймворки, мови програмування), наявність програмних методів захисту (CSRF-токени, фільтрація вхідних даних, тощо)
	SQLi-вразливості	Використання технологій, орієнтованих на безпеку ПЗ (безпечні фреймворки, мови програмування), наявність програмних методів захисту (CSRF-токени, фільтрація вхідних даних, тощо)
	Витік інформації	Ретельний контроль за витоками, Threat Intelligence
	Використання слабких паролів	Використання багатофакторної аутентифікації, політики паролів
ОС	Зараження зловмисним ПЗ	Використання засобів захисту від зловмисного ПЗ (антивірусне ПЗ, EDR)
	Вразливості ОС	Своєчасне оновлення системи, використання додаткових систем захисту
	Використання слабких паролів	Використання багатофакторної аутентифікації, політики паролів
	Неавторизований доступ	Контролі доступу, аутентифікація та авторизація
Мережа	Мережеві атаки	Використання систем FW, NGFW, NDR, IPS, IDS

	Фізичне пошкодження	Можливість швидкого переходу на інше мережеве з'єднання

Слід врахувати, що у таблиці наведені лише деякі з можливих загроз і на меті цієї таблиці є наочний приклад суті індикаторів та відповідних їм загроз.

2.2.7 Обґрунтування вибору метрик

Вибір контролів для оцінки кожного індикатору можливий за допомогою поєднання різних підходів – NIST CSF, NIST SP 800-82, ISO 27001, ISO 27002, залежно від можливостей та ресурсів виділених на вибір індикаторів. Чим більше обрано контролів – тим точніший буде результат оцінки, але разом з цим зростатиме складність оцінки. Деякі контролі очевидно будуть пересікатись і в цьому випадку пропонується оцінити контроль за основним підходом, додатковим підходом та взяти середнє значення оцінки. Середнє значення оцінки контролів для загрози і є фінальним індикатором.

Такий підхід до вибору індикаторів має певні недосконалості – він не враховує специфіку самих контролів та систем, щодо яких проводиться оцінка. Деякі контролі будуть більш ефективними для протидії певним загрозам, ніж іншим. Деякі системи мають підвищені (або навпаки – дещо знижені) вимоги до захисту інформації і загального рівня захищеності. Наприклад, система опрацювання медичних даних матиме набагато вищі вимоги до конфіденційності інформації, ніж інтернет-форум.

Для вирішення цих проблем пропонується використання ваги та коефіцієнтів.

Почнемо із підходу до визначення загроз.

Будь-яка загроза має певну «вагу» – те, наскільки критичною є її реалізація. Для розрахунку ваги пропонується використання методів DREAD та CVSS у поєднанні.

Значення, отримане з цього аналізу і буде вагою загрози – наскільки вона дійсно критична для системи.

Але це не враховує вимоги самої системи – для цього пропонується використання коефіцієнту – значення в межах від 0.8 до 1.2 у випадку кількісних показників. Коефіцієнт визначається для кожної системи за допомогою експертної думки, залежно від потреб, вимог, нормативних документів та будь-яких інших факторів. Арифметичний добуток значення ваги та коефіцієнту стає новим значенням ваги загрози, який і буде використано для фінального моделювання.

Щодо підходу до контролів та індикаторів.

Вага контролю – показник того, наскільки конкретний контроль дозволяє впоратись із загрозою. Значення ваги контролю – типові і залежать від самого контролю. Знову, цей показник може варіюватись залежно від ІС і для врахування цього пропонується використання такого же коефіцієнту – значення від 0.8 до 1.2, яке буде враховане для остаточного визначення ваги контролю.

2.2.7.1 Визначення типів метрик

Запропонована модель враховує декілька типів метрик – вага загрози, коефіцієнт загрози, вага контролю, коефіцієнт контролю, загальна оцінка контролю.

Ці метрики можуть бути як кількісними, так і якісними, в першу чергу залежно від доцільності використання кількісних або якісних показників та простоти їх використання.

2.2.7.2 Джерела даних

Вибір джерел даних є неймовірно важливим в контексті оцінки захищеності системи та аналізу загроз. У якості джерел даних пропонується використовувати будь-

які джерела, використання яких є доцільним. Це можуть бути логи моніторингу, експертна думка, повідомлення про загрози від автоматизованих систем, попередні аудити безпеки, результати оцінки вразливостей та тестувань на проникнення, вимоги нормативних документів, політики безпеки.

Вибір контролів для оцінки індикаторів, як вже зазначалось, являє собою поєднання контролів наведених в загальнопоширених підходах до оцінки захищеності та практик кібербезпеки – ISO 27000, NIST SP 800-82, NIST CSF. Задля полегшення роботи із моделлю у якості основного підходу пропонується використання NIST CSF – кількість контролів, визначена цим стандартом менша, ніж у інших, але в цілому покриває ті самі галузі безпеки.

Недолік підходу – незалежно від обраних джерел даних фінальне значення оцінки повністю кладеться на суб'єктивну думку експерта, який проводить оцінку контролів.

Висновки за розділом 2

У другому розділі роботи проаналізовано питання розробки моделей загроз для інформаційних систем. Моделювання загроз – це процес не лише виявлення потенційних небезпек, але й розробка моделі шляхом поетапної оцінки вразливостей у системі. Ця модель допомагає виявляти, систематизувати та розуміти ризики та заходи, спрямовані на їх зменшення, у контексті захисту критичних ресурсів.

Детально проаналізовано найпоширеніші методи побудови моделей загроз – STRIDE, дерева атак, MITRE ATT&CK.

Вивчено питання вибору індикаторів та метрик оцінки захищеності для подальшої розробки моделі оцінки захищеності ІС. Визначено основні принципи та цілі, враховані при виборі індикаторів.

Розглянуто питання визначення переліку активів та важливість цього процесу для загального моделювання загроз та оцінки захищеності ІС.

Розроблено структурований опис потенційних загроз ІС, який базується на визначеному переліку активів ІС.

Виділено набір метрик та індикаторів для використання у моделі, заснований на найкращих світових практиках. Запропоновано використання підходу до оцінки захищеності, орієнтованого на загрози ІС. У якості метрик для оцінки пропонується використання оцінки загрози за допомогою існуючих моделей та підходів аналізу загроз, визначення критичності кожної загрози відповідне вимогам до інформаційної безпеки та захищеності інформації конкретної ІС, визначення оцінки контролів за допомогою підходів, що описано в ISO 27000, NIST SP 800-82 та NIST CSF з урахуванням відповідності кожного контролю загрозі, оскільки не всі контролі однаково ефективні для запобігання загрозі. Наведені переваги та недоліки використання таких метрик та доцільність їх використання у моделюванні.

Підхід до вибору метрик буде використано для розробки моделі захищеності ІС.

РОЗДІЛ 3
РОЗРОБКА МОДЕЛІ ОЦІНКИ ЗАХИЩЕНОСТІ ІС

Цей розділ присвячений самій моделі оцінки захищеності загроз. Для вирішення поставлених задач необхідно обрати та обґрунтувати методологію моделі, розробити модель, синтезувати її за допомогою штучних нейронних мереж та протестувати точність результатів.

