Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

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

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітньої програми)

освітньо-наукова програма *кібербезпека*

на тему: «Модель оцінки захищеності ІС на об’єктах критичної інфраструктури»

Виконавець: студент ІІ курсу, групи КБм-21

(підпис) **Бужора Віктор Юрійович**
(прізвище ім’я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	Бабенко Т.В.		
Рецензент			
Нормоконтроль	Даков С.Ю.		

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«__» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту КБм-21 (група) Бужорі Віктору Юрійовичу (прізвище ім'я по-батькові)

Тема дипломної роботи Модель оцінки захищеності ІС на об'єктах критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес оцінювання рівня захищеності інформаційних систем КІ.
Предмет досліджень	Механізми захисту ІС об'єктів критичної інформаційної інфраструктури.
Мета	Розробка моделі оцінки захищеності ІС об'єктів критичної інфраструктури.
Вихідні дані для проведення роботи	Модель оцінки захищеності ІС об'єктів критичної інфраструктури

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Синтезована модель оцінки рівня зрілості процесів ІБ дозволяє оцінювати СУІБ, що побудовані з використанням різних стандартів ІБ

Практична цінність інтелектуальна модель оцінки рівня зрілості впроваджених процесів ІБ може бути використана, як елемент СУІБ ОКІІ

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)
Розробка плану для досягнення мети роботи	29.10.2021 – 23.01.2022
Аналіз літературних джерел	24.01.2022 – 14.02.2022
Розробка методу захисту від витоку даних платіжних карток через інтернет-браузер	15.02.2022 – 24.04.2022
Оформлення і друк пояснювальної записки	25.04.2022 – 19.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зменшення часових та фінансових витрат підприємств на проведення оцінки рівня захищеності ІС.

Соціальний ефект Покращення об’єктивності та ефективності оцінки рівня захищеності ІС.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка: 73 с., 4 рис., 4 табл., 1 додаток, 61 джерело.

Мета роботи: розробити модель оцінки захищеності ІС об’єктів критичної інфраструктури.

Об’єкт дослідження: процес оцінювання рівня захищеності інформаційних систем КІ.

Предмет дослідження: механізми захисту ІС об’єктів критичної інформаційної інфраструктури.

Методи дослідження: аналіз, синтез, імітаційне моделювання.

В основній частині роботи здійснено аналіз існуючих підходів до забезпечення інформаційної безпеки та визначено теоретичні засади вимог до середовища ІС та методів оцінки ефективності їх впровадження. Зроблено висновок, що існує необхідність об’єднання методологічних підходів, які викладено у поширених галузевих стандартах.

На основі проведеного порівняльного аналізу було визначено базову парадигму для розробки моделі оцінювання рівня захищеності інформаційних систем, алгоритм попередньої підготовки даних для навчання, виконано підготовку даних та виконано синтез та навчання пропонованої моделі. Визначено, що навчена модель описує реальний неавтоматизований процес оцінки зрілості ІС на прийнятному рівні, і її можна рекомендувати використовувати в процесі реальної перевірки.

Практичне значення полягає в тому, що запропонована в роботі інтелектуальна модель оцінки рівня зрілості впроваджених процесів ІБ може бути використана, як елемент СУІБ ОКІІ

Наукова новизна полягає в тому, що синтезована модель оцінки рівня зрілості процесів ІБ дозволяє оцінювати СУІБ, що побудовані з використанням різних стандартів ІБ та у випадку гетерогенної структури СУІБ отримати інтегральний показник рівня зрілості і відповідно захищеності ОКІІ.

Ключові слова: модель зрілості процесів, машинне навчання, захист критичної інфраструктури, міжнародні стандарти, загальні критерії, SCADA, алгоритм Decision Tree.

ЗМІСТ

ВСТУП

Актуальність. Сьогоднішній світ і наша держава особливо чутливі до будь-якої небезпеки техногенного та природного характеру. Збройні конфлікти, гібридні війни, епідемія Covid-19, розвиток кіберзлочинності та інші загрози становлять значний ризик для країн та суттєво підвищують уразливість важливих об’єктів інфраструктури, що мають велике значення для функціонування суспільства та безпеки населення.

Таке підґрунтя потребує підвищеної уваги у сфері захисту інфраструктури, що має стратегічне значення. Це, зокрема, підприємства оборонної галузі, електромережі, транспортні вузли та інші об’єкти, виведення з ладу, або порушення функціонування яких може негативно вплинути на стан національної безпеки і оборони, навколишнього природного середовища, заподіяти майнову шкоду та становити загрозу для життя і здоров'я людей [1].

Загальні компоненти критичної інфраструктури, які потребують врахування питань безпеки, включають промислові системи керування (Industrial Control Systems - ICS), експлуатаційні (операційні) технології (Operation Technology - OT), інформаційні технології (Information Technology - IT) та системи диспетчерського управління і збору даних (Supervisory Control And Data Acquisition - SCADA).

Інформаційні системи в критичній інфраструктурі мають власний набір специфікацій та особливостей, включаючи використання застарілих і запатентованих систем з недостатньою, або неактуальною документацією, відсутність підготовки персоналу у безпекових питаннях, високий рівень бюрократії та жорстко регламентоване правове і нормативне середовища, ризики безпеки, пов’язані з наявним фізичним обладнанням. Але чи не найважчим викликами є питання, пов’язані з кіберзагрозами та забезпеченням безперервності бізнесу.

Посилення кіберстійкості найважливіших систем для суспільства є пріоритетом для урядів держав та уповноважених інституцій, які забезпечують обмін досвідом та знаннями, об’єднуючи всі зацікавлені сторони, включаючи

державний та приватний сектор, наукові кола. Завдяки такому тісному партнерству ми працюємо разом, щоб зробити світ і нашу державу зокрема безпечнішим місцем.

Майже щодня інциденти доводять, що ризики, пов’язані з кібербезпекою, є високими, і відповідальність за ці інциденти несуть як окремі хакери, так і професійно організовані групи кіберзлочинців. Розуміння ризиків кібербезпеки та можливих контрзаходів має першорядне значення з огляду на ймовірність і вплив цих ризиків. В епоху кіберфізичних систем та Інтернету речей (IoT) кібербезпека виходить за рамки певної організації. Тим не менш, через постійно мінливу природу кібер ризиків, а також з постійним включенням нових активів, організації потребують цілісного та наполегливого підходу до кібербезпеки. Це дослідження зосереджено на кібербезпеці з організаційної точки зору, щоб допомогти загальним організаціям вирішувати проблеми кібербезпеки.

У результаті уваги, що приділяється кібербезпеці, у це десятиліття було проведено велику кількість наукових досліджень, які зростали інтенсивно. Проте було проведено мало досліджень щодо розробки системи покращення процесу на основі стандартів. Невелика кількість доступних фреймворків здебільшого базується на моделі зрілості можливостей (CMM), але вони отримали деякі критичні зауваження; в основному пов'язані з витратами на впровадження, застосовністю та надійністю [2].

Метою даної роботи є створення універсальної моделі оцінки захищеності ІС, яка буде зрозумілою і матиме потенціал застосування у реальному світі. Така модель повинна спростити та визначити основні підходи до процесу оцінки, не втративши при цьому достатності охоплення сфер.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

1. Виконати порівняльний аналіз міжнародних стандартів та визначити принцип застосування моделей зрілості у сфері ІБ;
2. Визначення базової парадигми моделі оцінювання;
3. Розробка алгоритму попередньої підготовки даних;
4. Підготовка даних для моделювання;

5. Синтезувати модель зрілості СУІБ з визначенням відповідності досліджуваної ІС на відповідність вимогам стандарту ISO/IEC 27001 з використанням технологій штучного інтелекту та здійснити її навчання;

6. Провести аналіз адекватності розробленої моделі.

Об’єктом дослідження є процес оцінювання рівня захищеності інформаційних систем КІ.

Предметом дослідження виступають механізми захисту ІС об’єктів критичної інформаційної інфраструктури.

При цьому, основними методами дослідження є системний аналіз, порівняння, моделювання та інші.

Наукова новизна полягає в тому, що синтезована модель оцінки рівня зрілості процесів ІБ дозволяє оцінювати СУІБ, що побудовані з використанням різних стандартів ІБ та у випадку гетерогенної структури СУІБ отримати інтегральний показник рівня зрілості і відповідно захищеності ОКІІ.

Практична цінність отриманих результатів полягає в тому, що запропонована в роботі інтелектуальна модель оцінки рівня зрілості впроваджених процесів ІБ може бути використана, як елемент СУІБ ОКІІ.

РОЗДІЛ 1
АНАЛІЗ НАЯВНИХ ПІДХОДІВ ДО ОЦІНКИ ЗАХИЩЕНОСТІ ТА ОСОБЛИВОСТІ ІС НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасне суспільство залежить від безпечного та надійного функціонування звичного стану речей: коли продукти виробляються і є доступними, а послуги надаються. Перерви в такій діяльності можуть призвести до значних збоїв із серйозними фінансовими та соціальними наслідками. Насамперед, комфортне існування такого світу є можливим завдяки ефективній та постійній роботі об'єктів критичної інфраструктури.

Сьогодні, з огляду на «нову норму» [3], пов'язану з пандемією, війною та складністю прогнозування ринкових відносин, захист критичної інфраструктури є однією з найбільш базових та гострих проблем, з якими доводиться мати справу керівництву держав та міжнародних організацій. Щоб підтримувати стабільність і безпеку регіону, громади та економіки, управлінці критичною інфраструктурою докладають великих зусиль, щоб успішно підтримувати свої системи безпеки та залишатися на плаву перед обличчям можливих загроз.

Критичні інфраструктури — це організації, які мають велике значення для держави та громади. Їх погіршення або вихід з ладу призводить до значних порушень громадської безпеки, тривалого колапсу поставок або інших серйозних наслідків. Саме об'єкти критичної інфраструктури працюють на передовій, щоб забезпечити безпеку та здоров'я мільйонів людей. Ось чому на цих об'єктах повинні особливо піклуватися про конфіденційність і безпеку.

За національним визначенням, об'єктами критичної інфраструктури слугують підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з

ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв. Об'єктом критичної інформаційної інфраструктури у свою чергу визначено комунікаційну або технологічну систему об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [4].

Як можна побачити навіть із формулювання визначень, Україна, як суб’єкт забезпечення безпеки, не надає чіткої дефініції, тому при означенні ОКІІ варто додатково посилатися на іноземні практики.

Наприклад [5] дуже широко визначає критичну інформаційну інфраструктуру. Автор статті відносить сюди будь-які дані, бази даних, мережу, комунікаційні інфраструктури (або їх частини) або все, що пов’язано з ними. Подібну класифікацію надає також і Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) [6].

У свою чергу, у публікації [7] науковці надають механізм, який можуть використовувати країни без сформованої нормативної бази. У цій роботі пропонується методологія, яка підтримує посилене визначення послуг ОКІІ на основі двох аналітичних компонентів: визначення основних зацікавлених сторін та ілюстративний каркас, який називається базується на отриманні постійного зворотного зв’язку між учасниками всього процесу.

Вразливості та загрози, пов’язані з критичними інфраструктурами, вже давно визнані ризиками. Як державні, так і приватні установи несуть відповідальність за захист населення від потенційних кібератак, від аварії на атомній електростанції до відкритої електричної мережі. Ось чому безпека критичної інфраструктури є важливою для захисту громадян від стихійних лих, терористичної діяльності та шкідливих кіберзагроз.

Атаки на критичні інфраструктури представляють нові та складні сценарії, які можуть поставити під загрозу ціле населення. Від атаки зловмисного програмного забезпечення Shamoon на нафтового гіганта Саудівської Аравії Aramco у 2017 році до атаки програмного забезпечення-вимагача в 2019 році, що спричинило зупинку

виробництва в Норвегії, за останнє десятиліття спостерігається значна частка атак на критичну інфраструктуру.

У сучасному підключеному мережею середовищі цифрові та фізичні системи зближуються та створюють нові проблеми кібербезпеки. В одному дослідженні дослідники виявили, що гіпотетична атака на електромережу США може призвести до нанесення шкоди 70-90% населення та бізнесу протягом 12 місяців [8].

З огляду на все це, нижче наведено п’ять основних ризиків і загроз для безпеки критичної інфраструктури, про які кожна організація повинна знати та від яких має бути готова захиститись.

1. Сегментація мережі

Сегментація мережі — це архітектурний підхід, який поділяє мережу на кілька сегментів, що дозволяє адміністраторам мережі контролювати потік трафіку на основі визначених політик адміністратора. У разі відсутності сегментації мережі погані суб’єкти можуть підключитися до мережевої інфраструктури організації та отримати доступ до цінних активів, таких як інформація про персонал, засоби захисту, або конфіденційна інформація як про інтелектуальну власність та ноу-хау.

2. DDoS-атаки

DDoS-атаки можуть пошкодити публічну хмарну інфраструктуру організації та вплинути на доступність підприємств, які використовують критичну інфраструктуру в хмарі. Цей вид зловмисної атаки може бути виснажливим для будь-якої організації, сповільнюючи роботу системи або час затримки запитів, споживаючи при цьому велику кількість процесорної потужності.

Сучасні зловмисники застосовують все більш складні способи здійснення атаки, які збільшують час реакції детектувальних систем, перш ніж сотні тисяч автоматизованих запитів на обслуговування можуть бути виявлені та перевірені. Це ускладнює IT-фахівцям визначення, які компоненти вхідного трафіку надходять від зловмисних суб’єктів, а які від законних користувачів.

3. Атаки веб-додатків

Оскільки традиційні системи OT, такі як інтерфейси управління людьми (HMI) і програмовані логічні комп’ютери (PLC), все частіше підключаються до

глобальної мережі, вони також доступні через віддалений доступ, що робить їх особливо вразливими. Незахищені та відкриті системи вразливі до міжсайтових сценаріїв та атак із застосуванням SQL-ін’єкцій.

Організаціям рекомендується використовувати мережі доставки вмісту (CDN) і брандмауери веб-додатків (WAF), а також ділитися важливими ресурсами з адміністраторами вищого рівня ієрархії під час виконання регулярних аудитів безпеки для виявлення вразливостей.

4. Атаки шкідливих програм (Malware)

Атаки зловмисного програмного забезпечення можуть мати руйнівний вплив на критичну інфраструктуру. Оскільки програмне забезпечення-вимагач є зброєю для багатьох хакерів, навряд чи ця тенденція зникне у найближчі кілька років. Атаки на міста США в 2019 році, включаючи Пенсаколу, Рів'єра-Біч і Лейк-Сіті, зробили недоступними на відчутний період часу державні служби, як-от урядову електронну пошту та навіть служби екстреної допомоги .

Шкідливе програмне забезпечення може призвести до втрати даних, пошкодити пристрої та викинути адміністраторів із системи в обмін на великі суми викупу, або виконання інших вимог зловмисників. Лише кілька прикладів шкідливого програмного забезпечення: NotPetya, Stuxnet, Shamoon і Dark Seoul. Ось чому дуже важливо, щоб системи OT, які є вразливими до атак, включали захист від шкідливого програмного забезпечення, засоби керування брандмауером на основі хоста та політику керування виправленнями, щоб зменшити ризик.

5. Введення команд і маніпулювання параметрами

Ін'єкції запитів і команд є одними з найбільш руйнівних класів вразливостей, які існують. Введення команд може відбуватися, коли неперевірений, контрольований користувачем ввід даних передається як дійсний для викликів виконання інструкцій. Небезпека виникає, коли зловмисник використовує динамічно створені команди, внаслідок яких відбудеться виконання потрібних зловмиснику дій на базових операційних системах, або інших рівнях інформаційної системи.

