КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК

рішенням кафедри радіотехніки та радіоелектронних систем

від ___ травня 2025 року, протокол № ___.

Завідувач кафедри доктор фіз.-мат. наук, професор

_____ Ігор АНІСІМОВ

ДИПЛОМНА РОБОТА МАГІСТРА

на тему:

«ОЦІНЮВАННЯ РИЗИКІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА РОЗРОБКА ВИМОГ ДО КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВЕБСАЙТУ УКРАЇНСЬКОГО ЦЕНТРУ ОЦІНЮВАННЯ ЯКОСТІ ОСВІТИ»

Виконала:

студентка 2-го курсу магістратури денної форми навчання

спеціальності 172 – Електронні комунікації та радіотехніка

ОНП «Інформаційна безпека телекомунікаційних систем і мереж»

Литвенюк Ірина Геннадіївна _____

Науковий керівник:

канд. військ. наук, доцент

Довбня Сергій Якович _____

Рецензент:

канд. технічних наук, старший науковий співробітник

Генадій Павлович Леоненко_____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань

Студентка _____ Ірина ЛИТВЕНЮК

Київ 2025

РЕФЕРАТ

Магістерська робота: 82 с., 5 рис., 4 табл., 12 джерел.

За допомогою SWOT аналізу проаналізовано особливості функціонування інформаційно комунікаційної системи ВЕБ САЙТ УЦОЯО. Побудовані модель загроз та модель порушників інформаційної безпеки, на основі проведеного аналізу. Виставлені оцінки ефективного рівня загрози за трьома параметрами впливу на систему: доступність конфіденційність, цілісність. Методом попарних порівнянь (AHP - Analytic Hierarchy Process) визначені вагові коефіцієнти кожного параметру для різних типів інформації (конфіденційна, технологічна, відкрита) і розрахована оцінка ризику для кожної загрози. Проведений аналіз отриманих результатів та на його основі розроблені вимоги до комплексів заходів захисту, які можуть бути впроваджені в подальшому для підвищення рівня захисту інформації що циркулює в системі та зниження ризиків.

ІНФОРМАЦІЙНА БЕЗПЕКА, ОЦІНКА РИЗИКІВ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ, ЗАГРОЗ, SWOT – АНАЛІЗ, МЕТОД ПОПАРНИХ ПОРІВНЯНЬ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІКС – Інформаційно комунікативна система

ІБ – Інформаційна безпека

УЦОЯО - Український центр оцінювання якості освіти

ЗОО – Зовнішнє освітнє оцінювання

ТІ – Технологічна інформація

СЗІ – Служба захисту інформації.

СКБД – Система керування базами даних

АРМ -Автоматизоване робоче місце

ВСТУП

У сучасному цифровому світі інформаційна безпека є важливим критерієм, коли йдеться про захист персональних даних та захист інформаційних систем. Однією із таких систем є веб-сайт Українського центру оцінювання якості освіти (УЦОЯО), що зберігає багато конфіденційних даних, як наприклад результати тестувань, особисті дані абітурієнтів та важлива статистична інформація.

Враховуючи значення цих даних важливо побудувати комплекс заходів захисту для такої системи, що буде забезпечувати інформаційну безпеку. Це вимагає комплексного підходу, що включає не тільки технічні засоби захисту, а й організаційні, правові та адміністративні. Першим етапом розробки ефективної стратегії безпеки для інформаційно-комунікативної системи (ІКС) є оцінка ризиків та виявлення можливих загроз і вразливостей системи.

Оцінювання ризиків дозволяє зрозуміти, які загрози є більш ймовірними та які можуть нанести найбільші збитки. Для цього використовуються методи аналізу, які дозволяють систематизувати ризики та визначити пріоритети заходів безпеки.

Одним із інструментів в управлінні ризиками є SWOT-аналіз. Він дозволяє оцінити слабкі та сильні сторони системи, а також виявити можливості й загрози які мають вплив на безпеку. Доповненням до SWOT-аналізу виступає метод аналізу ієрархій (AHP), який дозволяє кількісно оцінити ризики, та порівняти їх між собою, а також визначити пріоритетні напрямки захисту системи.

Мета роботи: Провести оцінювання ризиків захисту інформації веб-сайту УЦОЯО та на основі цього розробити вимоги до комплексу заходів захисту з урахуванням актуальних загроз і специфіки системи.