3.1 Вибір та обґрунтування методології моделі оцінки захищеності

Робота пропонує концепцію моделі оцінки захищеності інформаційних систем, засновану на підході, орієнтованому на загрози. Модель використовує комплексний підхід, який включає ідентифікацію та оцінку загроз за допомогою моделі DREAD, аналіз наявних контролів безпеки та їх відповідність виявленим загрозам, а також застосування штучної нейронної мережі для обчислення кількісних оцінок захищеності системи.

Підхід, орієнтований на загрози, в контексті цієї роботи передбачає аналіз системи з точки зору потенційних загроз безпеці. Основна ідея полягає в тому, щоб ідентифікувати та оцінити потенційні загрози, які можуть вплинути на інформаційну систему. Для цього використовується модель DREAD, яка дозволяє оцінити рівень загрози з точки зору п'яти критеріїв: Damage, Reproducibility, Exploitability, Affected users та Discoverability. Ця оцінка дозволяє визначити потенційний вплив загрози на систему та її складові елементи. Кожен з критеріїв оцінюється по шкалі від 0 до 10, загальна оцінка – сума оцінок критеріїв. Чим вища сума – тим критичніше загроза.

Переваги підходу, орієнтованого на загрози, включають:

1. Фокус на реальних потенційних загрозах: цей підхід дозволяє ідентифікувати та оцінити конкретні загрози, які можуть становити найбільшу небезпеку для інформаційної системи.

2. Проактивний підхід до захисту: шляхом передбачення потенційних загроз та їх оцінки можна розробити стратегії захисту, що дозволить уникнути потенційних проблем у майбутньому.

3. Глибоке розуміння уразливостей системи: аналіз потенційних загроз дозволяє зрозуміти слабкі місця інформаційної системи та вжити заходів для їх вирішення.

Однак цей підхід також має свої недоліки:

1. Обмежена відомість про нові загрози: модель DREAD базується на відомих загрозах і може не враховувати нові атаки або уразливості.

2. Підвищена складність аналізу: ідентифікація та оцінка потенційних загроз може вимагати значних зусиль та ресурсів.

3. Значна кількість даних: для ефективного застосування цього підходу потрібна достатня кількість інформації про загрози та їх потенційний вплив на систему.

Одним з методів часткового виправлення недоліків є створення опису типових загроз. Всі інформаційні системи мають спільні елементи, компоненти та підходи. Більшість загроз для різних систем будуть по своїй суті однаковими, тому аналіз типових загроз і повторне використання результатів такого аналізу дозволяють зекономити час і ресурси.

Варто врахувати, що на меті роботі стоїть розробка універсальної моделі оцінки захищеності ІС, яку можна застосувати до будь-якої ІС, незалежно від наявних загроз. Для цього, як вже згадувалось раніше, пропонується використання коефіцієнтів – числових модифікаторів, які створені для уточнення оцінки загроз для різних типів систем.

Коефіцієнт загрози – значення в межах 0.8 до 1.2, яке надає можливість дещо змінити числове значення загрози, залежно від системи. Цей підхід гарантує

адаптованість моделі до різних типів ІС, хоч і має суттєвий недолік – коефіцієнт потрібно розраховувати для кожної загрози для кожного типу ІС, що збільшує складність аналізу.

Після ідентифікації потенційних загроз і їх оцінки за допомогою моделі DREAD, наступним кроком є оцінка контролів безпеки, які призначені для запобігання або зменшення впливу цих загроз на інформаційну систему. Оцінка контролів полягає в тому, щоб визначити, наскільки ефективні існуючі заходи безпеки у протидії конкретним загрозам.

Оцінка контролів включає такі етапи:

1. Ідентифікація контролів: спочатку необхідно зібрати інформацію про всі наявні заходи безпеки, що застосовуються в інформаційній системі. Це може включати політики, процедури, технічні засоби, персонал і т. д.

2. Оцінка ефективності контролів: наступним кроком є оцінка того, наскільки ефективними є ці контролі у захисті від конкретних загроз. Це може вимагати аналізу технічних параметрів, якості реалізації, вартості, ступеня покриття загроз та інших факторів.

3. Призначення ваги контролю: після оцінки ефективності кожного контролю їм можуть бути призначені ваги в залежності від їх важливості та впливу на систему. Це допомагає врахувати різний внесок кожного контролю у загальну захищеність системи.

Призначення ваги контролю використовує підхід, схожий до аналізу загроз – використання коефіцієнту відповідності контролю.

Коефіцієнти відповідності в контексті оцінки контролів є важливими показниками, які допомагають врахувати різницю в ефективності різних контролів в контексті конкретної інформаційної системи. Ці коефіцієнти визначаються на основі порівняння між стандартним еталоном контролю та реальними заходами безпеки, що застосовуються в системі.

Основна ідея полягає в тому, щоб призначити кожному контролю коефіцієнт відповідності, який відображає, наскільки ефективно цей контроль відповідає стандартам безпеки або найкращим практикам. Зазвичай цей коефіцієнт є значенням від 0,8 до 1,2, де 1 вказує на повну відповідність стандарту, менші значення вказують на меншу ефективність, а більші – на більшу ефективність, ніж вимоги.

Переваги використання коефіцієнтів відповідності включають:

1. Порівняльна оцінка: дозволяє порівнювати різні контролі за їх ефективністю на одній шкалі, що спрощує процес оцінки та вибору контролів для впровадження.

2. Урахування контексту: коефіцієнти відповідності можуть бути налаштовані залежно від специфіки інформаційної системи та її вимог до безпеки, що дозволяє краще враховувати унікальні особливості системи.

3. Гнучкість: дозволяє швидко змінювати коефіцієнти відповідності у відповідь на нові загрози або зміни у вимогах до безпеки.

Оцінка контролів – дуже складний процес, описаний в багатьох різних підходах до оцінки захищеності ІС. В контексті запропонованої моделі оцінка контролів відбувається за допомогою фреймворку NIST CSF, оскільки це один з найпростіших способів кількісної оцінки контролів.

Оцінка контролю – цифрове значення в діапазоні між 1 та 8, де 8 – найвищий рівень контролю та його відповідності загрозі.

Після аналізу загроз і оцінки контролів, наступним кроком є синтез моделі оцінки захищеності інформаційної системи. Цей етап включає об'єднання результатів аналізу загроз, оцінки контролів та їх ваги для створення цілісної моделі, яка визначає рівень захищеності системи.

Наступним кроком оцінки захищеності інформаційної системи (ІС) за використання моделі на основі індикаторів захищеності є обчислення фінального значення індикатора захищеності для кожної загрози. Пропонується використання

кількісних показників від 1 до 4, де 1 відповідає якісній оцінці «незадовільно», 2 – «задовільно», 3 – «добре», 4 – «відмінно».

1. Аналіз індикаторів захищеності: кожен індикатор захищеності аналізується за допомогою штучної нейронної мережі для визначення його значення на основі наданих вхідних даних. Ці дані включають в себе інформацію про загрозу, вагу загрози, контроль, та вагу контролю, скориговані за допомогою коефіцієнтів.