Несанкціоновані дані, які не були визначені як законний системний трафік, дають зловмиснику можливість виконувати довільні системні команди в системах ОТ, просто додаючи додаткові команди до призначеного командного рядка. Подібно до SQL-ін'єкції, початкова точка такого роду загроз починається, коли система не може належним чином перевірити введені користувачем дані [8].

Критичні інфраструктури також можуть бути атаковані опосередковано. Зловмисники часто створюють профілі співробітників і ставлять під загрозу їхні домашні мережі та кінцеві точки, намагаючись знайти конфіденційні дані, пов’язані з роботою, або використовувати скомпрометовані пристрої BYOD (Bring your own device), щоб отримати доступ до ресурсів критичної інфраструктури.

Наявність плану захисту критичної інфраструктури може допомогти організаціям підготуватися до серйозних інцидентів, пов’язаних із середовищем критичної інфраструктури, та запобігти їм. Щоб захистити від постійно зростаючого числа загроз, експерти з безпеки повинні регулярно перевіряти цілісність систем критичної інфраструктури, щоб переконатися, що вони протистоять унікальним загрозам і атакам.

Світ змінюється, цифрові та фізичні системи зближуються. Системи, які колись керували критичною інфраструктурою, підключаються до Інтернету та обмінюються конфіденційними даними. Ця нова структура світу несе з собою нові проблеми безпеки.

Збільшення цифровізації критичної інфраструктури призвело до того, що системи IT та OT стають дедалі складнішими, а внутрішні та зовнішні мережі об’єднані разом. Зовнішні загрози та внутрішні ризики постійно змінюються, що ще довго буде «новою нормою» [3].

Традиційно системи керування були відокремлені від відкритого Інтернету, оскільки вони були розгорнуті в мережах контрольованої зони та під жорсткою фізичною охороною. Поширення Інтернету речей, яке скорочує трудові та експлуатаційні витрати, забезпечуючи дистанційне керування та керування розумними перемикачами та розумними лічильниками з будь-якої точки світу, також привідкрило ці мережі кіберзлочинцям.

Розумні датчики та комунікаційні технології, об’єднані в різні промислові системи управління, піддають інфраструктури та організації ризику. Чим більше розумних пристроїв увімкнено та підключено до критично важливих інфраструктурних мереж, тим більша область потенційної атаки та потенційна шкода. Наприклад, один вразливий розумний датчик, підключений до Інтернету, може діяти як шлюз для розгортання атак або компрометації інших критично важливих систем у тій самій мережі, якщо його скомпрометують суб’єкти загрози.

Виявлення вразливостей та отримання інформації про кількість розумних пристроїв та їх роль в інфраструктурі може допомогти зменшити ризик успішної кібератаки. Отже, важливо вести детальний інвентар усіх IoT, постійно перевіряти наявність нових оновлень безпеки, які усувають відомі вразливості, і підтримувати їх в окремій мережі, яка повністю ізольована від інших критично важливих систем.

Ці операційні технології, такі як програмне та апаратне забезпечення, які можуть спричинити зміни фізичних пристроїв, процесів і подій, рідко мають функції безпеки чи навіть можливості відбивати загрози. Іноді через їх базові можливості це виключає можливість їх захисту за допомогою традиційних технологій безпеки. Станом на зараз відомо багато прикладів загроз, таких як BlackEnergy, Triton і навіть спалахи програм-вимагачів NotPetya і WannaCry, які вже мали руйнівний вплив на критичну інфраструктуру [9].

Щоб ефективно виявляти загрози для IoT або OT, ключовим фактором є видимість усієї інфраструктури. Щоб підвищити кіберстійкість та надійність роботи інфраструктури, критично важливо розгортати технології моніторингу мережі в реальному часі, які можуть виявляти ненормальну поведінку або навіть використовувати спроби, спрямовані на певні пристрої.

Консолідована видимість у кількох мережах і навіть у цілих об’єктах може допомогти командам безпеки швидко ідентифікувати та стримувати будь-яку загрозу, яка може переміщатися по інфраструктурі. Це також може допомогти командам з безпеки та IT розробити більш активний підхід до безпеки. Помітність, розвідка про загрози та розширена аналітика даних можуть допомогти передбачити

ризик і розробити комплексні стратегії захисту за допомогою практичних розвідувальних даних.

Більшість критичної інфраструктури, включаючи основні комунальні послуги, промислові мережі та транспортні системи, контролюються системами SCADA. Системи SCADA — це розумні, інтелектуальні системи керування, які отримують вхідні дані від різноманітних датчиків і, у багатьох випадках, реагують на систему в режимі реального часу за допомогою виконавчих механізмів під керуванням програми. Система SCADA може функціонувати як система моніторингу/нагляду, система управління або їх комбінація.

Перехід на IP-системи дає величезні економічні переваги в умовах жорсткої конкуренції. Отже, очікується, що все більше і більше систем перейдуть до систем на основі IP. Наприклад, переваги переходу від власної радіомережі до мережі на основі IP включають спільні мережеві ресурси для кількох програм, покращення мережі, такі як додаткове резервування та ємність у всіх програмах, спільні системи керування мережею та необхідність підтримувати лише один набір навичок для допоміжного персоналу на місці. Проте всі відомі вразливості та загрози, пов’язані з традиційним TCP/IP, також стають доступні для експлуатації, що робить це викликом для кібербезпеки SCADA. Хоча всі фактори ризику, пов’язані з IT-системами, стосуються систем SCADA, неможливо повністю накласти каркас IT-безпеки на системи SCADA [10].

Інформаційна система - організований набір елементів, що збирає, обробляє, передає, зберігає та надає дані. Інформаційна система складається із людей, обладнання, процесів, процедур, даних та операцій. Кожна інформаційна система включає в себе наступні компоненти [11]:

- структура системи;
- функції кожного елемента системи;
- вхід і вихід кожного елементу і системи в цілому;
- мета і обмеження системи та її окремих елементів.

Інформаційні системи в критичній інфраструктурі загалом мають власний набір специфікацій та особливостей та переважно є ще й кіберфізичними системами.

Кіберфізична (інтелектуальна) система — це автоматизована комп’ютерна система в гетеродинному середовищі, в якій механізм керується або контролюється за допомогою комп’ютерних алгоритмів та яка дозволяє з'єднати операції фізичної реальності з обчислювальними та комунікаційними інфраструктурами. У кіберфізичних системах фізичні та програмні компоненти глибоко переплетені між собою, здатні діяти в різних просторових і часових масштабах, демонструють численні й відмінні поведінкові модальності та здатні взаємодіяти один з одним у спосіб, який змінюється залежно від контексту [12, 13]. Кіберфізичні системи спрямовані на тісний зв'язок вбудованих систем для моніторингу та управління фізичними процесами за допомогою датчиків і виконавчих механізмів через засоби зв'язку з глобальними цифровими мережами

Приклади таких систем включають автономні автомобільні системи, медичний моніторинг, промислові системи керування, роботизовані системи, автоматичну авіоніку тощо.

На ІС сектору КІ часто звичною картиною є використання застарілих і запатентованих систем з недостатньою, або неактуальною документацією, відсутність підготовки персоналу у безпекових питаннях, високий рівень бюрократії та жорстко регламентоване правове і нормативне середовища, ризики безпеки, пов’язані з наявним фізичним обладнанням. Але чи не найважчим викликами є питання, пов’язані з кіберзагрозами та забезпеченням безперервності бізнесу. Об’єктам критичної інфраструктури часто не вистачає стійкості, і вони легко втрачають критичні функціональні можливості в разі несприятливих подій. Стратегії управління безперервністю для операторів критичної інфраструктури та мереж, які вони утворюють, також покладаються на функціональність інших взаємопов'язаних мереж. Збої в роботі можуть вплинути на суспільство, і з цієї причини забезпечення діяльності операторів критичної інфраструктури є важливим [14].

Згідно зі Звітом Світового економічного форуму про глобальні ризики [15], очікується, що кібератаки та крадіжки даних залишаться одними з найбільш довготривалих ризиків, з якими бізнес зіткнеться протягом наступних десяти років.

Хакери роками атакували критичні інфраструктури; важливо усвідомити, наскільки складно може бути захистити їх від зовнішніх та внутрішніх загроз. Організації КІ повинні звернути увагу на створення та дотримання вимог для покращення їхньої кібербезпеки [3].

Протягом останніх кількох років суб'єкти загроз постійно націлювалися на організації в енергетичному, комунальному та інших секторах. Кібератаки на критично важливу інфраструктуру стають дедалі складнішими та дедалі більш руйнівними, що призводить до вимикання систем, порушення роботи або навіть надання зловмисникам можливості дистанційно керувати ураженими системами.

Захищеність являє собою наявність дієвої адекватної системи технічних, організаційних та інших розвинених і ефективних процедур та засобів (механізмів) для безпечного функціонування інформаційної системи та досягнення нею поставлених цілей та прогнозованих результатів. Захищеність у рамках даної роботи варто розглядати як міру одночасно безпеки (умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [16]) та захисту інформації в системі (діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [17]).

Питання оцінки захищеності інформаційних систем не нове і не втрачає актуальності з початку та середини 1990-х років, коли світова наукова та професійна спільнота активно почала ним займатись.

Станом на сьогодні існує велика кількість стандартів, фреймворків та методологій, які мають спільні риси, але володіють різною складністю використання, сферою застосування та по-своєму описують основні принципи та підходи до оцінки захищеності. Проаналізувавши значну кількість матеріалів та співставивши їх з особливостями ОКІ, згаданими вище, варто виокремити частину із них, які або вже використовуються для оцінки захищеності ОКІ, або мають такий потенціал.

Оскільки ІС на ОКІ характеризуються високим рівнем бюрократії та суворо регулюються, до них ставляться вимоги проходження сертифікованої перевірки на ефективність впровадження КСЗІ. В Україні документом, який встановлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах від несанкціонованого доступу є НД ТЗІ 2.5-004-99 [18].

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі тощо) критичної інформації, а також для органів, які здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою [19].

У відповідності до використання даного нормативного документу, у науковій статті [20] на основі відомого методу аналізу ієрархій запропоновано функціональну модель розрахунку кількісного критерію оцінки захищеності ІТС, яка за рахунок обробки експертних оцінок, дозволяє отримати кількісний показник захищеності ІТС. На думку авторів статті, описаний механізм дає можливість спростити процедуру підбору експертів, уникнути специфіки обробки експертних даних, а також здійснити оцінювання ІТС в умовах обмежених обсягів статистики.

Також відомим, але складним у розумінні та використанні стандартом у царині оцінки стану захищеності є ISO 15408 Загальні критерії оцінки безпеки інформаційних технологій (далі Загальні критерії), які визначають функціональні вимоги безпеки (security functional requirements) та вимоги до адекватності реалізації функцій безпеки (security assurance requirements) [21].

При проведенні робіт з аналізу захищеності ІС, Загальні критерії часто рекомендується використовувати як основні критерії, що дозволяють оцінити рівень захищеності ІС з погляду повноти реалізованих у ній функцій безпеки та надійності реалізації цих функцій.

Хоча застосовність Загальних критеріїв обмежується механізмами безпеки програмно-технічного рівня, в них міститься також певний набір вимог до механізмів безпеки організаційного рівня та вимог щодо фізичного захисту, які безпосередньо пов'язані з функціями безпеки, що описуються.

Зокрема варто відзначити роботи Да Бао [22] та Александера Фекете [23], які досить широко підійшли до пояснення і застосування принципів міжнародного стандарту. Тут розглядається саме їх науковий доробок, оскільки ці автори надають ґрунтовний аналіз Загальних критеріїв.

Да Бао зумів поєднати ISO 15408 та ISO 18045 (про які також йтиме мова у наступному розділі цієї роботи) та надав власне бачення контролів, які потрібні для перевірки та відповідні метрики їх оцінювання. Результатом його роботи стали 674 детальних оцінювальних завдання. Їх слідування мало б спростити розуміння стандарту та полегшити процес самої оцінки, тим самим дозволивши зменшити рівень гранично допустимий набір експертизи осіб, які проводитимуть оцінку. Фактично, такий підхід організовано у вигляді своєрідного чеклиста.

У свою ж чергу, Александра Фекете намагався надати нового значення “критичності” та описати принцип відбору елементів, яким її варто присвоювати і чому. Його робота вирізняється тим, що стосується якраз застосування Загальних критеріїв у оцінюванні ІС ОКІ у загальному випадку та у Німеччині зокрема.

Про застосування Загальних критеріїв для отримання відомостей стосовно рівня захищеності можна прочитати не тільки в іноземних публікаціях, але й у працях українських науковців. Наприклад у роботі [24] на основі загальних критеріїв була запропонована формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації, яка може розглядатися як базова та застосовуватись для подальших досліджень процесу оцінювання гарантій інформаційної безпеки.

Автори [25, 26] розглядають Загальні критерії разом із іншими міжнародними стандартами, замислюючись над тим, аби знайти найбільш універсальну методику проведення оцінки захищеності ІС та гарантій ІБ, охопити достатньо обширну сферу, задіяну під час перевірки. В обох цих роботах автори дійшли висновку, що стандарт ISO 15408 може слугувати еталонною методологією із запропонованої таксономії стандартів, але, разом із тим, вимагає значного рівня професійності експертів, які проводять таку оцінку. Даний висновок значно обмежує потенціал використання Загальних критерій.

Додатково заслуговує на згадку Платформа для підвищення кібербезпеки критично важливих інфраструктур [27], яка опублікована NIST та забезпечує спільну мову для розуміння, управління та вираження ризику для кібербезпеки для внутрішніх та зовнішніх зацікавлених сторін. Вона може використовуватися для того, щоб допомогти визначати та встановлювати пріоритетні заходи щодо зниження ризику для кібербезпеки і є інструментом для узгодження політичних, ділових та технологічних підходів до управління цим ризиком. Вона може використовуватися для управління ризиком для кібербезпеки в усій організації або може зосереджуватися на наданні важливих послуг в рамках організації. Різні типи організацій, включаючи сектор, який координує структури, асоціації та організації, можуть використовувати Платформу для різних цілей, включаючи створення загальних Профілів.

Основа платформи провадить комплекс заходів для досягнення конкретних результатів кібербезпеки та посилання на приклади керівних принципів для досягнення цих результатів. Основа не є контрольним списком для дій. Вона представляє основні результати в галузі кібербезпеки, визначені зацікавленими сторонами як корисні для управління ризиком для кібербезпеки. Основа містить чотири елементи: Функції, Категорії, Підкатегорії та Інформаційні посилання.

Інформаційні посилання - це конкретні розділи стандартів, керівних принципів та практик, що є загальними для секторів критично важливих інфраструктур, які ілюструють метод досягнення результатів, пов'язаних із кожною Підкатегорією. Інформаційні посилання, представлені в Основі платформи, є ілюстративними, а не вичерпними. Вони базуються на міжгалузевих керівних принципах, найчастіше згаданих під час процесу розробки Платформи. Таким чином, застосування Платформи дозволяє використовувати схему пов’язаних контролів між різними стандартами [27].

Висновки за розділом 1

Кібератаки на критичні інфраструктури можуть мати значний економічний вплив, особливо якщо вони спрямовані на конфлікт між державами. Захист цих кіберфізичних систем — це не питання повного повернення до фізичного доступу, а питання розуміння того, як працюють системи керування, підключені до Інтернету, як вони налаштовані та як до них отримують доступ. Наочність і керування є ключовими для посилення безпеки для систем SCADA і ICS, але фахівці з безпеки та IT повинні знати про ризики та встановлювати засоби контролю безпеки, спрямовані на зменшення впливу потенційної кібератаки та збільшення вартості атаки для суб'єктів загроз.