Завдання роботи:

1. Дослідити особливості структури та функціонування веб-сайту УЦОЯО як об’єкта інформаційної безпеки.
2. Побудувати модель порушників та модель загроз.

3. Розрахувати ризик для кожної окремої загрози.

4. Сформулювати вимоги до комплексу засобів захисту інформації з урахуванням результатів аналізу.

1. ОГЛЯД ЛІТЕРАТУРИ

1.1. Оцінювання ризику

Ризик інформаційної безпеки – це числова (або словесна) функція, яка описує ймовірність настання загрози для ІБ та величину збитку у разі реалізації цієї загрози з використанням слабких місць інформаційної системи для нанесення шкоди системі. [1]

Керування ризиками є важливим процесом для ІБ системи, що базується на прийнятті рішень та здійсненні заходів для зменшення вразливостей системи. Основними етапами цього процесу є встановлення оточення (визначення основних параметрів керування ризиком та сферу застосування), загальне оцінювання ризику (забезпечує розуміння ризиків, їхні причини та наслідки, а також ймовірність реалізації), оброблення ризику (впровадження мір та заходів, що направленні на зниження ймовірності реалізації ризиків). [2].

Основним етапом є загальне оцінювання ризику, тож розглянемо його більш детально. Оцінювання ризику поділяється на три етапи: ідентифікація ризику, аналіз ризику, оцінювання ризику. Ідентифікація ризику спрямована на аналіз системи та визначення ситуацій які можуть статися та негативно повипливати на функціонування системи. Процес ідентифікації ризику охоплює визначення причин та джерел ризику, подій, ситуацій або обставин які можуть чинити матеріальний вплив на досягнення цілей системи, а також визначення характеру цього впливу. Аналізування ризику полягає у визначенні наслідків у разі реалізації ризику, а також ймовірність реалізації ризику. Оцінювання ризику побудоване на основі результатів попереднього етапу, слугує для прийняття рішень щодо подальших дій. Рішення залежать від потреби в обробленні ризику, пріоритетів оброблення, доцільності виконання якоїсь роботи. [2]