2. Обчислення оцінки захищеності: на основі отриманих значень індикаторів захищеності обчислюється фінальна оцінка захищеності для кожної загрози. Це виконується шляхом агрегації значень індикаторів, враховуючи їх вагу та інші фактори, що впливають на рівень захищеності ІС.

3. Визначення рівня захищеності: оцінки захищеності для кожної загрози агрегуються для визначення загального рівня захищеності інформаційної системи. Це може включати середнє значення оцінок захищеності або інші методи агрегації, що враховують важливість кожної загрози для ІС, залежно від побажань користувача моделі. В контексті цієї роботи буде використане середнє значення оцінок захищеності.

4. Визначення рівня в зрілості системи безпеки: нарешті, на основі отриманого рівня захищеності можна визначити рівень в зрілості системи безпеки відповідно до ступенів (Tiers) зрілості системи безпеки відповідно до фреймворку NIST CSF. Це допомагає визначити, наскільки ефективно система захищена та які ще кроки можна здійснити для покращення безпеки.

Після оцінки захищеності ІС йде етап розробки планів та стратегій, орієнтованих на покращення захищеності системи у відповідності до отриманих результатів аналізу загроз, оцінки контролів та загальної оцінки захищеності.

3.2 Розробка моделі оцінки захищеності ІС

Для реалізації моделі оцінки захищеності ІС обрано штучні нейронні мережі, через ряд причин:

1. Здатність до роботи з складними нелінійними залежностями: штучні нейронні мережі можуть моделювати складні нелінійні зв'язки між вхідними та вихідними даними, що дозволяє їм ефективно аналізувати та прогнозувати складні системи, такі як безпека інформаційних систем.
2. Адаптивність до нових даних: нейронні мережі можуть навчатися на вхідних даних і підлаштовуватися до змін в середовищі, що дозволяє їм підтримувати актуальність та ефективність моделі з часом.
3. Обробка великих обсягів даних: штучні нейронні мережі можуть ефективно обробляти великі обсяги даних, які зазвичай виникають в контексті безпеки інформаційних систем.
4. Здатність до адаптації до нових ситуацій: модель, побудована на основі штучних нейронних мереж, може виявляти нові типи загроз та контролів, що дозволяє системі швидко реагувати на зміни в середовищі.
5. Висока точність та надійність: штучні нейронні мережі можуть досягати високого рівня точності та надійності у виявленні та прогнозуванні загроз, що робить їх ефективними для застосування в сфері безпеки інформаційних систем.

3.2.1 Архітектури моделі оцінки захищеності

У якості моделі ШНМ було обрано Random Forest [71].

Random Forest є потужним методом машинного навчання, що використовується для класифікації та регресії. Вона базується на ідеї ансамблю дерев рішень, де кожне дерево у лісі є класифікатором, і кінцеве рішення приймається на основі голосування

або усереднення результатів всіх дерев. Random Forest відомий своєю високою точністю та стійкістю до перенавчання.

Random Forest має кілька переваг, таких як висока точність, здатність роботи з великими обсягами даних, автоматичний відбір ознак і стійкість до перенавчання. Крім того, він може виявляти складні зв'язки між ознаками та ефективно прогнозувати класи.

Для оцінки ефективності моделі та уникнення перенавчання використовується крос-валідація [75].

Крос-валідація – це метод оцінки ефективності моделі машинного навчання, який дозволяє оцінити її здатність до узагальнення на нових даних та уникнути перенавчання. Основна ідея полягає в тому, щоб поділити набір даних на кілька піднаборів, відомих як "фолди", і потім навчати модель на одному фолді, використовуючи решту як тестовий набір. Цей процес повторюється декілька разів з різними комбінаціями навчальних і тестових наборів, і результати об'єднуються для отримання загальної міри ефективності моделі. Крос-валідація дозволяє поділити навчальний набір даних на кілька піднаборів, що дозволяє навчати модель на одному піднаборі та перевіряти її на інших. Цей процес повторюється кілька разів, щоб отримати більш стабільні оцінки ефективності моделі.

Співвідношення навчальних, валідаційних та тестових даних було визначено на рівні 70:20:10 задля отримання якнайточнішої моделі.

3.2.2 Вимоги до алгоритму навчання

В контексті цієї роботи було виділено наступні вимоги до алгоритму навчання:

1. Ефективність: алгоритм навчання повинен бути ефективним і здатним обробляти великі обсяги даних. Це пояснюється тим, що робота ведеться з комплексними інформаційними системами, які можуть мати велику кількість атрибутів та екземплярів.

2. Масштабованість: алгоритм навчання повинен бути масштабованим, тобто здатним працювати зі зростанням розміру набору даних без значного збільшення часу навчання.

3. Здатність до перенавчання: оскільки використовується складна модель Random Forest, важливо, щоб алгоритм навчання був здатним до перенавчання. Він повинен ефективно управляти складністю моделі, забезпечуючи при цьому її здатність до узагальнення на нові дані.

4. Параметризація: може виникнути потреба в налаштуванні параметрів моделі Random Forest, таких як кількість дерев, максимальна глибина дерева, мінімальне число об'єктів у листі та інших. Тому алгоритм навчання повинен підтримувати можливість параметризації моделі з урахуванням особливостей задачі.

5. Інтерпретованість результатів: оскільки модель використовується для оцінки захищеності інформаційних систем, важливо, щоб алгоритм навчання забезпечував інтерпретованість результатів. Це означає, що має існувати можливість пояснити, які саме аспекти системи спричинили певний рівень захищеності.

3.3. Підготовка даних для моделювання оцінки захищеності

Підготовка даних для моделювання оцінки захищеності є критичним етапом у розробці моделі оцінки.

Чим більша кількість вхідних даних для навчання моделі, тим точніше будуть результати використання цієї моделі. Однак, слід врахувати, що дані мають бути максимально репрезентативними – описувати реальні ситуації, пов’язані з реальними системами і мати якомога вищий рівень якості оцінки вхідних параметрів.

3.3.1 Збір даних

Для збору даних для навчання моделі було використано декілька підходів:

1. Журнали подій (логи систем): ці дані містять інформацію про всі події, які сталися в системі, включаючи спроби вторгнень, зміни в налаштуваннях безпеки, автоматичні сповіщення систем безпеки тощо. Системні логи часто є публічно доступними, особливо в контексті інформаційної безпеки.

2. Дані інцидентів безпеки: інформація про інциденти, які відбулися у минулому, такі як вторгнення, витоки даних, вірусні атаки, яка була публічно опублікована.

3. Дані від сторонніх постачальників безпеки: звіти від вендорів програмного забезпечення, розробників антивірусного програмного забезпечення, компаній з кібербезпеки, які надають інформацію про потенційні загрози та методи захисту.

Наведені вище джерела були використані для оцінки загроз за методом DREAD.

Для виявлення потенційних контролів та їх оцінок для кожної із загроз було використано наступні джерела:

1. Стандарти ISO 27000, NIST CSF, NIST SP 800-53: ці документи визначають величезний список контролів, відповідних певним загрозам. Було використано контролі, описані в кожному із цих стандартів. У випадку співпадіння контролів перевага надавалась NIST SP 800-53.