Майже щодня інциденти доводять, що ризики, пов'язані з кібербезпекою, є високими, і відповідальність за ці інциденти несуть як окремі хакери, так і професійно організовані групи кіберзлочинців. Розуміння ризиків кібербезпеки та можливих контрзаходів має першорядне значення з огляду на ймовірність і вплив цих ризиків. В епоху кіберфізичних систем та Інтернету речей (IoT) кібербезпека виходить за рамки певної організації. Тим не менш, через постійно мінливу природу кіберризиків, а також з постійним включенням нових активів, організації потребують цілісного та наполегливого підходу до кібербезпеки. Це дослідження зосереджено на кібербезпеці з організаційної точки зору, щоб допомогти загальним організаціям вирішувати проблеми кібербезпеки.

У результаті уваги, що приділяється кібербезпеці, у це десятиліття було проведено велику кількість наукових досліджень, які зростали інтенсивно. Проте наявні рішення не можуть повністю задовольнити потребу отримання оцінки захищеності через особливості кіберфізичних систем на об'єктах КІ та обмежений ресурс, які на це виділяється.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

У результаті уваги, що приділяється кібербезпеці, у це десятиліття було проведено велику кількість наукових досліджень, які зростали інтенсивно . Проте було проведено мало досліджень щодо розробки системи покращення процесу на основі стандартів. Невелика кількість доступних фреймворків здебільшого базується на моделі зрілості можливостей (CMM) [28], але вони отримали деякі критичні зауваження, пов'язані з витратами на впровадження, застосовністю та надійністю.

Тому в цьому розділі буде розглянуто як уже відомі підходи до проведення оцінки захищеності, так і міжнародні стандарти з кращими практиками, які ляжуть в основу для розробки власної інтелектуальної моделі.

2.1 Аналіз Cybersecurity Capability Maturity Model (C2M2)

Модель зрілості можливостей кібербезпеки (C2M2) [29] є інструментом для оцінки та покращення кібербезпеки. Він був розроблений у 2012 році енергетичним сектором США та Міністерством енергетики (DOE). C2M2 керується Управлінням кібербезпеки, енергетичної безпеки та реагування на надзвичайні ситуації (CESER) Міністерства охорони здоров’я, відділом кібербезпеки для систем доставки енергії (CEDS). Відділ CEDS CESER просуває дослідження, розробку та впровадження інноваційних технологій, інструментів і методів для зниження ризику для енергетичної інфраструктури країни.

Мета C2M2 полягає в тому, щоб допомогти організаціям усіх секторів, типів і розмірів оцінити та покращити свої програми кібербезпеки та підвищити їхню операційну стійкість. C2M2 зосереджено на впровадженні та управлінні методами кібербезпеки, пов’язаними з активами інформаційних технологій (IT) та операційних технологій (OT), а також середовищами, в яких вони працюють.

Домен – це перелік методів кібербезпеки, зосереджених на певній предметній області. Кожен із 10 доменів моделі містить структурований набір методів кібербезпеки. Кожен набір практик представляє діяльність, яку організація може виконувати для створення та розвитку потенціалу в домені. Наприклад, домен управління ризиками – це група практик, які організація може виконувати для створення та розвитку можливостей управління кібер ризиками [29].

Практика в кожному домені організована в цілі, які представляють досягнення кібербезпеки, які можуть бути досягнуті шляхом впровадження практик у домені. Наприклад, домен управління ризиками включає п’ять цілей:

- створити та підтримувати стратегію та програму управління кібер ризиками;
- визначте кібер ризик;
- проаналізуйте кібер ризики;
- відповідь на кібер ризик;
- управлінська діяльність.

Для вимірювання прогресу C2M2 використовує шкалу 1-3 рівнів індикатора зрілості. Кожен рівень представляє атрибути зрілості, які описані в таблиці 2.1 [30]. Організації, які впроваджують методи кібербезпеки в кожній MIL, досягають цього рівня. Наявність вимірних перехідних станів між рівнями дозволяє організації використовувати шкалу для визначення поточного та більш зрілого майбутнього стану; і визначити можливості, які він повинен досягти, щоб досягти цього майбутнього стану.

Таблиця 2.1

Рівні зрілості за моделлю C2M2

Рівень показника зрілості	**Опис рівня**
0	Модель не містить цілей для досягнення рівня 0. Ефективність на рівні 0 просто означає, що рівня 1 у даному домені не досягнуто

Продовження табл.2.1

1	У кожному домені рівня 1 міститься набір початкових заходів. Для досягнення рівня 1 ці початкові заходи можуть виконуватися спеціально, але вони повинні виконуватися
2	Виконання організацією заходів є стабільнішим. На рівні 2 організація може бути впевненішою в тому, що ефективність доменних практик буде підтримуватися з часом
3	На рівні 3 практика у домені стабілізується і керується організаційними директивами високого рівня, такими як політика безпеки

Модель C2M2 має описовий характер. Зміст моделі представлений на високому рівні абстракції, так що її можуть інтерпретувати організації різних типів, структур та розмірів. Станом на кінець 2021 року, більше 40% компаній, які використовували дану модель належали до енергетичного сектору.

2.2 Аналіз Community Cyber Security Maturity Model (CCSMM)

Community Cyber Security Maturity Model — це скоординований план, який надає громадам або місцевим юрисдикціям основу для визначення того, що необхідно для побудови програми кібербезпеки, зосередженої на готовності «всього суспільства» та реагуванні на кіберінцидент або атаки. По суті, CCSMM є посібником, який допомагає громадам встановити базовий рівень кібербезпеки на місцевому рівні. Його також можна використовувати для спілкування з окремими особами та спільнотами про можливості та вдосконалення [31].

Стратегії, визначені в описі моделі також може виходити за рамки захисту систем і мереж у місцевих державних установах. CCSMM може допомогти громадам визначити, що необхідно зробити для створення життєздатної та стійкої програми кібербезпеки, що необхідно для підготовки до виявлення кібератаки, розробки планів реагування під час атаки та визначення, що робити після атаки.

CCSMM включає в себе три важливі функції [31]:

● показник, який можна використовувати для вимірювання поточного стану програми кібербезпеки громади та її позиції;

● дорожня карта, яка допоможе спільноті знати, які кроки необхідні для покращення їхньої безпеки;

● загальна точка відліку, яка дозволяє людям з різних спільнот і штатів обговорювати свої індивідуальні програми та пов’язувати їх один з одним.

Тривимірна модель розроблена для розширення можливостей фреймворка, що дозволяє йому бути гнучким для вирішення всіх аспектів програми кібербезпеки. Розширення CCSMM у тривимірну модель забезпечує прогрес покращення.

CCSMM може допомогти громадам визначити, що необхідно зробити для створення життєздатної та стійкої програми кібербезпеки, що необхідно для підготовки до виявлення кібератаки, розробки планів реагування під час атаки та визначення, що робити після атаки. відбулося. Щоб отримати більш глибоке розуміння різних рівнів і розмірів у моделі, див. нижче для отримання додаткової інформації.

У моделі CCSMM існує п’ять рівнів зрілості для організацій, громад та держав, які прогресують по кожному з них у порядку, наведеному в таблиці 2.2 [30].

Таблиця 2.2

Рівні зрілості за моделлю CCSMM

Рівень зрілості	**Опис рівня**
Рівень 1, "Початковий"	Організації, громади та держави на цьому рівні мають незначну інформацію про кібербезпеку, її аналіз та оцінку або зовсім відсутні
Рівень 2, “Створено”	Керівництво організацій, громад та держав цього рівня усвідомлює кіберзагрози, проблеми та необхідність прийняття кібербезпеки. Вони також визнають необхідність спільного навчання та освіти в галузі кібербезпеки

Продовження табл.2.2

Рівень 3, “самооцінювання”	На цьому рівні керівники організацій, громад та держав активно пропагують обізнаність щодо кібербезпеки та співпрацюють з іншими у створенні навчальних та освітніх програм
Рівень 4, “Інтегрований”	Коли кібербезпека інтегрована, вона включається в кожен процес, коли організація, громада чи держава мають чітко визначені програми
Рівень 4, “Постійне покращення”	Для організацій, громад та держав на цьому рівні кібербезпека є імперативом бізнесу. Суб’єкти на цьому рівні здатні навчати інших

2.3 Приклад іншого типу моделі The Cybersecurity Focus Area Maturity (CYSFAM) Model

Focus Area Maturity (FAM) має на меті забезпечити повне охоплення домену, для якого він розроблений, представляючи можливості, які несе в собі домен, і позиціонуючи можливості в матриці відносно один одного відповідно до їхніх залежностей. FAM складаються з кількох напрямків. Кожна зона фокусування містить унікальні можливості (2–6), які позначаються з великої літери [32]. Будівельний блок FAM, здатність, визначається як «здатність досягати заздалегідь визначеної мети, яка пов’язана з певним рівнем зрілості» [33].

CYSFAM охоплює 11 фокусних областей (субдоменів) у сфері кібербезпеки. Ці напрямки згруповані в дві категорії: технічні та організаційні, щоб полегшити розуміння та керованість. Оскільки CYSFAM є моделлю зрілості, вона містить компоненти оцінки та вимірювання. 144 питання оцінки для оцінки можливостей кібербезпеки становлять велику частину моделі, і вони включені в окремий звіт, який є у відкритому доступі. Візуальне представлення та супровідний опис можливостей кібербезпеки в CYFAM можуть дати можливість організаціям сформулювати план впровадження своїх можливостей. Оскільки CYSFAM був

оцінений експертами з кібербезпеки та продемонстрований на прикладі компанії, він забезпечує міцну основу для створення організацій [34].

Загалом особливості використання подібного підходу до сфери оцінки захищеності запропоновано вперше саме авторами [34]. Така модель має спільні риси із більш поширеними, які базуються на рівнях зрілості, та, разом із тим пропонує дещо інший погляд на стан речей, але недолік застосування конкретно цієї моделі полягає у відсутності використання її у реальних випадках оцінювання поза дослідницьким середовищем.

2.4 Сфера застосування ISO 27001та ISO 27002

Структура ISO — це комбінація політик і процесів, які можуть використовувати організації. ISO 27001 забезпечує структуру, яка допомагає організаціям будь-якого розміру або галузі захищати свою інформацію систематичним і економічно ефективним способом, шляхом впровадження системи управління інформаційною безпекою (СУІБ) [35].

Цей стандарт не тільки надає компаніям необхідні ноу-хау для захисту їхньої найціннішої інформації, але компанія також може отримати сертифікацію відповідно до ISO 27001 і, таким чином, довести своїм клієнтам і партнерам, що вона захищає їхні дані.

Основною метою ISO 27001 є захист трьох аспектів інформації [35]:

- конфіденційність: доступ до інформації мають лише уповноважені особи;
- цілісність: змінювати інформацію можуть лише уповноважені особи;
- доступність: інформація має бути доступною уповноваженим особам, коли це необхідно.

Захист тріади CIA здійснюється шляхом з’ясування, які потенційні проблеми можуть виникнути з інформацією (тобто, оцінки ризику), а потім визначення того, що необхідно зробити, щоб запобігти виникненню таких проблем (тобто, зменшення ризику або уникнення ризику).

Таким чином, основна філософія ISO 27001 заснована на процесі управління ризиками: з’ясувати, де знаходяться ризики, а потім систематично обробляти їх за допомогою впровадження контролю безпеки (або гарантій).

Є чотири суттєві переваги для бізнесу, які компанія може отримати із впровадженням цього стандарту інформаційної безпеки, які перелічені нижче [36].

Дотримання юридичних вимог – існує постійно зростаюча кількість законів, нормативних актів та договірних вимог, пов’язаних з інформаційною безпекою, і хороша новина полягає в тому, що більшість із них можна вирішити шляхом впровадження ISO 27001 – цей стандарт надає ідеальну методологію для того, щоб дотримуватись їх усіх.

Отримання конкурентної переваги – якщо ваша компанія отримала сертифікат, а ваші конкуренти – ні, ви можете мати перевагу перед ними в очах тих клієнтів, які дбайливо ставляться до захисту своєї інформації.

Менші витрати – головна філософія ISO 27001 полягає в запобіганні інцидентів безпеки – і кожен інцидент, великий чи малий, коштує грошей. Тому, запобігаючи їх, компанія може заощадити досить багато грошей – інвестиції в ISO 27001 набагато менші, ніж економія коштів, отримана в результаті.

Краща організація – як правило, компанії, що швидко розвиваються, не мають часу зупинятися і визначати свої процеси та процедури – як наслідок, дуже часто співробітники не знають, що, коли і ким потрібно робити. Впровадження стандарту ISO 27001 допомагає вирішувати такі ситуації, оскільки спонукає компанії записувати свої основні процеси (навіть ті, які не пов’язані з безпекою), дозволяючи їм скоротити час, який їхні співробітники витрачають.

Стандарт розділений на дві частини. Перша, основна частина складається з 11 пунктів (від 0 до 10). Друга частина, яка називається Додатком А, містить рекомендації щодо 114 цілей та засобів контролю.

Додаток А стандарту підтримує пункти та їх вимоги переліком засобів контролю, які не є обов’язковими, але вибираються як частина процесу управління ризиками.

Існує 14 «доменів», перерахованих у Додатку А ISO 27001, організованих у розділах А.5–А.18 [36].

А.5. Політики інформаційної безпеки: елементи керування в цьому розділі описують, як працювати з політиками інформаційної безпеки.

А.6. Організація інформаційної безпеки: засоби контролю, що забезпечують основу для впровадження та функціонування інформаційної безпеки, визначаючи її внутрішню організацію (наприклад, ролі, відповідальність тощо), а також через організаційні аспекти інформаційної безпеки, як-от управління проектами, використання мобільних пристроїв та дистанційну роботу.

А.7. Безпека людських ресурсів: засоби контролю щодо людей, які перебувають під контролем організації, їх найму, навчання і управління безпечним способом; також розглядаються принципи дисциплінарного стягнення та розірвання угод.

А.8. Управління активами: засоби контролю, які гарантують, що активи інформаційної безпеки (наприклад, інформація, пристрої обробки, пристрої зберігання тощо) визначені, що визначено відповідальність за їх безпеку та що люди знають, як поводитися з ними, відповідно до попередньо визначеної класифікації рівнів.

А.9. Контроль доступу: елементи керування в цьому розділі обмежують доступ до інформації та інформаційних активів, відповідно до реальних бізнес-потреб. Елементи керування призначені як для фізичного, так і для логічного доступу.

А.10. Криптографія: елементи керування, які забезпечують основу для правильного використання рішень шифрування для захисту конфіденційності, автентичності та/або цілісності інформації.

А.11. Фізична безпека та безпека навколишнього середовища: засоби контролю в цьому розділі запобігають несанкціонованому доступу до фізичних зон, а також захищають обладнання та засоби від компрометації в результаті людського або природного втручання.

A.12. Безпека операцій: елементи керування, що забезпечують безпеку IT-систем, включаючи операційні системи та програмне забезпечення, і захист від втрати даних. Крім того, засоби контролю в цьому розділі вимагають засобів для запису подій та створення доказів, періодичної перевірки вразливостей та вжиття запобіжних заходів для запобігання впливу аудиторської діяльності на операції.

A.13. Безпека зв'язку: елементи керування в цьому розділі захищають мережеву інфраструктуру та послуги, а також інформацію, яка проходить через них.

A.14. Придбання, розробка та обслуговування системи: засоби контролю в цьому розділі гарантують, що інформаційна безпека враховується під час придбання нових інформаційних систем або оновлення існуючих.

A.15. Взаємовідносини з постачальниками: засоби контролю в цьому розділі гарантують, що аутсорсингові дії, що здійснюються постачальниками та партнерами, також використовують відповідні засоби контролю інформаційної безпеки, а також описують, як контролювати ефективність захисту третьої сторони.