Алгоритм керування ризиками представлений на Рис 1.1

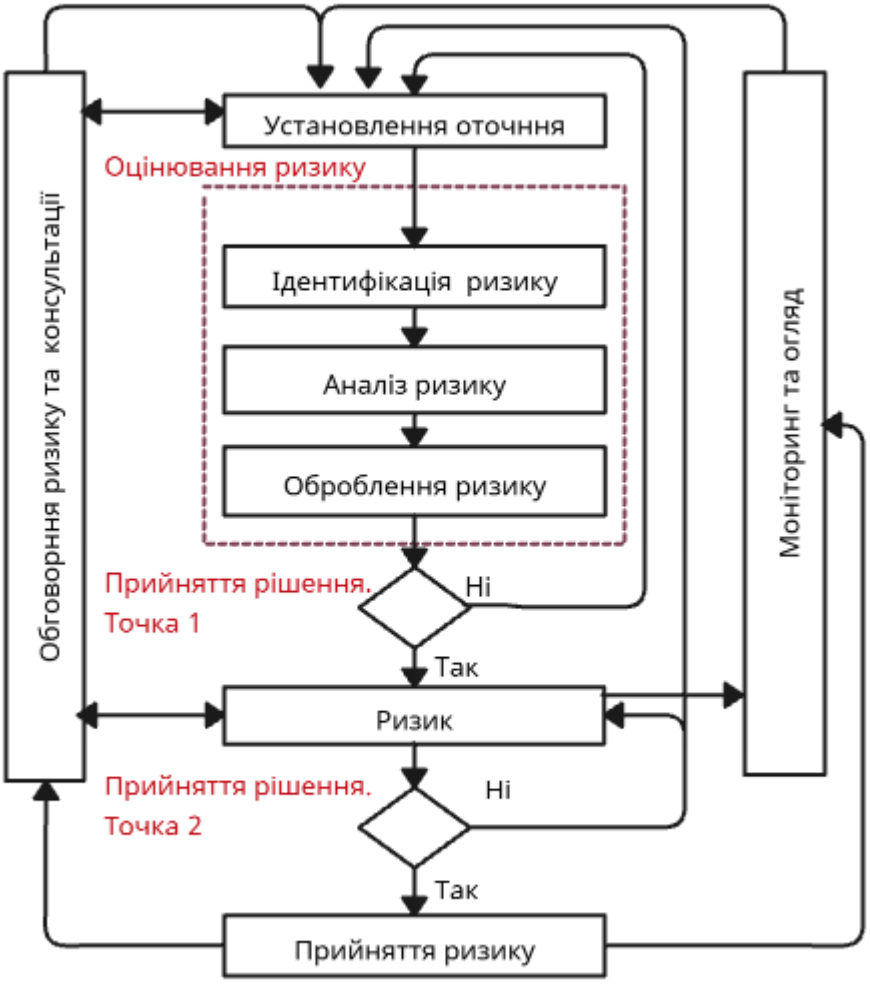


Рис. 1.1 Схема керування ризиками [6]

1.2. Модель порушника

Порушник – це людина, яка навмисно або випадково вчиняє дії, що можуть нанести шкоду ІКС. Розділення потенційних порушників за категоріями, значно допомагає зрозуміти їх можливості та загрози що вони можуть нести. Для оцінки рівня загрози порушника в залежності від категорії будується модель порушника.

Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, знання, час та місце його дії, тощо. [4]

В загальному випадку порушники класифікуються за чотирма рівнями можливостей:

- Перший рівень – найнижчий рівень можливостей, що передбачає тільки запуск фіксованого набору завдань, що реалізують заздалегідь передбачені функції обробки інформації.
- Другий рівень – характеризується можливістю створення і запуску власних програм обробки інформації.
- Третій рівень – визначається можливістю впливу на базове програмне забезпечення ІКС.
- Четвертий рівень – визначається всім обсягом можливостей осіб, що забезпечують функціонування КЗЗ в ІКС.

Порушником по відношенню до ІТК можуть бути особи з персоналу і користувачів системи, а також сторонні особи. [4]

1.3. Модель загроз

Моделювання загроз передбачає створення моделі різних дій зловмисників і вразливостей, які потенційно загрожують безпеці ІКС.

Вразливості – нестача засобів захисту ІКС, що може бути використана зловмисником, для реалізації загрози.

Загрози для інформації що обробляється залежить від фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об’єктивну або суб’єктивну природу. Тому модель загроз будується на основі аналізу особливостей функціонування системи та її компонентів, а також важливості інформації яка циркулює в ній. [5]

Загроза безпеки інформації виникає за наявності наступних взаємопов’язаних компонентів:

- джерела загрози,
- уразливості активу,
- способу реалізації загрози,
- об’єкту впливу,
- шкідливого впливу.

2. МЕТОДОЛОГІЯ

2.1. SWOT аналіз

SWOT-аналіз є початковим етапом планування стратегії організації та може слугувати відправною точкою для більш детального вивчення проблем у сфері ризиків ІБ. Він є досить простим застосуванні і не потребує наявності досвідчених експертів для його проведення. [6]

SWOT (Strength, Weakness, Opportunities, Threats) аналіз передбачає детальний опис сильних сторін, слабких сторін, можливостей та загроз при розробці стратегії організації. Результати проведеної роботи представляються у вигляді матриці (Рис 2.1).

Сильні сторони (Strength)	Слабкі сторони (Weakness)
S1 S2	W1 W2
Можливості (Opportunities)	Загрози (Threats)
O1 O2	T1 T2

А

	Загрози (T)	Можливості (O)
Сильні сторони (S)	Покращити сильну сторону щоб протистояти загрозі ST	Використовувати сильну сторону щоб отримати перевагу у даній можливості SO
Слабкі сторони (W)	Мінімізувати кількість вразливостей щоб уникнути загрозі WT	Мінімізувати вплив слабких сторін за рахунок можливостей WO

Б

Рис 2.1 А) Матриця якісного SWOT-аналізу, Б) Матриця прийняття рішень.

Основними принципами застосування цього методу є:

- Дослідження сильних сторін системи, та конкурентні переваги;
- Вивчення слабких сторін системи та внутрішніх негативних чинників;
- Визначення можливих загроз та своєчасного попередження втрат;
- Аналіз можливостей системи для посилення сильних сторін і зменшення слабких.

Такий підхід до первинного аналізу системи може бути застосований до оцінки ризиків ІКС. Реалізуючи його для оцінки ризиків слід акцентувати увагу на протидії внутрішнім слабким сторонам системи з боку зовнішніх загроз та побудові стратегії захисту із використанням сильних сторін та можливостей. [6]

Існують два види SWOT-аналізу – якісний та кількісний.