2. Дані від сторонніх постачальників безпеки: звіти від вендорів, які стосуються оцінки потенційних рішень безпеки та їх відповідності існуючим загрозам.

Для збільшення кількості вхідних даних (що веде до покращення якості та точності прогнозів за допомогою моделі) було додатково згенеровано псевдовипадковим чином дані, максимально наближені до реальних та вручну скореговано їх значення.

3.3.2 Очищення даних

Очищення даних – це важливий етап підготовки даних для моделювання, оскільки воно допомагає уникнути помилок та неточностей, які можуть вплинути на результати аналізу.

Перш ніж аналізувати дані, було проведено перевірку щодо дублікатів. Дублікати можуть спотворити результати та вплинути на аналіз. Після цього – обробка пропущених значень. Рядки даних з пропущеними значеннями були видалені із датасету, задля забезпечення неупередженості та реалістичності даних.

Наступним важливим етапом є обробка аномалій. Аномальні значення можуть вплинути на аналіз, тому вони повинні бути виявлені та відфільтровані або замінені на відповідні значення. Значення, які сильно «вибивались» із загального датасету були видалені.

Ще одним важливим кроком є видалення зайвих атрибутів. Якщо деякі атрибути не мають значущого впливу на аналіз – вони видаляються. В наявному датасеті доволі значна кількість даних ніяк би не вплинула на аналіз – в основному це стосується випадків загроз, які не мають високого впливу на систему (за методом аналізу DREAD їх значення були близькі до нуля). Визначення ефективності контролів для таких загроз не має практичної цінності, адже незалежно від самих контролів ризики, пов'язані з цими загрозами відсутні.

На рисунку 3.1 зображено декілька прикладів даних, які було видалено із датасету та вказані причини.

```
0.0,0.98,5.0,0.95,3 - значення DREAD = 0
24.0,1.04,7.0,0.85,1 - значення індикатора занадто низьке
50.0,1.18,5.0,0.93,4 - значення індикатора занадто високе
```

Рисунок 3.1 – Приклад видалених із датасету даних

І нарешті, проведення нормалізації даних може допомогти збалансувати вагу різних атрибутів та зробити модель більш стійкою до змін в масштабі даних.

Для очищення даних було використано бібліотеки Pandas та NumPy мови програмування Python та побудовані на них програми.

3.3.3 Формування навчального, валідаційного та тестового наборів даних

Після того, як дані були зібрані та очищені, наступним важливим кроком є їх розділення на навчальний, валідаційний та тестовий набори. Це робиться з метою гарантування того, що модель машинного навчання може бути належним чином навчена, налаштована та оцінена перед її впровадженням у реальне середовище.

Навчальний набір використовується для того, щоб навчити модель розпізнавати закономірності та робити прогнози. Це набір даних, на основі якого модель буде навчатися.

Валідаційний набір використовується для налаштування гіперпараметрів моделі. Він складається з даних, які модель не бачила раніше, але схожі на дані з навчального набору. Це допомагає уникнути перенавчання моделі, коли вона стає занадто добре підігнана під навчальний набір і не може ефективно узагальнювати на нових даних.

Тестовий набір використовується для остаточної оцінки продуктивності моделі. Він містить дані, які модель ніколи раніше не бачила, що дає неупереджену оцінку її продуктивності в реальних умовах.

Розділення даних на ці три набори є важливим для забезпечення того, що модель машинного навчання буде надійною та узагальнюваною. Такий підхід допомагає уникнути того, щоб модель просто запам'ятовувала навчальний набір, а замість цього ефективно навчалася на нових даних.

Для поділу даних у набори їх було перемішано та розділено на три списки у пропорції 70:20:10, що забезпечить найкращий рівень навчання моделі.

Вхідні дані для навчання та валідації моделі мають наступний вигляд:

Оцінка загрози, коефіцієнт оцінки загрози, оцінка контроля, коефіцієнт оцінки загрози, оцінка захищеності.

У таблиці 3.1 зображено фрагмент загальної вибірки даних у тому вигляді, в якому їх сприймає синтезована модель.

Таблиця 3.1 – Приклад вхідних даних

Оцінка за DREAD	Коефіцієнт загрози	Оцінка контролю	Коефіцієнт контролю	Загальна оцінка
23.0	1.07	1.0	0.93	1
20.0	1.12	6.0	0.95	4
18.0	0.89	6.0	1.16	4

3.3.4 Статистичні характеристики даних

Оцінка статистичних властивостей даних є важливим кроком у розумінні їх розподілу, тенденцій та потенційних проблем у використовуваних датасетах для навчання, валідації та тестування моделі. Аналіз цих властивостей дозволяє оптимізувати параметри моделі та підвищити її точність та надійність.

Деякі з найбільш важливих статистичних метрик, які можуть бути використані для оцінки даних та моделей, включають:

1. Середнє значення (Mean): це середнє значення всіх точок даних і використовується для визначення центральної тенденції.
2. Медіана (Median): це значення, яке розділяє впорядкований набір даних на дві рівні частини. Вона нечутлива до викидів і може бути кращим показником для симетричної або важкої розподілу.

3. Стандартне відхилення (Standard Deviation): це міра розкиду даних навколо їх середнього значення. Велике стандартне відхилення вказує на великий розкид, а мале – на невеликий розкид.

В таблиці 3.2 наведено вищевказані статистичні метрики для вхідних даних моделі.

Таблиця 3.2 – Статистичні метрики вхідних даних

Метрика	Оцінка загрози	Коефіцієнт загрози	Оцінка контролю	Коефіцієнт контролю	Значення індикатора
Середнє значення	24.1	1.003	4.063	1.005	2.31
Медіана	24.0	0.99	4.0	1.008	2.0
Стандартне відхилення	14.35	0.114	1.97	0.115	1.06

3.4 Моделювання

Для моделювання нейронної мережі було використано програмне забезпечення Weka – це програмне забезпечення з відкритим вихідним кодом, що випускається під ліцензцією GNU General Public License та вміщує набір алгоритмів машинного навчання для задач інтелектуального аналізу даних [78]. Він містить інструменти для підготовки даних, класифікації, регресії, кластеризації, видобування правил асоціації та візуалізації.

3.4.1 Навчання моделі на навчальному наборі даних

Для навчання моделі використано Weka Explorer – частину програмного комплексу Weka, яка призначена для опрацювання даних, класифікації, кластерізації, асоціації та візуалізації даних, навчання та тестування моделей.

Вхідні дані подаються у вигляді документу формату ARFF – це текстовий формат файлу, який використовується для представлення даних у вигляді таблиці з атрибутами та їх значеннями. Цей формат часто використовується в машинному навчанні та іншій обробці даних для зручності зберігання та обміну даними між різними програмами.

Файл ARFF складається з двох основних секцій: секції атрибутів (Attributes) та секції даних (Data). У секції атрибутів перераховуються всі атрибути (колонки) даних разом з їх типами. У секції даних подаються реальні значення цих атрибутів для кожного екземпляра даних (рядка).