A.16. Управління інцидентами інформаційної безпеки: засоби контролю в цьому розділі забезпечують основу для забезпечення належної комунікації та обробки подій та інцидентів безпеки, щоб їх можна було вчасно вирішувати; вони також визначають, як зберегти докази, а також як вивчити інциденти, щоб запобігти їх повторенню.

A.17. Аспекти інформаційної безпеки управління безперервністю бізнесу: засоби контролю в цьому розділі забезпечують безперервність управління інформаційною безпекою під час збоїв і доступність інформаційних систем.

A.18. Відповідність (compliance): засоби контролю, наведені в цьому розділі, забезпечують основу для запобігання порушенням законодавства, закону, нормативно-правових актів і договорів, а також перевірку того, чи впроваджено інформаційну безпеку та чи діє вона відповідно до визначених політик, процедур і вимог стандарту ISO 27001.

Більш уважний розгляд цих доменів показує, що управління інформаційною безпекою стосується не лише IT-безпеки (тобто брандмауери, антивіруси тощо), а й

управління процесами, правовим захистом, управлінням людськими ресурсами, фізичним захистом тощо.

Яка різниця між ISO 27001 та 27002?

ISO 27001 визначає вимоги до системи управління інформаційною безпекою (СУІБ), тоді як ISO 27002 надає рекомендації щодо впровадження засобів контролю з ISO 27001, Додатку А.

Іншими словами, для кожного елемента керування ISO 27001 надає лише короткий опис, тоді як ISO 27002 надає детальні вказівки.

2.5 Необхідність застосування ISO 22301

В сучасних реаліях особливо важливо утримувати стійку позицію організації на ринку, а саме зберігати здатність компанії продовжувати працювати під час збоїв, тому Міжнародна організація зі стандартизації (ISO) випустила нову версію стандарту ISO 22301:2019.

ISO 22301:2019 – це визнаний на міжнародному рівні стандарт про систему менеджменту безперервності бізнесу (BCMS), який дозволяє будь-якій організації залишатися актуальною у сучасному бізнес-середовищі.

Цей стандарт гармонізовано з багатьма міжнародними стандартами системи менеджменту завдяки тому, що він заснований на структурі високого рівня (HLS), такими як: система менеджменту якості (ISO 9001), система екологічного менеджменту (ISO 14001), система менеджменту інформаційної безпеки (ISO 27001) і багато інших [37].

У разі виникнення надзвичайної ситуації багато підприємств та організацій повинні мати можливість зменшити збитки та продовжити роботу. ISO 22301 є міжнародним стандартом управління безперервністю бізнесу (BCM). ISO 22301 призначений для того, щоб допомогти організаціям запобігати, готуватися, реагувати та усувати непередбачувані та руйнівні інциденти. Для цього стандарт забезпечує практичну основу для створення та управління ефективною системою

безперервності бізнесу. ISO 22301 спрямований на захист організації від широкого спектру потенційних загроз та збоїв.

Застосування даного стандарту допомагає продемонструвати зацікавленим сторонам, що організація може швидко подолати збої в роботі, щоб забезпечити постійне та ефективне обслуговування.

У всьому світі у багатьох країнах діє законодавство, що визначає обов'язки організацій із планування дій у надзвичайних ситуаціях. Ці обов'язки часто включають впровадження управління безперервністю бізнесу. В результаті сертифікація ISO 22301 повинна вважатися необхідною для будь-якої організації, яка за законом зобов'язана брати участь у плануванні дій у надзвичайних ситуаціях, включаючи комунальні послуги, транспорт, охорону здоров'я тощо. Незалежно від того, чи потрібно конкретній компанії впроваджувати стандарт, щоб відповідати галузевим нормам чи ні, отримання сертифіката ISO 22301 може допомогти організації розвинути стійкість та покращити управління ризиками [38].

У цьому документі вказуються вимоги до впровадження, підтримки та вдосконалення системи управління безперервністю бізнесу для зменшення ймовірності виникнення, підготовки, реагування та відновлення після збоїв.

Вимоги, зазначені у цьому документі, є спільними та призначені для застосування у всіх організаціях або їх частинах, незалежно від типу, розміру та характеру організації. Ступінь застосування вимог залежить від операційного середовища та складності організації.

ISO 22301 застосовується до всіх типів та розмірів організацій, які хочуть [38]:

- впровадити, підтримувати та покращувати BCMS;
- прагнуть забезпечити відповідність заявленій політиці безперервності бізнесу;
- мати можливість продовжувати виробляти продукцію та надавати послуги на прийнятну зумовлену потужність під час збою;
- прагнуть підвищити свою стійкість з допомогою ефективного застосування BCMS.

Цей документ може використовуватися для оцінки можливості організації задовольняти власні потреби та зобов'язання щодо безперервності бізнесу.

Основною метою ISO 22301 є забезпечення безперервності поставок продуктів і послуг для бізнесу після настання руйнівних подій (наприклад, стихійних лих, техногенних катастроф тощо). Це робиться шляхом з'ясування пріоритетів безперервності бізнесу (за допомогою аналізу впливу на бізнес), які потенційні руйнівні події можуть вплинути на бізнес-операції (за допомогою оцінки ризиків), визначення того, що необхідно зробити, щоб запобігти подібним подіям, а потім визначення способів мінімального та нормального відновлення операцій в найкоротші терміни (тобто зниження ризику або інше його опрацювання). Таким чином, основна філософія ISO 22301 заснована на аналізі впливів та управлінні ризиками: з'ясувати, які види діяльності найбільш важливі та які ризики можуть на них вплинути, а потім систематично обробляти ці ризики.

Стратегії та рішення, які мають бути реалізовані, зазвичай мають форму політики, процедур та технічної/фізичної реалізації (наприклад, програмне забезпечення та обладнання). У більшості випадків організації не мають усіх засобів, обладнання та програмного забезпечення, тому впровадження ISO 22301 передбачатиме не лише встановлення організаційних правил (тобто написання документів), які необхідні для запобігання руйнівним інцидентам, але й розробку планує та розподіляє технічні та інші ресурси для забезпечення безперервності та відновлення ділової діяльності. Оскільки для такого впровадження буде потрібно керувати низкою політик, процедур, людей, активів тощо, ISO 22301 описує, як об'єднати всі ці елементи разом у Системі управління безперервністю бізнесу (BCMS).

2.6 Управління ризиками на прикладі NIST SP 800-37

NIST SP 800-37 (Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy), або RMF забезпечує гнучкий і адаптований семикроковий процес, який інтегрує кібербезпеку та конфіденційність, а також діяльність з управління ризиками ланцюга поставок у життєвий цикл розробки системи. NIST RMF пов'язаний з набором стандартів і

рекомендацій NIST для підтримки впровадження програм управління ризиками для відповідності вимогам Федерального закону про модернізацію інформаційної безпеки (FISMA), включаючи вибір контролів, впровадження, оцінку та постійний моніторинг. NIST оновив RMF для підтримки управління ризиками конфіденційності та включення ключових концепцій кібербезпеки та системної інженерії. Спочатку націлений на федеральні агентства, сьогодні RMF також широко використовується державними та місцевими агентствами та організаціями приватного сектора [39].

Ця публікація (стандарт) описує систему управління ризиками та надає рекомендації щодо застосування RMF до інформаційних систем та організацій. RMF забезпечує дисциплінований, структурований і гнучкий процес для управління ризиками безпеки та конфіденційності (privacy), що включає категоризацію інформаційної безпеки; вибір, виконання та оцінку контролів; дозволи системних та загальних контролів; і постійний моніторинг.

RMF включає заходи з підготовки організацій до застосування документу на належних рівнях управління ризиками. RMF також сприяє управлінню ризиками майже в режимі реального часу та діючими контролями інформаційної системи, шляхом впровадження процесів безперервного моніторингу; надає керівникам вищого рівня та виконавцям необхідну інформацію для прийняття ефективних, економічно ефективних рішень щодо управління ризиками щодо систем, які підтримують їхні цілі та бізнес-функції; і включає безпеку та конфіденційність у життєвий цикл розробки системи.

Виконання завдань RMF пов’язує основні процеси управління ризиками на рівні систем з процесами управління ризиками на рівні організації. Крім того, він встановлює відповідальність та підзвітність за контроль, запроваджений в інформаційних системах організації та успадкований цими системами.

При розробці стандартів і рекомендацій NIST консультується з федеральними агентствами, штатними, місцевими урядами та організаціями приватного сектору. Це дозволяє уникнути непотрібного та дорогого дублювання зусиль і гарантує, що

його публікації доповнюють стандарти та інструкції, які вже використовується для захисту систем національної безпеки

RMF цілеспрямовано розроблено, щоб бути технологічно нейтральним, щоб методологія могла бути застосовна до будь-якого типу інформаційної системи без змін. Для специфічних контролів деталі реалізації контролю, а також методи та об'єкти оцінки контролю можуть відрізнятися з різними типами IT-ресурсів, але немає потреби налаштовувати процес RMF для відповідності специфічним технологіям.

Вважається, що організації повинні максимально використовувати автоматизацію, де це можливо, для збільшення швидкості та ефективності виконання кроків у рамках системи управління ризиками.

Ця публікація покликана допомогти організаціям керувати ризиками безпеки та конфіденційності, а також задовольняти вимоги FISMA та інших нормативних документів США. Хоча RMF є обов'язковим для використання федеральним урядом, він може застосовуватися до будь-якого типу не федеральних організацій (наприклад, бізнесу, промисловості, науки).

У RMF є сім кроків; підготовчий крок для забезпечення готовності організацій до виконання процесу та шість основних кроків. Усі сім кроків необхідні для успішного виконання RMF [40].

Prepare. Підготовка до виконання RMF з точки зору організації та системи, встановивши контекст і пріоритети для управління ризиками безпеки та конфіденційності.

Categorize. Класифікація системи та інформації, що обробляється, зберігається і передається системою на основі аналізу впливу втрат.

Select. Вибір початкового набору засобів контролю для системи та адаптація засобів контролю відповідно до потреби для зниження ризику до прийнятного рівня на основі оцінки ризику.

Implement. Запровадження засобів контролю та опис, як вони використовуються в системі та середовищі її функціонування.

Assess. Оцінка засобів контролю, щоб визначити, чи вони запроваджені правильно, чи працюють за призначенням та чи дають бажані результати щодо задоволення вимог безпеки та конфіденційності.

Authorize. Санкціонування системи, або загальних засобів контролю на основі визначення, що ризик для організаційних операцій та активів, окремих осіб, інших організацій та країни є прийнятним.

Monitor. Моніторинг на постійній основі системи та пов'язаних з нею засобів контролю, включаючи оцінку ефективності контролю, документування змін у системі та середовищі функціонування, проведення оцінки ризиків та аналізу впливу, а також звітування про стан безпеки та конфіденційності системи.

2.7 Сфера застосувння та підходи ITIL 4

ITIL 4 надає цифрову операційну модель, яка дозволяє організаціям спільно створювати ефективну цінність своїх продуктів і послуг, що підтримуються IT.

ITIL 4 спирається на десятиліття прогресу ITIL, розвиваючи усталені методи ITSM для ширшого контексту клієнтського досвіду, потоків створення цінності та цифрової трансформації. ITIL — це всесвітньо визнана, провідна у світі структура для управління IT-послугами (ITSM) — і все більше для загального управління послугами, що забезпечує цінність бізнесу [41].

Тепер, у своїй четвертій ітерації, випущеній взимку 2019 року, ITIL 4 надає вказівки, необхідні для вирішення нових проблем управління послугами та використання потенціалу сучасних технологій в епоху хмари, Agile, DevOps та трансформації.

Ключовими компонентами фреймворка ITIL 4 є система цінності послуг ITIL (SVS) і чотиривимірна модель.

Система цінності послуг ITIL забезпечує гнучку операційну модель для створення, надання та постійного вдосконалення послуг. Основними компонентами ITIL SVS є: ланцюг створення вартості послуг, практика, керівні принципи, управління та постійне вдосконалення.

Чотири виміри описують збалансований акцент на ITIL SVS через цілісний та ефективний підхід [42]:

- організації та люди;
- інформація та технології;
- партнери та постачальники;
- потоки та процеси створення цінностей.

Ці компоненти є значною еволюцією ITIL від попередніх ітерацій. Від конкретного зосередження на наданні послуг до ширшої точки зору цінності, створеної продуктами та послугами, які надаються клієнту. ITIL 4 розроблений для забезпечення плавного переходу від наявних інвестицій організації в ITIL та її поточного способу роботи до швидшого, більш гнучкому та гнучкому підходу.

Поширеною критикою фреймворку ITIL V3 було те, що в ньому бракує набору загальних принципів для розробки та виконання процесів ITSM. ITIL V3 іноді вважався стандартом, що надто наказує, оскільки він вказував IT-організаціям, які процеси впроваджувати і коли, але часто не пояснював, чому і як процесом слід керувати певним чином.

Щоб вирішити цю проблему, структура ITIL 4 включає набір із семи керівних принципів, яких фахівці ITIL можуть дотримуватися, прагнучи створити цінність для своїх IT-організацій. Ці керівні принципи можуть відігравати важливу роль у прийнятті рішень IT та допомагати IT-менеджерам розробляти власні стратегії та висновки у випадках, коли структура ITIL не надає чітких рекомендацій. Нижче ми описуємо кожен із семи нових керівних принципів ITIL 4 [41].

Робити фокус на цінності (Focus on value). Перший керівний принцип ITIL нагадує практикам, що вони завжди повинні бути зосереджені на забезпеченні цінності бізнесу, прямо чи опосередковано, за допомогою ефективного управління IT-послугами.

Відштовхуватися від поточної позиції (Start where you are). Другий провідний принцип ITIL нагадує організаціям не викидати свої існуючі системи під час прийняття платформи ITIL 4. Натомість організаціям заохочується зберігати

можливості, які відповідають їхнім потребам, удосконалювати їх, коли це необхідно, і розвивати нові, коли потрібно.

Рухатись ітеративно, використовуючи зворотний зв'язок (Progress iteratively with feedback). Великі зміни, навіть великі покращення, часто можуть призвести до великих проблем, які важко виміряти чи вирішити. Практикам ITIL 4 заохочується ітераційно вдосконалювати свої процеси, збираючи зворотний зв’язок і вимірюючи успіх на цьому шляху, щоб уникнути невдач. Зміна вимагає часу. Повільні та постійні перемоги та зміни слід оцінювати на предмет успіху, перш ніж організація розвиватиме їх далі.

Забезпечити співпрацю та заохотити прозорість та візуалізацію (Collaborate and promote visibility). Практиків ITIL 4 заохочується сприяти прозорості та видимості IT-операцій між членами команди, зацікавленими сторонами та партнерами. Підвищена наочність сприяє комунікації та співпраці між відділами, дозволяє власникам проектів і процесів збирати цінний зворотний зв’язок та інформацію з усієї організації, а також допомагає усунути надмірності та розрізи інформації чи знань.

Думати та діяти цілісно (Think and work holistically). П’ятий керівний принцип ITIL 4 заохочує практикуючих брати на себе відповідальність за те, як їхня робота вписується в загальну систему цінностей обслуговування. Жодне завдання не існує на порожнечі, і кожна дія, підпроцес або процес повинні виконуватися з метою мінімізації ризиків і витрат, забезпечуючи при цьому найбільшу цінність для бізнесу.

Бути простішим та практичним (Keep it simple and practical). Простота і практичність суперечать думці, яку деякі практикуючі фахівці мають про ITIL як про директивну та негнучку структуру. ITIL 4 усуває цю критику, спрямовуючи своїх практиків спростити та підібрати правильний розмір використання процесів, інструментів і ресурсів для відповідності організаційним потребам. Зауважимо, що "процеси" ITIL V3 називаються "практиками" в ITIL 4, зміна, яка відображає їхню гнучкість, яку нещодавно підкреслили для потреб IT-організацій.