Якісний SWOT-аналіз базується на словесній шкалі можливих наслідків (низькі, середні, високі) та ймовірності цих наслідків. Використовується якісний аналіз зазвичай у таких випадках:

- Як відправна точка в ідентифікації ризиків;
- Якщо такого рівня аналізу достатньо для прийняття рішення;
- Якщо відсутні числові дані для кількісного оцінювання ;

Після збору інформації про ІКС яка потребує захисту заповнюються SWOT матриці (Рис 2.1), а також може бути зроблена інтерактивна матриця пріоритетності між зовнішніми загрозами та внутрішніми слабкими сторонами (Рис 2.2) [6]

	T1 (Природні катастрофи)	T2 (Переманювання фахівців)	T3 (Кіберзагрози)
W1	+	+	+
W2	+	0	+
W3	0	+	+

Рис. 2.2 Інтерактивна матриця пріоритетності

Кількісний SWOT-аналіз працює з числовими даними, тому є більш точним. Для поєднання кількісного оцінювання зі SWOT-аналізом також застосовується метод аналізу ієрархій. [6]

Кількісний аналіз включає в себе десять кроків:

1. Визначити контекст ризиків для ІКС. Тобто проаналізувати вразливості системи та скласти список можливих загроз;
2. Збір статистичних даних;
3. Визначення вагових коефіцієнтів внутрішніх та зовнішніх загроз за допомогою методу аналізу ієрархій;
4. Обчислення ступеня ризику за формулою

$$r_{ij} = p_i q_j, \tag{2.1}$$

де p_i – ступінь вразливості системи, q_j – оцінка ймовірності реалізації загрози;

5. Знаходження ймовірності виникнення інциденту;
6. Створення ранжованого списку ризиків;
7. Обчислення загального рівня ризику

$$R_{заг} = \sum r_{ij}; \tag{2.2}$$

8. Порівняння загального ризику із граничним рівнем ризику;
9. Обробка ризику;
10. Прийняття ризику;

2.2. Метод попарних порівнянь (AHP – Analytic Hierarchy Process)

AHP метод який допомагає обрати оптимальне рішення серед можливих альтернатив, враховуючи кілька критеріїв. Він полягає в оцінці відносної важливості критеріїв та альтернатив через серію попарних порівнянь, де експерт визначає відносну важливість кожного критерію. Такий підхід дозволяє математично розрахувати вагу кожного критерію, та ранжувати альтернативи відповідно до їхніх переваг.

Першим етапом цього методу є визначення критеріїв а також альтернатив за якими оцінюються дані критерії. На другому етапі проводиться експертне оцінювання, де кожна пара критеріїв порівнюється за допомогою шкали важливості. Зазвичай ця шкала має значення від 1 до 9, де 1 — однакова важливість обох критеріїв, 9 – абсолютна перевага одного з критеріїв.

На основі результатів попарних порівнянь створюється матриця попарних порівнянь. Для кожної пари критеріїв чи альтернатив вводиться коефіцієнт a_{ij} який описує важливість *i* критерію відносно *j* критерію. Діагональні елементи такої матриці будуть дорівнювати 1, бо критерій порівнюється сам із собою, а $a_{ij} = \frac{1}{a_{ji}}$.

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & 1 & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \frac{1}{a_{3n}} & \cdots & 1 \end{pmatrix} \tag{2.3}$$

Далі потрібно знайти вагові коефіцієнти. Спочатку обчислюємо найбільше власні значення матриці за формулою:

$$det(A - \lambda I) = 0. \tag{2.4}$$

Вагові коефіцієнти знаходяться за формулою:

$$\omega_i = \frac{1}{\lambda_{max}} \sum_{j=1}^{n} a_{ij} \omega_j \tag{2.5}$$

та сума вагових коефіцієнтів:

$$\sum_{i=1}^{n} \omega_i = 1 \tag{2.6}$$

Таким чином розраховані вагові коефіцієнти можна використовувати в подальшому для прийняття оптимальних рішень щодо використання альтернатив. Більш детальний опис використання методу AHP описаний в роботі [7].

3. ОРИГІНАЛЬНА ЧАСТИНА

3.1. Опис ІКС ВЕБ САЙТ УЦОЯО

3.1.1. Інформація що обробляється в ІКС ВЕБ САЙТ УЦОЯО

Інформація що оброблюється у ІКС ВЕБ САЙТ УЦОЯО поділяється на дві категорії:

- відкрита інформація;
- інформація з обмеженим доступом – конфіденційна інформація (персональні дані, технологічна інформація).