Типи атрибутів в ARFF можуть бути числовими (numeric), рядковими (string) або категоріальними (nominal), які вказуються у вигляді списку можливих значень. Крім того, можна використовувати також логічний (logical) та дата/часовий (date) типи.

Для моделювання було використано датасет, який містить сумарно 1658 записів, з яких на навчання виділено 1160 записи, на валідацію 332, а на тестування 166.

Після навчання моделі показник коректно ідентифікованих записів склав 98.7069%.

```
=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances        1145               98.7069 %
Incorrectly Classified Instances        15                1.2931 %
Kappa statistic                          0.9824
Mean absolute error                      0.0151
Root mean squared error                  0.0865
Relative absolute error                  4.1084 %
Root relative squared error             20.1773 %
Total Number of Instances             1160

=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0,990    0,001    0,997      0,990    0,994      0,991    0,999     0,996     1
               0,988    0,006    0,985      0,988    0,986      0,981    0,994     0,986     2
               0,991    0,009    0,980      0,991    0,986      0,980    0,992     0,978     3
               0,970    0,002    0,988      0,970    0,979      0,975    0,985     0,962     4
Weighted Avg.  0,987    0,005    0,987      0,987    0,987      0,983    0,994     0,983

=== Confusion Matrix ===

   a   b   c   d   <-- classified as
 312   3   0   0 |   a = 1
   1 326   3   0 |   b = 2
   0   1 346   2 |   c = 3
   0   1   4 161 |   d = 4
```

Рисунок 3.2 – Результати навчання моделі

На рисунку 3.3 зображено графік похибок при навчанні моделі.

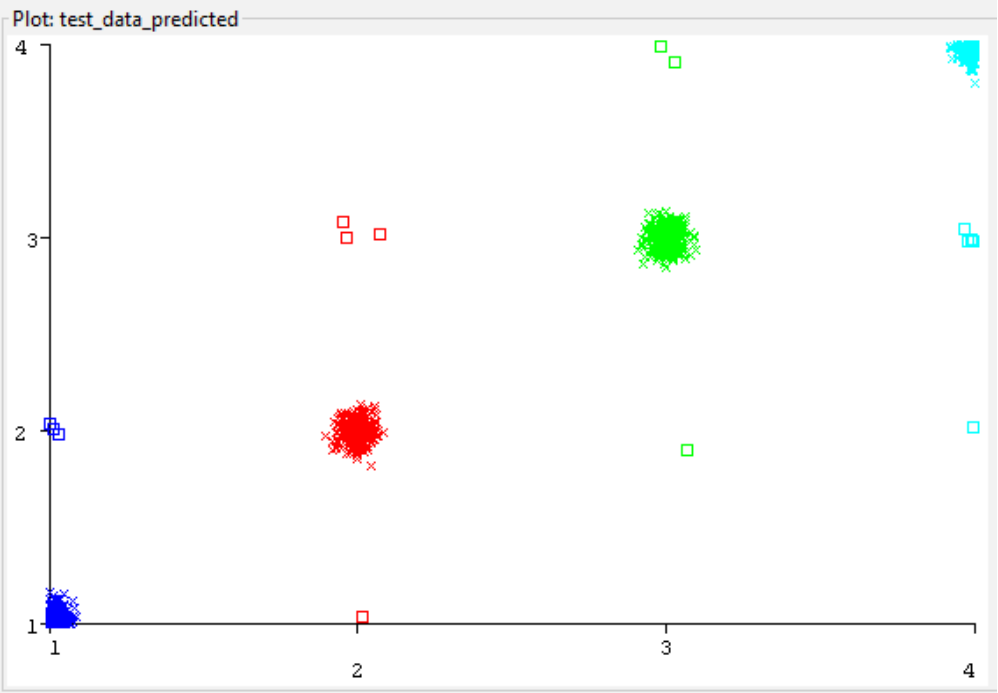

Рисунок 3.3 – Графік похибок при навчанні моделі

3.5 Валідація та тестування моделі оцінки захищеності ІС

Валідація та тестування є кроком, на якому оцінюється ефективність та надійність моделі на нових, раніше не бачених даних. Цей етап є вирішальним для забезпечення того, що модель може ефективно працювати в реальних умовах та надавати корисні результати.

3.5.1 Тестування моделі на контрольному та тестовому наборах даних

Контрольний (валідаційний) набір даних – це дані, які не використовуються під час навчання моделі або налаштування її параметрів. Цей набір дозволяє оцінити, наскільки добре модель узагальнює на нових, але схожих на навчальні дані. Це

допомагає виявити будь-яке перенавчання моделі. Основна мета тестування моделі на контрольному наборі даних – покращення ефективності моделі (перевірка адекватності).

Результати тестування моделі на контрольному наборі даних зображені на рисунку 3.4.

```
=== Summary ===

Correctly Classified Instances         328               98.7952 %
Incorrectly Classified Instances         4                1.2048 %
Kappa statistic                          0.9836
Mean absolute error                      0.0111
Root mean squared error                  0.0507
Relative absolute error                  3.0238 %
Root relative squared error             11.8378 %
Total Number of Instances              332

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1,000    0,013    0,970      1,000    0,985      0,978    1,000     1,000     1
                 0,964    0,000    1,000      0,964    0,982      0,976    1,000     1,000     2
                 0,990    0,000    1,000      0,990    0,995      0,993    1,000     1,000     3
                 1,000    0,004    0,979      1,000    0,989      0,988    1,000     1,000     4
Weighted Avg.    0,988    0,004    0,988      0,988    0,988      0,984    1,000     1,000

=== Confusion Matrix ===

   a   b   c   d   <-- classified as
  96   0   0   0 |   a = 1
   3  81   0   0 |   b = 2
   0   0 104   1 |   c = 3
   0   0   0  47 |   d = 4
```

Рисунок 3.4 – Результати тестування моделі на валідаційних даних

Як видно з рисунку 3.4, кількість коректно ідентифікованих наборів складає 98.7952%, що не суттєво вище за початкову, отриману під час навчання моделі. Зміна гіперпараметрів моделі не буде мати суттєвого впливу на модель.

Тестовий набір даних – це другий окремий набір даних, який так само, як і валідаційний, не використовується під час навчання моделі. Він використовується для остаточної оцінки продуктивності моделі після її налаштування та підтримки. Тестовий набір даних є важливим для визначення точності, чутливості та специфічності моделі.