Оптимізувати та автоматизувати (Optimize and automate). Остаточний керівний принцип ITIL заохочує спеціалістів автоматизувати й оптимізувати процеси, де це можливо. Ручні процеси легко забуваються або не помічаються, вони за своєю природою схильні до помилок, а також стомлюють і забирають багато часу. IT-організації повинні автоматизувати все, що вони можуть, залишаючи людське втручання для процесів, де це дійсно необхідно.

2.8 Застосування принципів ISO 19011для проведення аудиту

Системи управління аудитом є життєво важливими для організацій, щоб підтримувати культуру постійного вдосконалення при досягненні бізнес-цілей, щоб допомогти організаціям підтримувати конкурентну перевагу на ринку.

Остання версія оголошує настанови ISO 19011:2018 для систем управління аудитом з основних принципів аудиту, програми управління аудитом, виконання аудитів та управління висновками аудиту, а також вказівки щодо оцінки рівня компетентності для людей бере участь у всьому процесі аудиту [43].

ISO 19011:2018 надає цінну інформацію про те, як систематично покращувати програму аудиту, так само, як очікується покращення інших відділів організації. Одним із аспектів такого вдосконалення є постійне забезпечення відповідності цілей програми аудиту політикам та цілям системи управління. Організації, домагаючись удосконалення аудиту, повинні враховувати потреби клієнтів та інших зацікавлених сторін.

Сферою все більшого значення в аудиті систем управління та бізнесу в цілому є концепція ризику. Починаючи з видання 2011 року, ризики були інтегровані в розділ управління програмою аудиту стандарту ISO 19011:2018.

У новому перегляді [44] принципів аудиту збільшується наголос на процесах аудиту, що ґрунтуються на оцінці ризиків з метою ефективного стимулювання постійного вдосконалення. Нові принципи також говорять про гармонізацію кількох доступних систем із стандартизованим підходом до всього процесу аудиту.

Поточна редакція стандарту демонструє збільшення кількості застосовних стандартів для систем менеджменту, які включають недавні перегляди загальновживаних стандартів, таких як ISO 9001 та ISO 14001.

Ця версія призначена для задоволення потреб галузевих стандартів для різних організацій. Оскільки можна легко знайти стандарти управління, що охоплюють різні аспекти, включаючи навколишнє середовище, послуги, охорону здоров'я та медицину, інформаційні технології тощо, існує потреба у надійних процесах аудиту для цих систем, щоб відображати ефективність нових стандартів, що розробляються.

ISO 19011 призначений для всіх організацій, яким необхідно проводити внутрішні або зовнішні аудити систем управління якістю, які вони використовують. Він підходить для широкого кола потенційних користувачів, включаючи аудиторів. У загальному випадку, впровадження системи управління якістю передбачає проведення аудиту систем менеджменту з метою регулювання та відповідності [44].

ISO 19011 також містить рекомендації щодо проведення зовнішніх аудитів, для сертифікації та перевірки якості постачальників, для підтримки впровадження систем управління якістю.

2.9 IoT Security Compliance Framework як приклад галузевого набору вимог

IoT Security Foundation випустив IoT Security Compliance Framework, який містить набір з 233 вимог.

Вимоги є обов'язковими або рекомендаційними та застосовні до певних класів пристроїв, які залежать від впливу зламаного пристрою. Пристрої, де злом може викликати незначні незручності, позначаються класом 0, і до таких пристроїв застосовуються менш суворі заходи безпеки. Пристрої, які обробляють конфіденційні дані, позначаються класом 3, і для них застосовуються більшість заходів безпеки. Оскільки багато пристроїв обробляють конфіденційні дані в тій чи іншій формі, вимоги безпеки, які накладає ця структура, досить суворі.

Поділ на класи значною мірою ігнорує непрямий, соціальний вплив атак. Навіть якщо пристрій не має комплексних вимог безпеки, його все одно можна використовувати для DDoS-атаки на непов’язаний веб-сайт [45].

Фреймворк містить багато вимог, які забезпечують безпечний бізнес-процес, або вимагають безпечного дизайну. Це допомагає постачальникам враховувати безпеку під час процесу проектування.

Незважаючи на те, що це хороші рекомендації, щоб допомогти постачальникам захистити продукти, ці вимоги менш корисні для тестування чорного ящика, щоб визначити, чи відповідає пристрій цим вимогам. Наприклад, 2.4.5.38, «зміни в технічному обслуговуванні повинні викликати повне регресійне тестування безпеки», більше стосується бізнес-процесу, ніж функціональності пристрою.

Незважаючи на це, існує також багато вимог, які є достатньо конкретними та вимірними. Наприклад, однією з найпростіших і найважливіших вимог є 2.4.8.4: продукт не допускає використання нульових або порожніх паролів [45].

Фреймворк має широкий діапазон і включає вимоги безпеки для мобільних додатків, хмарних сервісів, ланцюга поставок і виробничого процесу. Це викликає декілька дуже схожих вимог; паролі мають бути безпечними для пристрою IoT, для мобільного додатка, для веб-інтерфейсу тощо.

2.10 Світовий досвід та нормативна база, що стосується ОК(І)І

Автору даної роботи вважається доцільним звернутися до досвіду інших держав та об’єднань у сфері захисту критичної інфраструктури. Зокрема розглянемо основні аспекти нормативної бази Європейського Союзу (ЄС), США та Китаю.

Світовий досвід та нормативна база, що стосується ОК(І)І.

Особливої актуальності для європейських країн питання її захисту набуло у 2001 році, після трагічних подій 11 вересня (здійснення терористичного акту у місті Нью Йорк). У 2004 році Європейська комісія почала розробляти загальну методологію захисту критичної інфраструктури та рекомендувала підвищити увагу

до безпеки об’єктів, припинення функціонування яких матиме негативні наслідки [46].

Протягом наступного десятиріччя держави почали впроваджувати концепції захисту на законодавчому рівні. Наприклад, польський уряд ухвалив закон про управління кризовими ситуаціями, в рамках якого подано чітке розуміння параметрів критичної інфраструктури та її захисту. Не залишилась осторонь і Словаччина, де у 2011 р. було прийнято закон про критичну інфраструктуру, котрий чітко визначав перелік таких об’єктів та державні органи, що відповідають за їх захист. Одну з найбільш комплексних законодавчих баз у цій царині продемонструвала Угорщина: прийнятий нею закон про захист критичної інфраструктури чітко визначає порядок і принципи зарахування об’єктів до категорії критичних, проведення інспекцій та механізм взаємодії між державними органами у критичних ситуаціях.

На сьогоднішній день питання захисту критичної інфраструктури є важливим напрямом у сфері безпеки країн-членів ЄС та НАТО. Важливе місце її захисту відводять і експерти Світового банку, котрі вказують на важливість приділення урядами особливої уваги питанню безпеки стратегічних об’єктів, що має зменшити можливі наслідки аварій техногенного та природного характерів.

Саме поняття «критичної інфраструктури» було введене у міжнародну практику в середині 1990-х. Воно знайшло відображення у нормативно-правових актах, науковому і діловому колах.

На сьогоднішній день міжнародною спільнотою не вироблено загальноприйнятого універсального визначення критичної інфраструктури, але визначення, зафіксовані в документах різних держав і об'єднань, багато в чому перетинаються і не суперечать одне одному.

Проблема розробки загальних визначень існує не тільки на міжнародному, а й на національному рівні. Так, у США глосарій Національного інституту стандартів і технологій (NIST) містить 5 схожих, але не ідентичних визначень критичної інфраструктури, які використовуються в різних документах. Наприклад, у документі NIST «Платформа для поліпшення кібербезпеки критично важливої

інфраструктури» від квітня 2018 року наведено таке визначення: «Фізичні або віртуальні системи та активи, які настільки життєво важливі для Сполучених Штатів, що часткове або повне порушення їх працездатності негативно позначиться на кібербезпеці, національно-економічній безпеці, здоров'ї або безпеці громадян» [46].

А у директиві Європейської ради 2008/114/ЄС критична інфраструктура визначена як актив, система або її частина, розташована на території ЄС, що має велике значення для підтримки життєво важливих соціальних функцій, здоров'я, безпеки, економіки або благополуччя населення, порушення роботи або знищення якої призведе до значного впливу як мінімум на дві держави-члена [47].

У 2021 році уряд Китаю затвердив “Положення про захист критично важливої інформаційної інфраструктури. Правила захисту критично важливої інформаційної інфраструктури” [48].

Правила спрямовані на забезпечення безпеки критично важливої інформаційної інфраструктури та підтримання кібербезпеки.

Під загальною координацією національної адміністрації кіберпростору (Адміністрація кіберпростору Китаю) орган громадської безпеки при Державній раді (Міністерство громадської безпеки) відповідає за керівництво та нагляд за захистом критично важливої інформаційної інфраструктури. Компетентний орган електрозв'язку при Державній раді (Міністерство промисловості та інформаційних технологій) та інші відповідні органи несуть відповідальність за захист, нагляд та управління критично важливою інформаційною інфраструктурою у межах своїх відповідних функцій та обов'язків відповідно до Регламенту, відповідних законів та адміністративних постанов.

Держава забезпечує посилений захист критично важливої інформаційної інфраструктури і вживає заходів з моніторингу, запобігання та усунення ризиків і загроз кібербезпеці, що виникають всередині та за межами території Китайської Народної Республіки, захищає критичну інформаційну інфраструктуру від атак, вторгнень, втручання та завдає шкоди (карає) за незаконні та злочинні дії, які

становлять загрозу безпеці критично важливої інформаційної інфраструктури, відповідно до закону [48].

Очевидно, що наведені визначення відрізняються, але сходяться в головному: вони визнають значимість безперебійної роботи критичної інфраструктури. Крім того, всі держави визнають, що навколишнє середовище інформаційно-комунікаційних технологій взаємопов'язане і взаємозалежне.

Нинішня геополітична арена перетворила кібератаки на критичні інфраструктури в кібервійну, оскільки можливість руйнування критичної інфраструктури країни шляхом відключення електростанцій, руйнування нафтопроводів, навіть порушення роботи водопостачання та теплопостачання може дати значні військові переваги.

Військові альянси, такі як НАТО, навіть розглядають можливість класифікувати кібератаки на критично важливу інфраструктуру держав-членів як відкрите оголошення війни, викликаючи таку ж військову відповідь, що й традиційна атака за участю танків, літаків і солдатів. Проте варто зазначити, що інкримінувати причетність до кібератаки певній особі чи національній структурі в кіберпросторі важко, оскільки судовими доказами розслідування можна легко маніпулювати, щоб спрямувати розслідувачів інцидентів безпеки на шлях, що вводить в оману [46].

Висновки за розділом 2

Провівши комплексний аналіз нормативних документів, міжнародних стандартів та підходів до оцінки рівня захищеності як у загальному випадку, так і для ОК(І)І зокрема, було визначено, що використання наявного інструментарію є виправданим тільки за умови його попереднього аналізу та синтезу на його основі власного рішення, яке матиме той, або інший рівень запозичення.

РОЗДІЛ 3
ОПИС ТА СИНТЕЗ МОДЕЛІ ОЦІНКИ ЗАХИЩЕНОСТІ

3.1 Опис принципів та методики запропонованої моделі

Для того, щоб створити модель, використання якої дозволить отримати адекватну оцінку рівня захищеності ІС та її середовища, перш за все потрібно мати власне об’єкт оцінки (що?), її оцінювача (ким?) та методи (як?), за якими здійснюватиметься процес оцінки.

Характеристики, які відносяться безпосередньо до самої системи в рамках реалізації конкретної моделі є константними та залежать тільки від початкового вибору об’єкту оцінки. В той самий час, для кожного нового застосування запропонованих підходів, об’єкт оцінки може (буде) відрізнятися. Така особливість зумовлена акцентом на універсальності застосування запропонованої моделі. Це означає, що одним із вхідних параметрів у вигляді об’єкту оцінки, може виступати ІС будь-якого рівня складності, з різним набором функцій та з широким спектром задіяних процесів.

Дві інші складові частини являють собою *предмет дослідження*. Підходи, використані для їх формування викладено нижче.

Основна ідея створення нової моделі оцінки захищеності полягає у наданні максимально повної та обширної оцінки, використовуючи при цьому мінімальну кількість ресурсів. Також за ціль обрано надання достатнього рівня універсальності застосування, зрозумілості підходу та простоти його впровадження.

Для досягнення поставлених задач пропонується використовувати якомога ширший (з виправданою та обґрунтованою кількістю) перелік стандартів та наборів вимог. Такий підхід з імовірністю у 100% матиме долю надмірності, коли окремі контролі, або цілі домени є присутніми у текстах деяких, або навіть всіх нормативних документів. До прикладу, питання оцінки ризиків буде так, або інакше розкрито одночасно у стандартах, які регламентують загальні вимоги до кібербезпеки як-то NIST SP 800-53, управління ризиками ISO 27005, систему

менеджменту безперервності бізнесу ISO 22301, чи стандарт безпеки даних індустрії платіжних карток PCI DSS.

Подібний перетин є закономірним наслідком, якщо таксономія (структурна класифікація) стандартів передбачає застосування наборів вимог від різних регуляторів. Позитивним аспектом даного підходу все ж залишається відносно просте масштабування середовища перевірки (scope), коли покривається, по-перше, ширше коло питань та контролів та, по-друге, ми отримуємо кращий результат з точки зору повноти оцінки з особливо важливих тем. Так як при виборі стандартів прийнято опиратися на авторитет його видавців - отже ми приймаємо і структуру стандарту.

Однією з особливостей пропонованої моделі повинна стати достатня гнучкість для забезпечення простоти користування. Тому існує шлях уникнення лишньої надмірності. Він полягає у використанні результатів оцінки аналогічного (подібного) контролю, проведеної вперше та зменшення кількості контролів, за якими здійснюється перевірка. Тобто отримуємо ситуацію, коли конкретний повторюваний контроль перевіряється в рамках одного стандарту, а потім результат такої оцінки використовується в рамках перевірки за іншим стандартом. Також отримуємо можливість взагалі скоротити перелік контролів, якщо це вважається доцільним на думку аудитора.

Недоліком такого підходу є вагомий вплив людського фактору - саме від експертності аудитора залежатиме, чи буде встановлено залежність між контролями належним чином, та чи не буде викинуто за сферу оцінювання (scope) контролі, які є справді менш важливими. Тому доцільно ввести два обмежуєчих фактора на запозичення результатів оцінки інших (або власної, проведеної раніше в рамках цієї ж перевірки) та скорочення кількості вимог, які належить перевірити та оцінити.

1. Загальний список вимог, який регламентований конкретним стандартом не може бути змінено (зменшено) більше ніж на 20%. До цього ж показника належить і число контролів, оцінка яких запозичена із перевірки інших стандартів.

2. Кожен випадок скорочення та використання результатів інших повинен бути належно задокументований з викладенням обгрунтування такого рішення. При

цьому забороняється спиратися виключно на професійне судження (professional judgement) особи, яка приймає відповідне рішення без належного пояснення у письмовій формі.

Оскільки левова частка міжнародних, національних та галузевих стандартів у сфері ІБ створена різними інституціями, покликана виконувати різні завдання, досягати різних цілей та призначена для різної аудиторії людей, станом на сьогодні немає єдиного розуміння цих стандартів. Поширеною практикою є відсутність однозначного трактування навіть подібних їх складових частин у експертному середовищі спеціалістів з ІБ. Це є загальною проблемою і для досягнення цілей пропонованої моделі зокрема. Повноцінне її вирішення потребує значних наукових зусиль для досягнення консенсусу, але це питання явно виходить із предметної області даного дослідження.