Відкрита інформація, це та інформація доступ до якої мають користувачі системи. До інформації цієї категорії висуваються підвищені вимоги щодо забезпечення цілісності та доступності.

До відкритої інформації відноситься:

- інформація профільної діяльності УЦОЯО;
- інформаційно-довідкові ресурси ІКС ВЕБ САЙТ;
- статистична інформація;
- інформаційні матеріали (статті, публікації, посилання на зовнішні джерела, файли, дані), які знаходяться в публічному доступі;
- інформаційні ресурси загального користування - інформаційні об’єкти, що містять матеріали інформаційно-довідкового характеру, доступні всім користувачам (інформаційні ресурси загального користування представлені у вигляді – каталогів, файлів, електронних листів, веб-сторінок);
- інформація щодо проведення ЗНО.

Конфіденційна інформація потребує вищого рівня захисту, так як складається з персональних даних користувачів та технологічної інформації.

Персональні дані користувачів ІКС веб сайту УЦОЯО є конфіденційною інформацією у відповідності до Закону України «Про захист персональних даних».

Доступ до неї мають тільки вповноважені користувачі згідно зі своїх посадових обов’язків.

До персональної інформації відноситься:

- прізвище, ім'я, по батькові (за наявності);
- число, місяць і рік народження;
- тип, серія (за наявності) та номер документа, що посвідчує особу, на підставі якого здійснюється реєстрація;
- реєстраційний номер облікової картки платника податків (далі - РНОКПП);
- диплом про здобуття вищої освіти;
- інша персональна інформація.

Технологічна інформація (ТІ) складається з комплексу заходів захисту, інформації щодо адміністрування та управління ІКС. Вона призначена для використання тільки уповноваженими користувачами з числа співробітників служби захисту інформації та персоналу що забезпечує функціонування ІКС.

До технологічної відноситься інформація наступного змісту:

- параметри налаштування операційних систем, СКБД, правил розмежування доступу, параметрів безпеки домена;
- параметри налаштування СПЗ;
- параметри налаштування міжмережевих екранів та комунікаційного обладнання;
- налаштування параметрів антивірусного захисту для серверів, робочих станцій;
- паролі, пін-коди та інші конфіденційні реквізити доступу адміністраторів та користувачів ІКС;
- журнали подій та налаштування щодо фіксації подій у журналах.

За способом надходження інформація в ІКС поділяється на:

- зовнішню інформацію, яка надходить на об’єкт від зовнішніх

користувачів у вигляді транзитних IP-пакетів;

- внутрішню інформацію, яка створюється в ІКС у вигляді різноманітних електронних документів, яка зберігається, оброблюється і може передаватися зовнішнім користувачам;
- внутрішню, яка створюється в електронному вигляді і залежно від призначення виводиться на «тверді носії».

Інформація, що обробляється в ІКС, розподіляється за такими видами:

- дані – у вигляді електронних документів, окремих файлів, каталогів, записів БД та ін.;
- базове системне ПЗ – мережні ОС, ОС РС (АРМ), СКБД та ін.;
- ППЗ – для забезпечення обробки текстових, графічних та ін. даних;
- БД захисту – списки зареєстрованих користувачів, їх ідентифікаторів, повноважень користувачів, матриці доступу, журнали реєстраційних подій та ін.;
- додаткові спеціалізовані засоби захисту – засоби антивірусного захисту, засоби сканування мережі, міжмережеві екрани та ін.;
- сервісне ПЗ;
- інструментальні засоби розробки й налагодження програм.

3.1.2. Опис компонентів ІКС ВЕБ САЙТ УЦОЯО та технології обробки інформації

ІКС є багатомашинним багатокористувацьким комплексом, до складу якого входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі, технологія її оброблення.

ІКС має сервісно-орієнтовану архітектуру та складається зі структурних елементів та функціональних модулів.

Структурними елементами ІКС є адміністративна частина, загальнодоступна частина та особисті кабінети користувачів.

Функціональні модулі ІКС реалізують певні його функції і можуть працювати як незалежно, так і разом зі структурними елементами ІКС, створюючи єдину систему.