Результати тестування моделі на тестовому наборі даних зображені на рисунку 3.3.

```
=== Summary ===

Correctly Classified Instances         109               93.9655 %
Incorrectly Classified Instances         7                6.0345 %
Kappa statistic                          0.9173
Mean absolute error                      0.0387
Root mean squared error                  0.1722
Relative absolute error                 10.5464 %
Root relative squared error             40.2179 %
Total Number of Instances              116

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 0,914    0,000    1,000      0,914    0,955      0,939    0,983     0,974     1
                 0,933    0,047    0,875      0,933    0,903      0,869    0,972     0,949     2
                 1,000    0,037    0,921      1,000    0,959      0,942    0,976     0,900     3
                 0,875    0,000    1,000      0,875    0,933      0,926    0,958     0,920     4
Weighted Avg.    0,940    0,023    0,944      0,940    0,940      0,920    0,975     0,938

=== Confusion Matrix ===

  a  b  c  d   <-- classified as
 32  3  0  0 |  a = 1
  0 28  2  0 |  b = 2
  0  0 35  0 |  c = 3
  0  1  1 14 |  d = 4
```

Рисунок 3.5 – Результати тестування моделі на тестових даних

Як видно з рисунку 3.5 – точність моделі впала до 93.9655 % або 109 зі 116 наборів даних.

Таке падіння точності обумовлено невеликими розмірами вхідних датасетів.

3.5.2 Оцінка ефективності моделі на основі показників точності, F1-міри, AUC-ROC

Як було вказано раніше – точність моделі складає 93.9 % відсотки, що є достатньо якісним результатом з урахуванням розмірів наборів даних.

F1-міра – це метрика, яка використовується для оцінки ефективності моделі класифікації, особливо у випадках, коли класи даних незбалансовані (тобто кількість екземплярів різних класів значно відрізняється). Вона об'єднує точність (precision) та чутливість (recall) моделі в один числовий показник.

Точність (precision) вимірює, яка частка екземплярів, які класифікуються як позитивні, дійсно є позитивними. Вона обчислюється як відношення кількості правильно класифікованих позитивних екземплярів до загальної кількості екземплярів, які класифікуються як позитивні.

Чутливість (recall), відома також як true positive rate, вимірює, яка частка дійсно позитивних екземплярів була класифікована як позитивні. Вона обчислюється як відношення кількості правильно класифікованих позитивних екземплярів до загальної кількості дійсно позитивних екземплярів.

F1-міра обчислюється як гармонічне середнє точності та чутливості. Вона надає баланс між цими двома метриками і часто використовується в задачах класифікації, де обидві метрики є важливими. F1-міра може приймати значення від 0 до 1, де значення ближче до 1 вказує на кращу ефективність моделі.

Значення F1-міри для синтезованої моделі складає 0,940.

AUC-ROC (Area Under the Receiver Operating Characteristic Curve) – це метрика, яка використовується для оцінки ефективності бінарних класифікаторів, особливо в умовах дисбалансу класів або коли важливі як точність, так і чутливість класифікації.

ROC-крива – це графік, який відображає відношення між чутливістю (true positive rate) та специфічністю (1 – false positive rate) класифікатора при різних порогових значеннях. AUC-ROC вимірює площу під цією кривою.

AUC-ROC може приймати значення від 0 до 1, де значення ближче до 1 вказує на кращу ефективність класифікатора. Загальною інтерпретацією AUC-ROC є ймовірність того, що класифікатор правильно ранжує випадково вибрану пару позитивного та негативного екземплярів, де вища значення AUC-ROC вказує на кращу здатність класифікатора робити це.

Показник AUC-ROC при тестуванні на тестових даних складає 0.975, що є дуже хорошим результатом.

На рисунку 3.6 зображено графічну візуалізацію ROC-кривої.

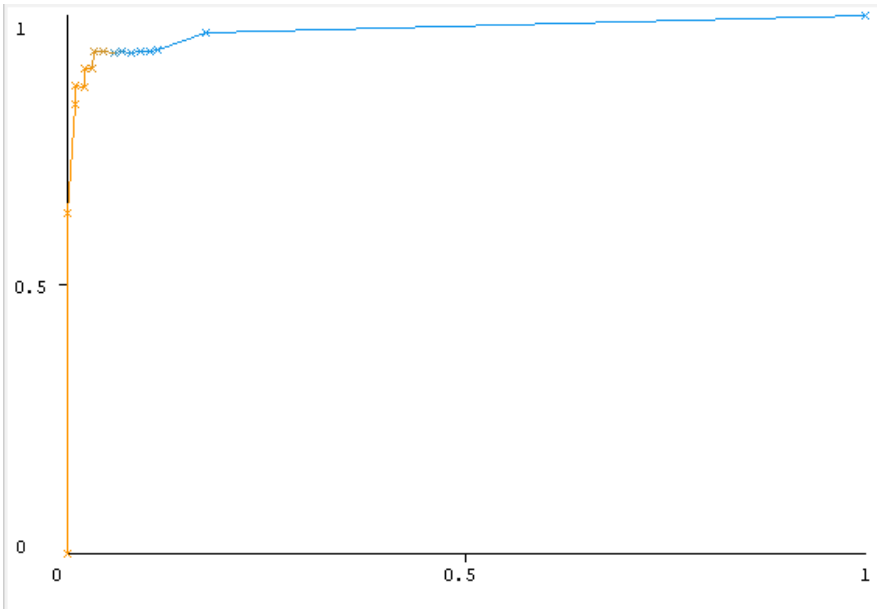

Рисунок 3.6 – ROC-крива

В цілому, для покращення ефективності моделі в першу чергу потрібен більший набір вхідних даних.

Висновки за розділом 3

В третьому розділі роботи було розроблено модель оцінки захищеності інформаційних систем. Модель оцінки має підхід, орієнтований на загрози та має наступні кроки: аналіз загроз, аналіз та оцінка контролів, корегування значень оцінок за допомогою коефіцієнтів відповідності, розрахунок значень індикаторів та розрахунок загального значення захищеності системи.

Також у розділі було синтезовано модель за допомогою штучних нейронних мереж на основі алгоритму random forest. Модель була навчена, валідована та протестована за допомогою зібраного набору даних.

Точність моделі складає 93.9%, що є хорошим показником з урахуванням обмеженого розміру вхідного датасету. F1-міра моделі складає 0.94, що є достатньо високим показником.

Показник AUC-ROC складає 0.975 при максимальному значенні в 1, що є дуже хорошим результатом і вказує на точність моделі.

Використання моделі для оцінки реальних систем є цілком реальною перспективою, але вимагатиме допрацювань. В першу чергу необхідно зібрати більший набір вхідних даних для навчання моделі. Наступними кроками буде корегування гіперпараметрів моделі для покращення точності та велика кількість тестів задля визначення оптимальних параметрів.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне наукове завдання щодо розробки нових методів проведення оцінки захищеності. В процесі розв’язання поставлених задач були отримані наступні результати.

В першому розділі роботи детально проаналізовано існуючі методи та підходи до оцінки захищеності різних типів інформаційних систем, включаючи NIST CSF, NISF SP 800-82, C2M2, ITIL, ISO 27001, ISA/IEC 62443, ISO 15408. Проаналізовано індикатори та метрики оцінки захищеності інформаційних систем.

У другому розділі роботи розглянуто питання моделювання загроз для ІС шляхом аналізу найпоширеніших існуючих підходів та методів аналізу загроз. Проаналізоване питання аналізу визначених загроз та їх оцінки з точки зору критичності впливу на систему та ймовірності реалізації загрози. Визначено набір метрик для подальшого використання у моделі оцінки захищеності та підходи до оцінки кожної метрики, максимально адаптивні для кожної системи та відносно прості у визначенні. Розроблено структурований опис загроз для ІС.