Натомість, для уніфікації методів оцінювання та, принаймні, часткового вирішення проблеми неоднозначності трактування, яка постає при виборі більш ніж одного стандарту, або набору вимог, тим більше не з одного сімейства, пропонується використовувати єдиний підхід у вигляді рівнів зрілості ITSM.

Рівень зрілості – це чітко визначене еволюційне плато, яке встановлює рівень спроможності для покращення можливостей робочої сили; кожен рівень зрілості визначає певні характеристики процесів, причому вищі рівні зрілості мають більш просунуті характеристики і є кроком до досягнення зрілого процесу, забезпечуючи набір цілей, які, якщо вони задоволені, переводять організацію на наступний рівень зрілості. Він також визначає шлях, по якому йде процес, переходячи від незрілого і спеціального процесу до високо зрілого процесу [49].

Структури ITSM включають цілий ряд моделей зрілості. Вони підтримують мету постійного вдосконалення. Хоча кожна модель зрілості працює по-різному, існує спільна методологія проектування. Ці моделі оцінюють такі фактори, як [41]:

- організаційні цілі;
- зовнішні вимоги;
- функціональна здатність;

● інші фактори, які визначають позиціонування компанії щодо можливостей ITSM та якості IT-послуг, що надаються кінцевим користувачам.

Характеристики організації визначаються на кількох рівнях зрілості на основі конкретних критеріїв. Ці рівні є послідовними і варіюються від найнижчих IT-можливостей до високої зрілості у використанні відповідних IT-функцій.

У цій роботі розглянуто модель зрілості відповідно до ITIL, оскільки це одна з найбільш широко застосовних структур та найкращих практик і сфері IT та суміжних.

Життєвий цикл служби ITIL документує рекомендації для різних процесів і функцій ITSM. Відповідно до ITIL, процес — це будь-який структурований набір діяльності, призначений для виконання певних завдань. Приклади процесів включають управління змінами та управління проблемами. IT-функції, таким чином, визначаються як команди, інструменти та ресурси, які використовуються для виконання діяльності в рамках цих процесів.

У моделі зрілості ITIL оцінка складається з анкети про атрибути, вхідні дані, інтерфейси та результати, пов’язані з процесами та функціями ITIL. Рівень зрілості кожного процесу та функції потім визначається відповідно до наступних п’яти рівнів (рівень 0 означає, що процес не впроваджено взагалі, або впроваджено вкрай неефективно і він не здійснює бажаних функцій) [49].

Рівень 1: початковий.

Перший рівень зрілості показує, що процеси та функції дезорганізовані, що свідчить про потенційні проблеми, які необхідно визначити та вирішити для покращення можливостей ITSM. Розподіл ресурсів здійснюється в кожному окремому випадку, а діяльність не відповідає попередньо визначеним найкращим практикам. Залучені процеси та функції не є життєво важливими для основного бізнесу.

Успішне виконання цих заходів може залежати безпосередньо від навичок та досвіду осіб, які беруть на себе ініціативу, а не від будь-якої загальної підтримки чи структури.

Рівень 2: повторюваний.

Використовується інтуїтивно зрозумілий проектний підхід для ефективного надання послуг для конкретних процесів і функцій ITIL. Менеджмент та відповідальні особи заздалегідь визначають зацікавлені сторони та цілі проекту, щоб отримати високу ефективність реалізації процесів та задоволеність клієнтів.

Хоча заходи заздалегідь визначені, успішне виконання також залежить від залучених осіб. Забезпечення неформального навчання гарантує, що особи несуть відповідальність за дотримання регулярного шаблону для виконання діяльності. Відсутність координації та підтримки також призводить до людських помилок, порушень та неефективності під час процесу впровадження.

Рівень 3: визначений.

На визначеному рівні вже можна побачити якісний підхід до управління процесами IT-послуг.

- Процеси задокументовані та стандартизовані.
- Корпоративні знання та зовнішні вимоги формують та забезпечують дотримання політики ITSM.
- Вжито відповідних заходів для забезпечення ефективного виконання процесу.
- Регулярне навчання та відповідні ресурси доступні, оскільки люди змушені дотримуватися проактивного підходу до виконання діяльності ITSM.

На цьому етапі перспектива організації спроможності характеризується вищою якістю та продуктивністю та меншими ризиками у порівнянні з двома попередніми.

Рівень 4: керований.

Керований рівень зрілості означає, що в організації керують функціями та процесами відповідно до кількісного підходу.

- IT-відділи визнають відповідну діяльність і встановлюють конкретні цілі, щоб узгодити IT із бізнес-стратегією компанії.
- Моніторинг відповідних показників забезпечує постійне вдосконалення IT-можливостей організації.
- Широке поширення отримали засоби автоматизації.

● Налаштовано спрощену міжфункціональну співпрацю та обмін знаннями.

На цьому етапі процеси є надійними, а ризик збою низький. Додаткове фінансування зазвичай доступне для задоволення додаткових вимог або запобігання збоям.

Рівень 5: оптимізований.

Найвищий рівень моделі зрілості досягається, коли всі процеси процесу підлягають сильному управлінському контролю.

● Інструменти автоматизації та моніторингу автономно координують завдання та здійснюють покращення протягом усього життєвого циклу служби.

● Цикл зворотного зв’язку забезпечує ітераційні та постійні вдосконалення.

● Послідовні засоби управління в організації та всі процеси ITSM інтегровані з бізнес-цілями.

Оцінюючи рівень зрілості, організації можуть визначити відповідну відправну точку для своїх стратегій. Завдання не обов’язково полягає в тому, щоб знати, яким процесам і функціям бракує необхідних ресурсів, політики та нагляду з боку керівництва.

На даному етапі слушним буде ввести поняття аудиту для його однозначного розуміння в подальшому.

Аудит безпеки інформаційної системи – це системний процес одержання об'єктивних якісних та кількісних оцінок поточного стану безпеки інформаційної системи, комплексна оцінка рівня інформаційної безпеки об’єкта з урахуванням як мінімум трьох основних факторів: персоналу, процесів і технологій. Результатом аудиту може слугувати порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками перевірок, опитування та анкетування, та цільового рівня ефективності процесів у відповідності до визначених стандартів, або внутрішніх вимог [50].

У свою чергу, оцінку захищеності у загальному випадку можна вважати синонімом до аудиту, але в рамках цієї роботи, до неї будуть ставитися менш строгі нормативні вимоги. Перш за все, аудит відноситься до деталізованої та регламентованої оцінки. Якщо ж описати рівень залучення аудиторів до процесу

перевірки, вимоги до ведення документації та механізм отримання доказів, то вийде наступна градація понять:

1) внутрішній аудит;
2) сертифікація;
3) зовнішній аудит;
4) оцінка за рівнем зрілості.

Відповідно до наданого вище визначення, можемо вважати, що аудит та оцінка захищеності є подібними, але не тотожними поняттями. Для більш чіткого розуміння їх відмінностей, нижче наведено пояснення щодо критеріїв, які застосовуються для оцінки захищеності.

Критерії оцінки захищеності (security evaluation criteria) — сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації [51].

У свою чергу захищеність являє собою наявність дієвої адекватної системи технічних, організаційних та інших розвинених і ефективних процедур та засобів (механізмів) для безпечного функціонування інформаційної системи та досягнення нею поставлених цілей та прогнозованих результатів. Захищеність у рамках даної роботи варто розглядати як міру одночасно безпеки (умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень [16]) та захисту інформації в системі (діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [52]).

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступенів захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Окрім функціональних критеріїв захищеності існують такі критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації [53].

Оскільки на даному етапі розвитку ІТ не є доцільним та можливим повністю уникнути людського фактору у таких складних та комплексних речах як оцінка захищеності ІС (в рамках запропонованої моделі зокрема процеси будуть часто апелювати до професійного судження особи), вважається необхідним запровадити певний набір вимог до оцінювача. Такі правила допомагають мінімізувати вплив людського суб'єктивізму, навіть при застосуванні кількісних показників оцінки, про які буде йти мова далі у цьому розділі.

Виходячи з цього, доцільно ставити перед особами та/або організаціями, які будуть брати участь у процесі оцінки, такі ж вимоги, як і до аудиторів (для спрощення розуміння, будемо вживати "аудитор" в обох випадках: коли мова йде про аудит та про оцінку). Зокрема, можна скористатися поширеною галузевою практикою, наведеною у міжнародному стандарті ISO 19011.

Аудит систем менеджменту базується на семи фундаментальних принципах, які роблять систему управління аудитом ефективним інструментом для підтримки процесів, засобів контролю та політики якості. Він направляє організацію критично важливою інформацією, щоб діяти та покращувати її загальну ефективність. Дотримання цих принципів дозволяє аудиторам працювати незалежно, оскільки вони можуть отримати більш відповідні висновки аудиту [44].

Чесність (Integrity).

Цей принцип недаремно розміщено першим. Його називають основою професіоналізму аудиторів, а також осіб, які беруть участь у програмі аудиту, які повинні виконувати всі свої обов'язки з належною етикою, відповідальністю та чесністю. Вони повинні виконувати аудиторську діяльність, для якої вони відчувають себе компетентними. Найголовніше, аудитори повинні бути

неупередженими у всіх своїх діях та не мати жодних переконань, котрі можуть на них впливати, коли виноситься будь-який остаточний висновок.

Чесна презентація (Fair Presentation).

Аудитори повинні точно продемонструвати всю аудиторську діяльність та матеріали, включаючи звіти, знахідки (findings) та висновки. Вони повинні повідомити про кожну серйозну та незначну перешкоду, з якою вони зіткнулися під час аудиту, навіть якщо це розбіжності в думках між ним/нею та аудиторською групою. Чітке, своєчасне та правдиве спілкування є запорукою успішного аудиту цільового об’єкту.

Належний професіоналізм (Due Professionalism).

Аудитори повинні проявляти належну увагу до завдань, які вони виконують, оскільки клієнти аудиту та інші залучені сторони виявили довіру до них та впевненість у їхніх діях. Аудитори не повинні йти на компроміс, якщо це стосується професіоналізму, коли мова йде про прийняття суджень у різних видах аудиторської діяльності. Чим більше вони будуть проявляти належний професіоналізм, тим грунтовніші судження вони зможуть робити.

Конфіденційність (Confidentiality).

Це може здатися дуже банальним, коли ми говоримо про безпеку інформації, але піклуватися про це дуже важливо. Аудитори не повинні за жодних умов розкривати інформацію, пов’язану з їхніми обов’язками, включаючи помилки та висновки, з якими вони зіткнулися в процесі проведення аудиту невідповідним чином для отримання особистої вигоди. Це також стосується клієнта аудиту. З усією інформацією про об’єкт аудиту слід розумно розпоряджатися, відповідно до положення про конфіденційну інформацію, яка залишатиметься між довіреними сторонами для захисту бізнесу.

Відсутність залежності (No Dependency).

Аудитори не повинні опиратися на будь-які упереджені впливи, або конфліктні ситуації, коли мова йде про аудиторську діяльність. Вони повинні дотримуватися залежність лише від перебігу, знаходжень і висновків аудиту, щоб зробити достовірний звіт. Для малих організацій так само важливо, як і для великих,

докладати достатніх зусиль, щоб уникати упередженості та заохочувати справедливі перевірки для подальших покращень.

Підхід, заснований на доказах (Evidence-Based Approach).

Аудитори, щоб вважати свою аудиторську діяльність надійною, повинні належним чином використовувати докази. Вони повинні виробити звичку збирати докази, оскільки аудит проводиться з обмеженими ресурсами протягом обмеженого часу. Зберігання доказів для всіх аудиторських заходів допомагає аудиторам зберігати довіру клієнтів аудиту до будь-яких висновків, які вони пропонують.

Підхід, орієнтований на ризик (Risk-Based Approach)

Будь-яку аудиторську діяльність слід виконувати лише після врахування всіх потенційних ризиків і можливостей. Такий підхід міг би змінити всі види діяльності від планування до виконання та звітування про події. Аудитори можуть більш ефективно досягати цілей програми аудиту за допомогою підходу, що ґрунтується на оцінці ризику, оскільки він може зосередити їх увагу на нових можливостях.

Після того, як визначено вимоги до суб’єктів проведення оцінки (об’єкта оцінки та аудиторів), варто детальніше описати методи, які використовуються в рамках запропонованої моделі та її особливості.

Насамперед, слід визначитися із методами для вирішення задачі оцінки, які можна розділити на кількісні та якісні. Вони відрізняються за вибором шкали вимірювання – числової та лінгвістичної відповідно. Кожна група методів має свої переваги та недоліки.

Мінімізувати перераховані недоліки, які наведено у таблиці 3.1 [54] дозволяє поєднання кількісних та якісних методів – використання шкали числових коефіцієнтів разом з лінгвістичним описом її окремих інтервалів (рівнів), але в рамках даної наукової роботи перевага надається кількісному методу. Як і у випадку із поставленими вимогами до аудиторів - це робиться для зменшення впливу людського фактору.

Таблиця 3.1

Переваги та недоліки кількісних та якісних методів

Методи оцінки	Переваги	Недоліки
Кількісні методи	1) Дозволяють чисельно оцінити необхідні параметри; 2) реалізують аналіз витрат та прибутку при виборі захисту; 3) надають більш точне відображення шуканих значень.	1) Кількісні міри залежать від об'єму та точності шкали виміру; 2) результати оцінки можуть бути неточними; 3) повинні доповнюватись якісними характеристиками; 4) оцінка з застосуванням цих методів зазвичай потребує більше досвіду та сучасного інструментарію.
Якісні методи	1) Дозволяють визначити області критичних рівнів в короткий проміжок часу без значних витрат; 2) дозволяють оцінювати відносно легко та дешево.	1) Не дозволяють визначити ймовірності та результати з використанням числових коефіцієнтів; 2) аналіз витрат та користі при виборі захисту важчий; 3) отримані результати мають загальний, наближений характер.

Мінімізувати перераховані недоліки дозволяє поєднання кількісних та якісних методів – використання шкали числових коефіцієнтів разом з лінгвістичним описом її окремих інтервалів (рівнів), але в рамках даної наукової роботи перевага надається кількісному методу. Як і у випадку із поставленими вимогами до аудиторів - це робиться для зменшення впливу людського фактору.

Ще одним методологічним підходом є використання циклу плануй-виконуй-перевіряй-дій - так званого Plan-Do-Check-Act (PDCA), зображеного на рисунку 3.1, також відомого як цикл Демінга.

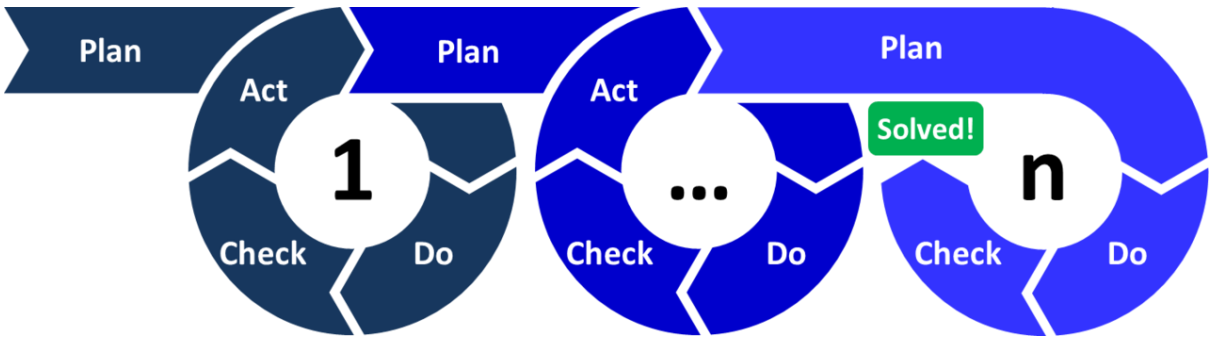

Рисунок 3.1 – Цикл плануй-виконуй-перевіряй-дій

Plan: визначити можливість і спланувати зміни.