ІКС ВБ САЙТ УЦОЯО взаємодіє з наступними ІКС:

- вебпортал «Дія»;
- сервіс «Дія.Підпис»;
- сервіс «Дія.Шеринг».
- ІКС УЦОЯО ;

Структура побудови ІКС ВЕБ САЙТ УЦОЯО наведена на рисунку 3.1.

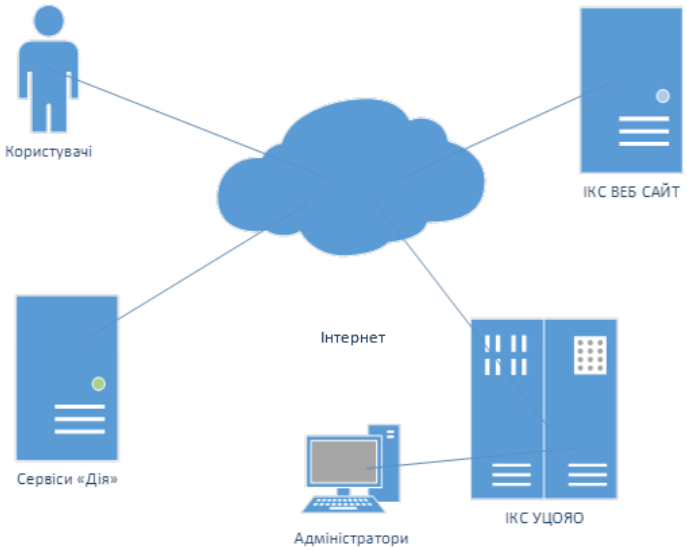


Рис. 3.1 Структурна схема ІКС ВЕБ САЙТ УЦОЯО

У точці доступу ІКС ВЕБ САЙТ до мережі Інтернет знаходиться апаратний засіб мережевого захисту – міжмережевий екран.

3.1.3. Загальний алгоритм роботи ІКС ВЕБ САЙТ УЦОЯО

ІКС функціонує у штатному режимі і надає послуги протягом робочого часу, визначеного внутрішніми розпорядчими документами УЦОЯО. Перерви в роботі

можливі для виконання необхідних технологічних процесів та в разі настання обставин аварійних характеру.

Всі інформаційні ресурси зберігаються та обробляються на серверному обладнанні ІКС. Технологія обробки інформації в ІКС побудована як клієнт серверний додаток, з урахуванням веб стандартів, за технологією «клієнт-сервер» шляхом взаємодії обчислювальних засобів сервера та ПК користувачів.

Інформація, що містить відомості про особу (персональні дані) зберігається на сервері БД ІКС ВЕБ САЙТ УЦОЯО та відображається з використанням внутрішнього доступу до ІКС користувачами з відповідними правами для подальшої її обробки.

Відомості що вносяться до ІКС зберігаються у БД ІКС ВЕБ САЙТ УЦОЯО. Безпосередній доступ користувачів до інформації, що зберігається в БД здійснюється у відповідності до визначених повноважень користувачів.

Інформація технологічного характеру компонентів ІКС використовується для функціонування ІКС та зберігається на сервері БД ІКС ВЕБ САЙТ УЦОЯО.

Інформація технологічного характеру призначена для використання тільки уповноваженими користувачами з числа співробітників служби захисту інформації (СЗІ) та персоналу, що забезпечує функціонування ІКС. Вони надають технологічну підтримку користувачам, виконують аналіз аудиту дій користувачів, управління сесіями, перегляд подій про помилки в ІКС та інше, передбачене службовими/посадовими обов’язками.

Адміністрування компонентів ІКС (серверу та комутаційного обладнання) здійснюється уповноваженими адміністраторами - штатними співробітниками УЦОЯО. Для адміністрування ІКС ВЕБ САЙТ УЦОЯО використовуються АРМ зі складу ІКС УЦОЯО.

Доступ адміністраторів до ІКС здійснюється з використанням логіна і пароля та носія ключової інформації.

Для доступу до ресурсів ІКС користувачі та адміністратори використовують АРМ у складі ПК та ноутбуків. АРМ дозволяють вносити та редагувати інформацію з використанням візуального інтерфейсу доступу та вводу-виводу інформації, що реалізовано за результатами функціонування ІКС.

Функції адміністрування ІКС включає моніторинг її роботи та забезпечує надання або припинення доступу користувачам до інформаційних ресурсів системи.