У третьому розділі роботи запропоновано нову модель оцінки захищеності інформаційних систем. За допомогою штучних нейронних мереж синтезовано модель, яка дозволяє з точністю у 93.9% оцінити захищеність систем, базуючись на аналізі загроз та оцінці контролів. Проаналізовано адекватність запропонованого рішення.

Подальші кроки у розвитку моделі включають збільшення навчальної вибірки та корегування параметрів моделі з метою підвищення точності моделі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike [Електронний ресурс]: Wired. – Режим доступу: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack.

2. Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done [Електронний ресурс]: The Conversation. – Режим доступу: https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802.

3.Cybersecurity Framework [Електронний ресурс]: NIST. – Режим доступу: https://www.nist.gov/cyberframework.

4. 40 об'єктів критичної інфраструктури посилять кіберзахист завдяки кібердіагностиці [Електронний ресурс]: Державна служба спеціального зв'язку та захисту інформації України. – Режим доступу: https://cip.gov.ua/ua/news/40-ob-yektiv-kritichnoyi-infrastrukturi-posilyat-kiberzakhist-zavdyaki-kiberdiagnostici.

5. The NIST Cybersecurity Framework (CSF) 2.0 [Електронний ресурс]: NIST. – Режим доступу: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final.

6. Achieving Successful Outcomes With the NIST Cybersecurity Framework 0 [Електронний ресурс]: Govloop. – Режим доступу: https://www.govloop.com/resources/achieving-successful-outcomes-with-the-nist-cybersecurity-framework.

7. What Is the NIST Cybersecurity Framework? [Електронний ресурс]: Cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html.

8. OWASP Risk Rating Methodology [Електронний ресурс]: OWASP. – Режим доступу: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

9. OWASP Risk Rating Methodology [Електронний ресурс]: OWASP. – Режим доступу https://www.owasp-risk-rating.com.

10. OWASP Risk Rating Methodology: A Guide to Web Security Assessment [Електронний ресурс]: Frohrer. – Режим доступу https://blog.frohrer.com/owasp-risk-rating-methodology-a-guide-to-web-security-assessment.

11. Secure Development and Integration [Електронний ресурс]: OWASP. – Режим доступу: https://owasp.org/www-project-developer-guide/draft/foundations/secure_development.

12. ISA/IEC 62443 Series of Standards [Електронний ресурс]: ISA. – Режим доступу: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

13. ISA/IEC-62443-3-3: What is it and how to comply? [Електронний ресурс]: Cisco. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html.

14. Understanding IEC 62443 [Електронний ресурс]: IEC. – Режим доступу: https://www.iec.ch/blog/understanding-iec-62443.

15. Guide to Operational Technology (OT) Security: NIST Publishes SP 800-82, Revision 3 [Електронний ресурс]: NIST. – Режим доступу: https://www.nist.gov/news-events/news/2023/09/guide-operational-technology-ot-security-nist-publishes-sp-800-82-revision.

16. NIST SP 800-82 Rev. 3 [Електронний ресурс]: NIST. – Режим доступу: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

17. Guide to Industrial Control Systems (ICS) Security [Електронний ресурс]: NIST. – Режим доступу: https://www.nist.gov/publications/guide-industrial-control-systems-ics-security.

18. Securing industrial networks: What is ISA/IEC 62443? [Електронний ресурс]: Cisco. – Режим доступу: https://blogs.cisco.com/security/securing-industrial-networks-what-is-isa-iec-62443.

19. The Essential Guide To ISA IEC 62443 [Електронний ресурс]: Waterfall Security. – Режим доступу: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/the-essential-guide-to-isa-iec-62443.

20. C2M2 Version 2.1 [Електронний ресурс]: Department of Energy. – Режим доступу: https://c2m2.doe.gov.

21. Cybersecurity Capability Maturity Model to NIST Cybersecurity Framework Mapping [Електронний ресурс]: NIST. – Режим доступу: https://www.nccoe.nist.gov/news-insights/cybersecurity-capability-maturity-model-nist-cybersecurity-framework-mapping.

22. Cybersecurity Capability Maturity Model (C2M2) – Overview [Електронний ресурс]: Axio. – Режим доступу: https://axio.com/insights/cybersecurity-capability-maturity-model-c2m2-overview.

23. What is ITIL? [Електронний ресурс]: Axelos. – Режим доступу: https://www.axelos.com/certifications/itil-service-management/what-is-itil.

24. ITIL 4 Information security and risk management practices: embedding safety culture and behaviour [Електронний ресурс]: Axelos. – Режим доступу: https://www.axelos.com/resource-hub/blog/itil-4-information-security-and-risk-management-practices.

25. ITIL 4 [Електронний ресурс]: IT Process Maps. – Режим доступу: https://wiki.en.it-processmaps.com/index.php/ITIL_4.

26. What is IT Infrastructure Library (ITIL)? [Електронний ресурс]: IBM. – Режим доступу: https://www.ibm.com/topics/it-infrastructure-library.

27. ISO/IEC 27001:2022 [Електронний ресурс]: ISO. – Режим доступу: https://www.iso.org/standard/27001.

28. New version of ISO/IEC 27001 to better tackle IT security risks [Електронний ресурс]: ISO. – Режим доступу: https://www.iso.org/news/2013/08/Ref1767.html.

29. ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide [Електронний ресурс]: Advisera. – Режим доступу: https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management.

30. The complete guide to ISO 27001 risk assessment [Електронний ресурс]: Hightable. – Режим доступу: https://hightable.io/iso-27001-risk-assessment-guide.

31. NIST CSF vs. ISO 27001: Understanding the Key Differences [Електронний ресурс]: Scytale. – Режим доступу: https://scytale.ai/resources/nist-csf-vs-iso-27001-understanding-the-key-difference.

32. Publicly Available Standards [Електронний ресурс]: ISO. – Режим доступу: https://standards.iso.org/ittf/PubliclyAvailableStandards.

33. Ю. Є. Яремчук, О. В. Салієва. Оцінювання рівня захищеності об’єктів критичної інфраструктури // Матеріали науково-практичної конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання – 2020.

34. General Data Protection Regulation [Електронний ресурс]: Intersoft Consulting. – Режим доступу: https://gdpr-info.eu.

35. Health Insurance Portability and Accountability Act of 1996 (HIPAA) [Електронний ресурс]: Centers for Disease Control and Prevention. – Режим доступу: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

36. PCI Data Security Standard (PCI DSS) [Електронний ресурс]: Centers for Disease Control and Prevention. – Режим доступу: https://www.pcisecuritystandards.org/standards/pci-dss.

37. Stine K. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Ukrainian Translation) [Електронний ресурс]: NIST. – Режим доступу: https://doi.org/10.6028/nist.cswp.04162018uk.

38. Батечко С. В., Лебедєва О. Ю. Методика оцінки захищеності інформаційних систем. Інформатика та математичні методи в моделюванні. 2021. Т. 11, № 3.

39. Формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації / Д. С. Комін та ін. Системи озброєння і військова техніка. 2018. № 4(56). С. 92–99.

40. A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045 [Електронний ресурс]: H. Chen et al. – Режим доступу: https://doi.org/10.1007/978-3-662-45402-2_18923.

41. Common criteria for the assessment of critical infrastructures. [Електронний ресурс]: International Journal of Disaster Risk Science. – Режим доступу: https://doi.org/10.1007/s13753-011-0002-y.

42. The Ultimate Beginner's Guide to Threat Modeling [Електронний ресурс]: Shostack + Associates. – Режим доступу: https://shostack.org/resources/threat-modeling.

43. Threat modeling explained: A process for anticipating cyber attacks [Електронний ресурс]: CSO Online – Режим доступу: https://www.csoonline.com/article/569225/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html.

44. The STRIDE Threat Model [Електронний ресурс]: Microsoft. – Режим доступу: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

45. Applying STRIDE [Електронний ресурс]: Microsoft. – Режим доступу: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee798544(v=cs.20).

46. Attack Trees [Електронний ресурс]: Schneier on Security. – Режим доступу: https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

47.What You Need to Know About Attack Trees [Електронний ресурс]: EC-Council. – Режим доступу: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/attack-trees-cybersecurity.

48. How mapping the Ocean's Eleven heist can make you better at application security testing [Електронний ресурс]: Synopsys. – Режим доступу: https://www.synopsys.com/blogs/software-security/attack-tree-diagram.html.

49. Internet Security Glossary, Version 2 [Електронний ресурс]: Network Working Group, R. Shirey. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc4949.

50. MITRE ATT&CK [Електронний ресурс]: MITRE. – Режим доступу: https://attack.mitre.org.

51. MITRE D3FEND [Електронний ресурс]: MITRE. – Режим доступу: https://d3fend.mitre.org.

52. What Are MITRE ATT&CK and MITRE D3FEND? [Електронний ресурс]: D3 Security. – Режим доступу: https://d3security.com/blog/mitre-attack-defend-explained.

53. Security/OSSA-Metrics [Електронний ресурс]: Openstack. – Режим доступу: https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD.

54. DREAD Threat Modeling Methodology [Електронний ресурс]: Practical DevSecOps. – Режим доступу: https://www.practical-devsecops.com/dread-threat-modeling.

55. Threat Modeling: The Ultimate Guide [Електронний ресурс]: Practical DevSecOps. – Режим доступу: https://www.splunk.com/en_us/blog/learn/threat-modeling.html.

56. How to Use DREAD Analysis with FAIR [Електронний ресурс]: FAIR Institute. – Режим доступу: https://www.fairinstitute.org/blog/how-to-use-dread-analysis-with-fair.

57. Threat Modeling with DREAD [Електронний ресурс]: Cyral. – Режим доступу: https://cyral.com/glossary/threat-modeling-with-dread.

58. DREAD [Електронний ресурс]: Alukos. – Режим доступу: https://ccsp.alukos.com/models/dread.

59. Threat Modeling [Електронний ресурс]: OWASP. – Режим доступу: https://owasp.org/www-community/Threat_Modeling.

60. PASTA Threat Modeling [Електронний ресурс]: Threat Modeling. – Режим доступу: https://threat-modeling.com/pasta-threat-modeling.

61. PASTA threat modelling – the complete cyber security meal [Електронний ресурс]: Cynance. – Режим доступу: https://www.cynance.co/pasta-threat-modelling.

62. Guide for PASTA Threat Modeling Methodology [Електронний ресурс]: Practical Devsecops. – Режим доступу: https://www.practical-devsecops.com/pasta-threat-modeling-methodology.

63. Threat Modeling Methodologies: What is VAST? [Електронний ресурс]: Threatmodeler. – Режим доступу: https://threatmodeler.com/threat-modeling-methodologies-vast.

64. What is Vast Modeling? Unleashing the Power of Cyber Security [Електронний ресурс]: Cyberinsight. – Режим доступу: https://cyberinsight.co/what-is-vast-modeling.

65. Stride, VAST, Trike, & More: Which Threat Modeling Methodology is Right For Your Organization? [Електронний ресурс]: ThreatModeler. – Режим доступу: https://threatmodeler.com/threat-modeling-methodologies-overview-for-your-business.

66. Threat Modeling Cheat Sheet [Електронний ресурс]: OWASP. – Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html.

67. Threat Modeling: Process, Frameworks, and Tools [Електронний ресурс]: HackerOne. – Режим доступу: https://www.hackerone.com/knowledge-center/threat-modeling-process-frameworks-and-tools.

68. Common Vulnerability Scoring System [Електронний ресурс]: First. – Режим доступу: https://www.first.org/cvss.

69. Common Vulnerability Scoring System [Електронний ресурс]: National Vulnerability Database. – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss.

70. What is Common Vulnerability Scoring System (CVSS) [Електронний ресурс]: SANS Institute. – Режим доступу: https://www.sans.org/blog/what-is-cvss.

71. Random Forests [Електронний ресурс]: Springer. – Режим доступу: https://link.springer.com/content/pdf/10.1023/A:1010933404324.pdf.

72. What is random forest? [Електронний ресурс]: IBM. – Режим доступу: https://www.ibm.com/topics/random-forest.

73. Random Forest: A Complete Guide for Machine Learning [Електронний ресурс]: Builtin. – Режим доступу: https://builtin.com/data-science/random-forest-algorithm.

74. Definitive Guide to the Random Forest Algorithm with Python and Scikit-Learn [Електронний ресурс]: Stack Abuse. – Режим доступу: https://stackabuse.com/random-forest-algorithm-with-python-and-scikit-learn.

75. Cross-validation: evaluating estimator performance [Електронний ресурс]: Scikit-learn. – Режим доступу: https://scikit-learn.org/stable/modules/cross_validation.html.

76. What is Cross-Validation? [Електронний ресурс]: Towards Data Science / Medium. – Режим доступу: https://towardsdatascience.com/what-is-cross-validation-60c01f9d9e75.

77. Mean, median, and mode review [Електронний ресурс]: Khan Academy. – Режим доступу: https://www.khanacademy.org/math/statistics-probability/summarizing-quantitative-data/mean-median-basics/a/mean-median-and-mode-review.

78. WEKA [Електронний ресурс]: Github. – Режим доступу: https://waikato.github.io/weka-site/index.html.

79. F1 Score in Machine Learning: Intro & Calculation [Електронний ресурс]: V7Labs. – Режим доступу: https://www.v7labs.com/blog/f1-score-guide.

80. AUC ROC Curve in Machine Learning [Електронний ресурс]: Geeks for geeks. – Режим доступу: https://www.geeksforgeeks.org/auc-roc-curve.

81. Classification: ROC Curve and AUC [Електронний ресурс]: Google. – Режим доступу: https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Андрій Віхров, Павло Ловигін, Тетяна Бабенко. Розробка моделі оцінки захищеності інформаційних систем. Проблеми кібербезпеки Інформаційно-Телекомунікаційних систем, PCSITS 2024, Київ – матеріали конференції, ст. 48 – 50.