Do: перевірити зміни. Провести невелике дослідження, тест.

Check: переглянути тест, проаналізувати результати та визначити, які проміжні висновки отримано.

Act: виконати дії на основі того, що дізналися на попередніх етапах. Якщо зміна не спрацювала, повторити цикл за іншим планом. Якщо ви досягли успіху, включити те, що ви дізналися з процесу, у майбутні зміни. Використовувати те, чому навчилися, щоб спланувати нові покращення, починаючи цикл знову.

Відповідно до принципів побудови циклу PDCA, було створено структуру, яка описує всі основні етапи, з яких складається запропонована модель оцінки захищеності, адаптований сценарій якого зображено на рисунку 3.2.

1. Початковий аналіз ІС та планування.

Після того, як вирішено проводити оцінку рівня захищеності та обговорено її загальні деталі відбувається більш детальний аналіз масштабу перевірки, розроблення плану, за яким проходитиме процес оцінювання та опис методології, яка буде застосована.

На цьому етапі також відбувається виокремлення складових частин ІС та її середовища, так званих доменів. До переліку доменів можуть входити такі елементи як, наприклад, СУІБ, окремо управління ризиками, технічні вимоги, вимоги фізичного захисту, процес управління бізнесом тощо. Визначення доменів відбувається у кожному випадку окремо та залежить від професійного судження особи (команди), яка проводитиме оцінку захищеності. Головною метою визначення

доменів є покриття якомога ширшої сфери діяльності, пов’язаної з ІС з урахуванням наявних для перевірки ресурсів - перш за все професійних якостей та експертизи аудитора.

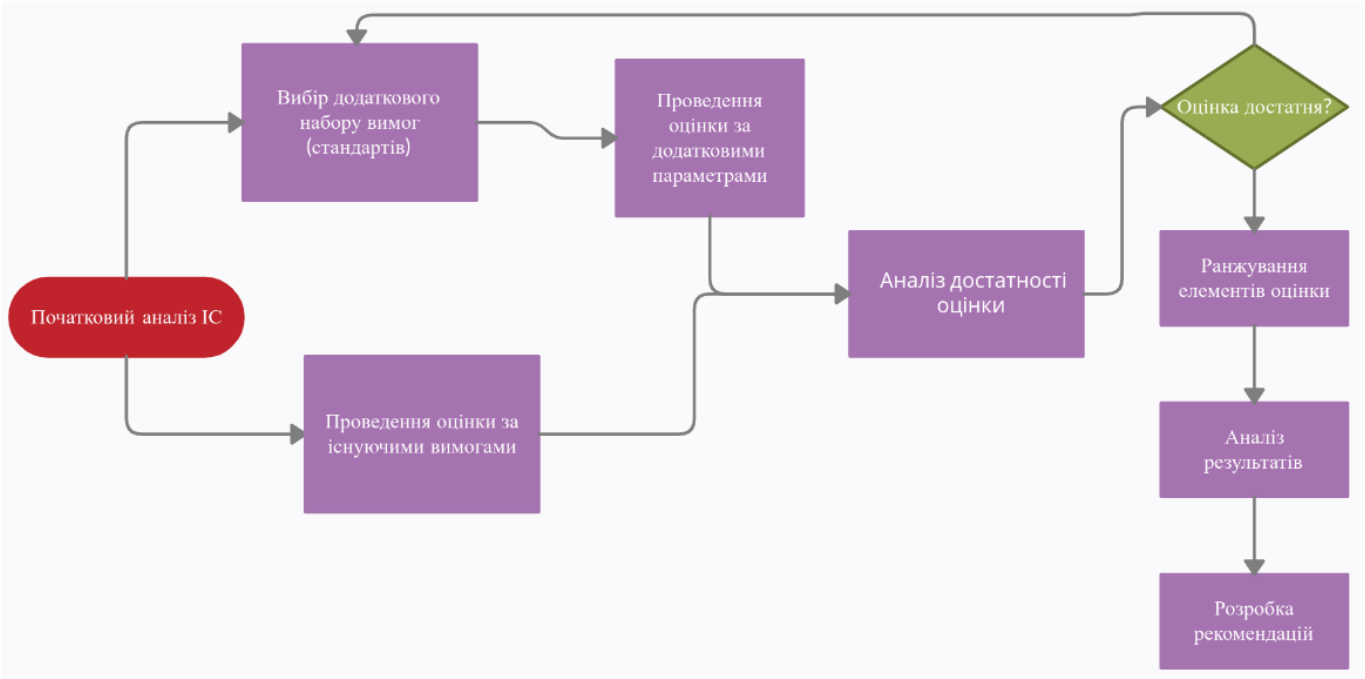

Рисунок 3.2 – Адаптований сценарій циклу плануй-виконуй-перевіряй-дій

2. Проведення оцінки за існуючими вимогами.

Кожна ІС створюється та функціонує відповідно до певних вимог. Хоча б на одному з цих етапів повинна відбуватися оцінка функціональних метрик для розуміння того, чи виконує система ті цілі, які перед нею поставлено. Тим більше це справедливо до такого регульованого бюрократичного середовища, як об’єкти критичної інфраструктури. Сюди можна віднести як технічну документацію, яка використовувалася при проектуванні, міжнародний стандарт, або окремий набір вимог, який диктує регулятор галузі.

Здебільшого, ІС проходять регулярну перевірку на відповідність обов’язковим специфічним вимогам, яку проводять авторитетні уповноважені органи, чия професійність не викликає сумнівів. В такому випадку буде доцільно перейняти результати їх перевірки та адаптувати їх до критеріїв оцінки захищеності запропонованої моделі.

Якщо ж результати регуляторського оцінювання недоступні, потрібно провести власну перевірку, згідно із розробленим у попередньому пункті планом.

3. Вибір додаткового набору вимог (стандартів).

Проаналізувавши систему та визначивши, якими наборами вимог вона регламентується, потрібно доповнити цей набір стандартами таким чином, щоб достатньо широко оцінити всі важливі її елементи (домени). Під достатністю варто розуміти належний рівень обгрунтування та переконаність [55] у тому, що важливі моменти враховано.

Наприклад, коли організація використовує як штатний стандарт по управлінню ризиками NIST RMF і він перевіряється у пункті 2, доцільно буде скористатися стандартами про СУІБ, безперервність бізнесу, а не використовувати ще ISO 31000, який виконує ту ж саму функцію з управління ризиками.

Рекомендований набір стандартів: ISO 27001 для СУІБ, NIST CSWP для узагальненої оцінки об'єктів критичної інфраструктури, COBIT 2019 для оцінки менеджменту, ISO 22301 для безперервності бізнесу. Даний перелік не є вичерпним та єдино правильним. На практиці він буде залежати переважно від досвіду та рівня експертизи аудитора.

4. Проведення оцінки за додатковими параметрами.

На даному етапі відбувається оцінювання рівнів зрілості процесів та контролів, з яких складаються набори вимог, обрані в попередньому пункті.

5. Аналіз достатності проведеної оцінки.

Після того, як процес оцінки згідно плану перевірки завершено, потрібно оцінити рівень покриття цієї оцінки основних доменів, визначених у пункті 1. Повинен відбутися процес порівняння отриманих результатів із запланованими. Якщо існують суттєві відмінності, або виникла ситуація, коли потрібно провести додаткову оцінку - потрібно повернутися до пунктів 3 і 4.

6. Ранжування елементів оцінки.

Маючи всі результати проведеної перевірки та визначивши, що вона достатньо покриває всі важливі домени аудитор переходить до розставляння коефіцієнтів, які можуть застосовуватись на трьох рівнях:

- контролю (підкатегорії);
- групи контролів (домену, або категорії);
- набору вимог (стандарту) в цілому.

По замовчуванню значення коефіцієнта дорівнює одиниці. Воно може бути змінено у рамках від 0.9 до 1.1, якщо потрібно адаптувати отримані кількісні результати до реального стану речей. Наприклад, якщо є зауваження до політики безпеки, але організація працює над її оновленням - оцінку на рівні контролю, або категорії можна частково підвищити.

7. Аналіз результатів проведеної оцінки.

На цьому етапі підсумовуються результати проведеної роботи та закінчується процес створення звітної документації.

8. Розробка рекомендацій щодо підвищення рівня захищеності ІС на основі проведеної оцінки.

Наостанок залишається розробити набір рекомендацій згідно з аналізом здійсненої оцінки.

3.2 Синтез та навчання моделі з використанням штучних нейронних мереж

Після того, як ми здійснили перевірку та отримали числові показники у вигляді значень рівнів зрілості для кожного окремого контролю, варто замислитися над процедурою, яка допоможе знайти потужне, масштабоване, але просте у використанні рішення. Таким інструментом було вирішено обрати використання машинного навчання на прикладі програмного забезпечення Weka — набору алгоритмів машинного навчання з графічною оболонкою для завдань прогнозування та аналізу великого об’єму даних. Програмний засіб містить інструменти для підготовки, класифікації, регресії, кластеризації даних, аналізу застосовуваних правил асоціацій та візуалізації результатів [56].

Weka дозволяє виконувати широкий спектр задач для машинного навчання із застосуванням різних алгоритмів, зокрема, дерев рішень - одного із підходів до

прогнозного моделювання, яке використовується у інтелектуальному аналізі даних, машинному навчанні та статистиці. Він використовує дерево рішень (як прогностичну модель), щоб перейти від спостережень за елементом (представленим у гілках) до висновків про цільове значення елемента (представленого у листку). Дерева рішень є одними з найпопулярніших алгоритмів машинного навчання, враховуючи їхню зрозумілість і простоту [57, 58].

За основний підхід було взято так званий random forest, який має тенденцію вивчати дуже нерегулярні моделі, переповнюючи свої навчальні набори, тобто має низьку міру упередження (bias), але дуже високу дисперсію. Random forest – це спосіб усереднення кількох глибоких дерев рішень, які навчаються на різних частинах одного навчального набору, з метою зменшення дисперсії. Це відбувається за рахунок невеликого збільшення зміщення та деякої втрати інтерпретації, але загалом значно підвищує продуктивність кінцевої моделі.

До того ж, даний алгоритм може бути використаний для оцінки важливості змінних у завданнях регресії та класифікації. Для того, щоб оцінити важливість параметра після тренування, значення параметра перемішуються для всіх записів тренувального набору та out-of-bag-помилка обчислюється знову. Важливість параметра оцінюється шляхом усереднення по всіх деревах різниці показників out-of-bag-помилок до і після перемішування значень. Параметри вибірки, які дають більші значення, вважаються більш важливими для тренувального набору. Метод має потенційний недолік - для категоріальних змінних з великою кількістю значень метод схильний вважати такі змінні найважливішими. Часткове перемішування значень у такому випадку може знижувати вплив цього ефекту [59, 60].

Як згадувалося вище, у запропонованому підході надається перевага поєднанню кількісної та якісної оцінки результатів, саме тому на останній стадії оцінювання знову відбувається перехід з отриманих значень рівнів зрілості на якісний поділ. Оскільки врахування всіх можливих труднощів реалізації моделі та особливостей проведення оцінки виходить за рамки цієї роботи, пропонується мінімізувати їх вплив, шляхом добавлення нової якісної шкали оцінювання як в університетському середовищі:

- відмінно оцінка всіх рівнів зрілості 4 і вище;
- добре - 3 і вище;
- задовільно - 2 і вище;
- незадовільно - наявна хоча б одне значення рівня зрілості, менше 2.

Остаточне встановлення залежності між двома підходами покладається на аудитора та може видозмінюватися, зважаючи на його експертну думку.

Повертаючись до використання інструментарію машинного навчання, було обрано набір оцінок рівнів зрілості на основі списку категорій та заходів безпеки, викладених у додатку А стандарту ISO 27001.

Першим етапом стало формування набору даних, необхідних для навчання та сам процес навчання моделі.

Потрібно створити вхідний набір даних, який включає в себе всі числові значення отриманих оцінок, що уособлюють рівень зрілості кожної із категорій з вибраного набору вимог. Ці значення повинні знаходитись у діапазоні від 0 до 5. У нашому випадку вхідних кількісних показників буде 14 - по кожному з доменів додатку А ISO 27001. Крім цього представлення о, потрібно додати ще один показник, який відповідає за якісне загальної оцінки.

Числові показники генеруються випадковим чином і мають наступні залежності числових значень: від 4 до 5 для якісного показника “відмінно”, від 3 до 5 - для “добре”, від 2 до 5 - для “задовільно” та діапазон від 0 до 5 - для “незадовільно”. В результаті отримуємо з вибірки 800 та 2800 екземплярів даних із 15 атрибутами. Типовий набір даних для одного екземпляра виглядає наступним чином: “4,4,5,4,5,5,4,5,5,4,4,5,5,4,відмінно”.

Weka підтримує імпорт даних у форматі ARFF (Attribute-Relation File Format). Це текстовий файл ASCII, який описує модель даних через атрибути та екземпляри даних. Файли ARFF впорядковані в такому порядку: назва відношення, список використаних атрибутів та екземпляри даних, що подаються рядок за рядком. Тобто всі файли, які будуть завантажуватись у дане програмне середовище повинні бути у даному форматі.

Для навчання моделі використовуватимемо крос-валідацію (перехресну перевірку) – статистичний метод оцінки моделі. У крос-валідації дані розбиваються на k підмножин, які по черзі використовуються в навчальній та тестовій вибірках. Одна підмножина використовується для тестування, інші (k-1) – для навчання. Процедура повторюється k разів у результаті ми отримуємо усереднені результати.

Налаштування моделі зазвичай накладається на етап навчання моделей. Деякі параметри визначають роботу моделі на високому рівні, такі як їх функція навчання чи модальність, і їх неможливо дізнатись із вхідних даних. Ці спеціальні параметри, які часто називають гіперпараметрами, потрібно налаштовувати вручну, хоча за певних обставин вони можуть бути налаштовані автоматично шляхом пошуку простору параметрів моделі. Для навчання моделі використовувались такі гіперпараметри: швидкість навчання 0.3 швидкість оновлення ваги 0.2, час навчання 50. Набір даних навчання складається спочатку із 800, а потім із 2800 прикладів оцінки зрілості.

Підсумок результатів із набором у 2800 екземплярів наведено в таблиці 3.2.

Таблиця 3.2

Підсумок аналізу точності моделі

Підсумок аналізу точності моделі	
Класифіковано правильно (у відсотках)	98.4286%
Класифіковано неправильно (у відсотках)	1.5714 %
Каппа-коефіцієнт	0.979
Середня абсолютна похибка	0.0394
Середньоквадратична похибка	0.1019
Відносна похибка	10.51%
Середньоквадратична відносна похибка	23.5305%

Статистика Каппи описує точність класифікатора [61]. Якщо значення менше або дорівнює нулю, це означає, що не існує відповідності (узгодженості) між еталонним значенням та вхідним вектором даних. В іншому випадку, якщо значення знаходиться в діапазоні від 0.01 до 0.20, це означає, що узгодженості немає або існує

незначна. Діапазон 0.21–0.40 можна інтерпретувати як незначний рівень точності. 0,41–0,60 – середній рівень точності. 0.61–0.80 великий рівень точності, а 0.81–1.00 – дуже високий рівень точності.

Як показують результати навчання, рівень точності передбачення покращився зі збільшенням вибірки для навчання: 96% для 800 екземплярів та 98.43% для 2800 екземплярів (помилковою класифікацією вважатимемо таку класифікацію, під час якої було зараховано вхідний вектор даних до класу, якому він не належить). Звіти сеансів навчання та візуалізація розбіжностей між очікуваним і отриманим результатом зображено на рисунку 3.2.