Моніторинг та аудит роботи ІКС здійснюється за рахунок використання системних інструментів.

Адміністратори та користувачі отримують доступ до компонентів веб сайту відповідно до своїх повноважень згідно визначених ролей та функціональних обов'язків.

Структурні компоненти ІКС та налаштування ПЗ забезпечують створення резервних копій баз даних, файлів налаштувань. Відновлення інформації у випадку аварій виконуються за допомогою сценаріїв системним адміністратором.

Обмін інформації з обмеженим доступом по незахищеним каналам зв'язку здійснюється з використанням засобів криптографічного захисту інформації що мають діючий експертний висновок в сфері криптографічного захисту інформації.

Доступ користувачів до персонального кабінету в ІКС ВЕБ САЙТ УЦОЯО здійснюється з використанням веб застосунку «Дія.Підпис» або самостійно, заповнивши реєстраційну форму.

Отримання копій цифрових документів користувачів в ІКС ВЕБ САЙТ здійснюється з використанням веб застосунку «Дія.Шеринг».

Обмін інформацією між ІКС УЦОЯО та ІКС ВЕБ САЙТ УЦОЯО здійснюється в автоматичному режимі з використанням засобів криптографічного захисту інформації.

3.2. Модель порушника безпеки інформації ІКС ВЕБ САЙТ УЦОЯО

Модель порушника для даної системи ІКС веб сайту була побудована на основі особливостей функціонування системи.

Класифікація зовнішніх і внутрішніх порушників здійснюється на основі критеріїв, що зведені до таблиці 3.1. Слід зауважити, що рівні знаходяться у ієрархічній залежності і отже кожен наступний рівень включає функціональні можливості попередніх.

Табл. 3.1

Критерії класифікації порушників за рівнями

Рівень	**Критерії**			
	можливості, які є у порушника	**рівень знань про ІКС**	**методи і способи порушень**	**місце здійснення дії**
1.	ведення діалогу і запуск фіксованого набору задач (програм), які реалізують наперед передбачені функції обробки інформації	знання інформації про функціональні особливості ІКС, закономірності формування в ньому масивів даних і потоків запитів до них, навички застосування штатних засобів	виключно агентурні методи впливу	без отримання доступу до складових частин ІКС
2.	створення і запуск власних програм з новими функціями	високий рівень знань та досвід роботи і	виключно штатні засоби ІКС або недоліки	з отриманням доступу на

	обробки інформації	обслуговування технічних засобів, що використовуються в ІКС	проектування КСЗІ для реалізації спроб НСД	територію власника ІКС, але без доступу до ІКС
3.	управління функціонуванням складових частин ІКС, тобто впливом на базове ПЗ системи, конфігурацію та склад і обладнання	високий рівень знань в галузі обчислювальної техніки, програмування, проектування і експлуатації ІКС	способи і засоби активного впливу на ІКС, які змінюють конфігурацію системи (підключення додаткових або модифікація технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ)	з отриманням доступу до РС (АРМ) ІКС
4.	усі можливості осіб, що здійснюють проектування, реалізацію, впровадження, супровід	Володіння інформацією про функції і механізми дії засобів захисту	–	з отриманням доступу до засобів адміністрування і засобів управління

	програмно-апаратного забезпечення ІКС, аж до включення в склад ІКС власних засобів з новими функціями обробки інформації			КСЗІ ІКС

За можливістю реалізації загроз конфіденційності, цілісності та доступності інформації і інформаційних ресурсів, що обробляються в ІКС, порушники в складових частинах системи розташовуються в такому порядку із зменшенням ступеня небезпеки:

- адміністратори;
- зареєстровані користувачі;
- незареєстровані користувачі;
- розробники;
- представники контролюючих органів;
- відвідувачі.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Тому для повної характеристики порушника були обрані такі параметри:

- мотив порушення;
- основні кваліфікаційні ознаки порушника;
- характеристика можливостей порушника;
- характеристика місця дії поршника;
- характеристика часу дії порушника;

Кожна окрема характеристика була проаналізована та оцінена за ефективним рівнем загрози. Результати представлені у вигляді таблиць у Додатку А.