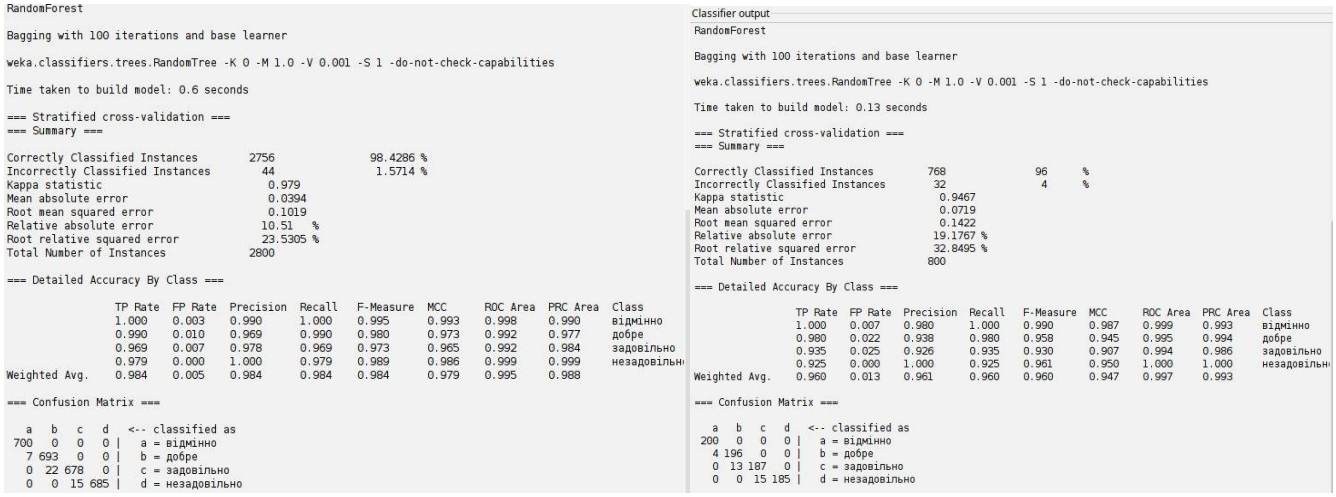

Рисунок 3.2 – Рівень точності передбачення

Після процесу навчання та одержання задовільних результатів передбачення класифікації, було сформований тестовий набір даних із десяти наборів оцінок.

Як наслідок роботи навченої моделі на тестовому наборі даних - ми отримали 90% точності передбачення (рисунок 3.3). В той час, коли перших 5 наборів були сформовані за тим самим принципом, що і вибірка для навчання, 5 інших - навмисно подані таким чином, щоб відловити можливі аномалії.

```
Time taken to test model on supplied test set: 0 seconds

=== Summary ===

Correctly Classified Instances           9               90      %
Incorrectly Classified Instances         1               10      %
Kappa statistic                          0.8667
Mean absolute error                      0.066
Root mean squared error                  0.1567
Relative absolute error                 17.6    %
Root relative squared error             36.1884 %
Total Number of Instances               10

=== Detailed Accuracy By Class ===

                 TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                 1.000    0.000    1.000      1.000    1.000      1.000    1.000     1.000     відмінно
                 1.000    0.125    0.667      1.000    0.800      0.764    1.000     1.000     добре
                 1.000    0.000    1.000      1.000    1.000      1.000    1.000     1.000     задовільно
                 0.667    0.000    1.000      0.667    0.800      0.764    1.000     1.000     незадовільно
Weighted Avg.    0.900    0.025    0.933      0.900    0.900      0.882    1.000     1.000

=== Confusion Matrix ===

 a b c d   <-- classified as
 2 0 0 0 | a = відмінно
 0 2 0 0 | b = добре
 0 0 3 0 | c = задовільно
 0 1 0 2 | d = незадовільно
```

Рисунок 3.3 – Результат класифікації тестової вибірки

Тільки в одному з цих випадків (“1,5,5,5,5,5,5,5,5,5,5,5,5,5,1,незадовільно”) модель не змогла вірно класифікувати рівень захищеності всієї системи.

Висновки за розділом 3

В даному розділі було вирішено задачу проведення аналізу адекватності розробленої моделі.

В результаті виконання задачі було виявлено, що пропонована модель є завершеною, адже має повне покриття контролів IEC 27001. Надмірність та надлишок відсутні. Навчена модель описує реальний неавтоматизований процес оцінки зрілості ІС на прийнятному рівні, і її можна рекомендувати використовувати в процесі реального аудиту СУІБ.

ВИСНОВКИ

Світ змінюється, цифрові та фізичні системи зближуються. Системи, які колись керували критичною інфраструктурою, підключаються до Інтернету та обмінюються конфіденційними даними. Ця нова структура світу несе з собою нові проблеми безпеки. На об’єктах критичної інфраструктури повинні використовуватись надійні засоби та інструменти, які можуть передбачати та пом’якшувати ризики в усьому середовищі критичної інфраструктури. Належний рівень захищеності критичної інфраструктури допомагає організаціям підготуватися до серйозних інцидентів і реагувати на них, а також убезпечити від постійно зростаючого числа загроз.

Сфера стандартизації ІБ дуже фрагментована і складна. Створено велику кількість стандартів, які володіють певною схожістю у використовуваних принципах. Часто стандарти адресують майже однаковий набір вимог та підходів. У таких випадках може бути доречно використовувати

У дипломній роботі розв’язано актуальне наукове завдання щодо розробки нових методів проведення оцінки захищеності. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

Проведено аналіз особливостей забезпечення безпеки об’єктів критичної інфраструктури та їх значення у забезпеченні базових потреб суспільства і держави.

Проаналізовано та описано основні стандарти та підходи в міжнародній, національній (українській зокрема) нормативній базі у сферах кібербезпеки, ІТ менеджменту, безперервності бізнесу та інших.

Запропонований новий метод проведення оцінки захищеності ІС, який володіє універсальністю застосування, зрозумілістю використання та достатністю покриття сфер оцінки. При цьому, запропонований метод потребує значно менше часових, фінансових та людських ресурсів у порівнянні з аудитом у звичному розумінні та підходам у наявних моделях оцінки захищеності.

Створено модель з використанням інструментарію машинного навчання. Модель дозволяє спрогнозувати загальне значення рівня захищеності за наявності оцінених окремих контролів з точністю у 90% відсотків, якщо наданий набір значень має аномалії та 98.43% після процесу навчання і вибірці у 2800 екземплярів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Maturity Models in Information Systems Research: Literature Search and Analysis / J.Poeppelbuss, Niehaves, B, Simons, A., Becker, J.. // Communications of the Association for Information Systems. – 2011. – №29.

3. Security in critical infrastructure [Електронний ресурс] // Sectra Communications AB. – 2020. – Режим доступу до ресурсу: https://sectraprodstorage01.blob.core.windows.net/communication-uploads/sites/4/2021/01/critical-infrastructure-customer-brochure.pdf.

4. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Каб. Міністрів України від 23.08.2016 р. № 563 : станом на 22 жовт. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/563-2016-п#Text

5. What is a Critical Information Infrastructure (CII)?. Michalsons. URL: https://www.michalsons.com/blog/what-is-a-national-critical-information-infrastructure/17701

6. Critical Information Infrastructures. ENISA. URL: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii?tab=details

7. Herrera L.-C., Maennel O. A comprehensive instrument for identifying critical information infrastructure services. International Journal of Critical Infrastructure Protection. 2019. Vol. 25. P. 50–61. URL: https://doi.org/10.1016/j.ijcip.2019.02.001

8. 5 Threats to Critical Infrastructure Security| HUB Security. HUB Security. URL: https://hubsecurity.com/blog/critical-infrastructure-security/5-threats-to-critical-infrastructure-security/

9. The Importance of Critical Infrastructure Security | Cipsec. About | Cipsec. URL: https://www.cipsec.eu/content/importance-critical-infrastructure-security

10. SCADA Cybersecurity | Supervisory Control & Data Acquisition | ISACA Journal. ISACA. URL: https://www.isaca.org/resources/isaca-journal/past-issues/2014/scada-cybersecurity-framework

11. Інформаційні системи та їх роль в управлінні економікою. Ужгородський національний університет. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/6742

12. Cyber-Physical Systems (CPS) (nsf10515). NSF - National Science Foundation. URL: https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

13. Jazdi N. Cyber physical systems in the context of Industry 4.0. 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 22–24 May 2014. 2014. URL: https://doi.org/10.1109/aqtr.2014.6857843

14. Ruoslahti H. Business Continuity for Critical Infrastructure Operators. Annals of Disaster Risk Sciences. 2020. Vol. 3, no. 1. URL: https://doi.org/10.51381/adrs.v3i1.46

15. Shareable Infographics. Global Risks Report 2020. URL: https://reports.weforum.org/global-risks-report-2020/shareable-infographics/?doing_wp_cron=1653566194.3149869441986083984375

16. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. 2012. № 5.

17. Про внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації : Закон України від 04.06.2020 р. № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text

18. ТЗІ - інформаційна безпека та захист інформації - Інформаційна безпека та захист інформації. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf

19. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань "Нормативний документ").

20. Model of the quantitative criterion calculation for security assessment of the information and telecommunications systems in the critical infrastructure of the state / O. Yudin et al. Advanced Information Systems. 2021. Vol. 5, no. 4. P. 109–115. URL: https://doi.org/10.20998/2522-9052.2021.4.15

21. ISO/IEC 15408. Encyclopedia of Cryptography and Security. Boston, MA, 2011. P. 648. URL: https://doi.org/10.1007/978-1-4419-5906-5_1338

22. A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045 / H. Chen et al. Computer Science and its Applications. Berlin, Heidelberg, 2015. P. 1359–1366. URL: https://doi.org/10.1007/978-3-662-45402-2_189

23. Fekete A. Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science. 2011. Vol. 2, no. 1. P. 15–24. URL: https://doi.org/10.1007/s13753-011-0002-y

24. 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. URL: https://doi.org/10.30748/soivt.2018.56.13

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

26. Толюпа С. В., Наконечний В. С., Якименко Ю. М. Оценка защищённости информации в автоматизированных информационных системах с помощью Общих критериев. Наукові записки Українського науково-дослідного інституту зв'язку. 2015. № 6.

27. Stine K. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Ukrainian Translation). National Institute of Standards and Technology, 2022. URL: https://doi.org/10.6028/nist.cswp.04162018uk

28. Maturity Models in Information Systems Research: Literature Search and Analysis / J. Poeppelbuss et al. Communications of the Association for Information Systems. 2011. Vol. 29. URL: https://doi.org/10.17705/1cais.02927

29. Cybersecurity Capability Maturity Model (C2M2). Energy.gov. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

30. Viktoriia Hrechko, Hryhorii Hnatiienko and Tetiana Babenko. An intelligent model to assess information systems security level // VII International conference on Information Technology and Interactions (WorldS4 2021)

31. Community Cyber Security Maturity Model – CIAS ISAO. CIAS ISAO – Community Cybersecurity Programs. URL: https://ciasisao.org/ccsmm/

32. Waldt, G.V.D. (2013), “Disaster risk management : disciplinary status and prospects for a unifying theory : original research”, Jamba : Journal of Disaster Risk Studies, Vol. 5 No. 2, pp. 1-11.

33. Modelling adaptive information security for SMEs in a cluster / B. Yigit Ozkan et al. Journal of Intellectual Capital. 2019. Vol. 21, no. 2. P. 235–256. URL: https://doi.org/10.1108/jic-05-2019-0128

34. Yigit Ozkan B., van Lingen S., Spruit M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. Journal of Cybersecurity and Privacy. 2021. Vol. 1, no. 1. P. 119–139. URL: https://doi.org/10.3390/jcp1010007

35. What is ISO 27001? A beginner’s guide. 27001Academy. URL: https://advisera.com/27001academy/what-is-iso-27001/

36. ISO 27001:2017, International Standard ISO/IEC Information technology — Security techniques — Information security management systems — Requirements, vol. 2017, 2017.

37. ISO 22301 - Система непрерывности бизнеса | TMS Academy. TMS Academy. URL: https://academy.tms.ua/sertificat/standart-iso-22301-sistema-menedzhmenta-nepreryvnosti-biznesa-bcms/

38. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. Official edition.

39. NIST Risk Management Framework | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/projects/risk-management/about-rmf

40. Risk management framework for information systems and organizations:. Gaithersburg, MD : National Institute of Standards and Technology, 2018. URL: https://doi.org/10.6028/nist.sp.800-37r2

41. The Complete Guide to ITIL 4. BMC Blogs. URL: https://www.bmc.com/blogs/itil-4/

42. Agutter C. ITIL Foundation Essentials ITIL 4 Edition: The Ultimate Revision Guide. IT Governance Ltd, 2020. 90 p.

43. ISO 19011: Guidelines for Auditing Management Systems | ASQ. Excellence Through Quality | ASQ. URL: https://asq.org/quality-resources/iso-19011

44. Overview of ISO 19011:2018 Guidelines for Audit Management Systems. Qualityze. URL: https://www.qualityze.com/a-quick-overview-of-iso-190112018-guidelines-for-auditing-standards/

45. Comparison of IoT Security Frameworks. Comparison of IoT Security Frameworks. URL: https://www.eurofins-cybersecurity.com/news/comparison-iot-security-frameworks/

46. Занадто критична інфраструктура - Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/publications/practice/transportne-pravo/zanadto-kritichna-infrastruktura.html

47. Critical infrastructure. Migration and Home Affairs. URL: https://ec.europa.eu/home-affairs/pages/page/critical-infrastructure_en

48. China's Cybersecurity Law: Critical Information Infrastructure | Protiviti - Hong Kong. Protiviti - United States. URL: https://www.protiviti.com/HK-en/insights/pov-critical-information-infrastructure

49. What is Maturity Level | IGI Global. IGI Global: International Academic Publisher. URL: https://www.igi-global.com/dictionary/maturity-metrics-health-organizations-information/18046

50. Аудит безпеки інформаційної безпеки. Техническая защита информации, средства защиты информации, информационная безопасность, тзи, ксзи, антижучки. URL: https://tzi.com.ua/audbezib.html

51. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Вид. офіц. Київ.

52. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

53. Учасники проектів Вікімедіа. Common Criteria – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Common_Criteria

54. Грабченко А., Федорович В. Методи наукових досліджень. Харків, 2009.

55. ДОСТАТНІЙ – Академічний тлумачний словник української мови. Академічний тлумачний словник української мови. URL: http://sum.in.ua/s/dostatnij

56. Weka 3 - Data Mining with Open Source Machine Learning Software in Java. Department of Computer Science: University of Waikato. URL: https://www.cs.waikato.ac.nz/ml/weka/

57. Top 10 algorithms in data mining / X. Wu et al. Knowledge and Information Systems. 2007. Vol. 14, no. 1. P. 1–37. URL: https://doi.org/10.1007/s10115-007-0114-2

58. Contributors to Wikimedia projects. Decision tree learning - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Decision_tree_learning

59. Contributors to Wikimedia projects. Random forest - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Random_forest

60. 1. Breiman L. Machine Learning. 2001. Vol. 45, no. 1. P. 5–32. URL: https://doi.org/10.1023/a:1010933404324

61. Portugal I., Alencar P., Cowan D. The use of machine learning algorithms in recommender systems: A systematic review //Expert Systems with Applications. – 2018. – Т. 97. – С. 205-227.

ДОДАТОК А

1. Бабенко Т.В., Бужора В.Ю., Модель оцінки захищеності ІС на ОКІІ. IV Міжнародної науково-практичної конференції PCSITS – 2022 – подано тези.