Фінальна модель порушника за усіма характеристиками представлена в таблиці 3.2

Таблиця 3.2

Оцінка ризиків по категоріям порушників

Позначення	Визначення категорії	Характер дій порушника					Оцінка ризику
		Мотив порушення	Кваліфі-кація	Можли-вості	Час дії	Місце дії	
П1	Адміністратор безпеки	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П2	Системний адміністратор	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П3	Редактор новин	М1, М2	К4	З3	Ч1-Ч3	Д2, Д3	5
П4	Зареєстрований користувач	М1, М2	К1-К4	З2	Ч1-Ч3	Д2	4.73
П5	Незареєстрований користувач	М1, М2	К1-К3	З1	Ч2	Д2	4.24
П6	Представники контролюючих органів	М2	К2-К4	З1	Ч1-Ч3	Д1	4.18
П7	Розробники	М2	К1-К4	З4	Ч3	Д2-Д3	4.27
П8	Відвідувачі	М2	К1-К4	З4	-	Д1	3.71

Кожна категорія порушників може мати декілька можливих характеристик по кожному параметру з різною оцінкою рівня загрози. Для адекватної оцінки ризику

було прийняте рішення використовувати максимальне значення загрози з усіх можливих характеристик по даному параметру.

Такий підхід зумовлений необхідністю моделювання найгіршого з можливих сценаріїв дій порушника в межах заданих характеристик. Іншими словами, навіть якщо порушник має доступ до кількох режимів часу або місць дії, оцінюється саме той режим, за якого загроза буде максимально ймовірною.

Крім того, використання максимального значення дозволяє враховувати ситуації, коли порушник може мати неповний, але потенційно критичний доступ до компонентів ІКС та гарантувати, що всі можливі шляхи реалізації загроз ураховані при формуванні матриці відповідності загроз і порушників.

Такий підхід відповідає підходам, рекомендованим у ISO/IEC 27005:2018, де акцент робиться на оцінці ризику з урахуванням усіх доступних можливостей порушника.

Оцінка ризику розрахована за формулою

$$R(P_i) = \omega_M M_i + \omega_K K_i + \omega_z Z_i + \omega_T T_i + \omega_L L_i, \quad (3.1)$$

де M_i – максимальне значення ефективного рівня загрози за мотивом порушення, K_i - максимальне значення ефективного рівня загрози за кваліфікацією, Z_i - максимальне значення ефективного рівня загрози за можливостями, Ti - максимальне значення ефективного рівня загрози за часом дії, Li – максимальне значення ефективного рівня загрози за місцем дії, $\omega_M, \omega_K, \omega_z, \omega_T, \omega_L$ - вагові коефіцієнти для відповідного параметра

Вагові коефіцієнти були розраховані за методом AHP.
1) На основі присвоєння кожному параметру оцінки важливості відносно іншого параметру за шкалою від 1 до 9 складена матриця попарних порівнянь:

Таблиця 3.3

Матриця попарних порівнянь

	M	K	Z	T	L
M	1	3	4	5	5
K	1/3	1	2	3	3
Z	1/4	1/2	1	2	2
T	1/5	1/3	1/2	1	2
L	1/5	1/3	1/2	1/2	1

2) Розрахована сума елементів по кожному стовпцю

3) Проводиться нормалізація матриці шляхом ділення кожного елементу на суму його стовпця

4) Для кожного критерію береться середнє значення по рядку нормалізованої матриці – це і буде вага критерію

Результати розрахунків представлені в таблиці 3.4.\

Таблиця 3.4

Вагові коефіцієнти критеріїв пораховані за методом AHP

Критерій	Значення коефіцієнта
Мотив	0.48
Кваліфікація	0.22
Можливості	0.14
Час	0.09
Місце	0.07

3.3. Модель загроз для ІКС веб сайт

Для формування повної моделі загроз ІКС ВЕБ САЙТ УЦОЯО було здійснено систематичний аналіз потенційних загроз, які можуть впливати на конфіденційність, цілісність та доступність інформаційних активів. Перелік загроз сформовано на основі: міжнародних стандартів ISO/IEC 27005:2018; національних документів (зокрема, КЗІ-каталоги типових загроз); документації УЦОЯО щодо структури інформаційних активів та інцидентів безпеки.

Кожна загроза оцінена за шкалою від 1 (низький вплив) до 5 (критичний вплив) по трьох параметрах впливу на систему: конфіденційність, доступність, цілісність. Також визначні значення вразливості та ймовірності реалізації загрози. Рівень вразливості визначний на основі аналізу наявності існуючих заходів захисту, які можуть протидіяти загрозі, а також ступеня слабкості захисту. Ймовірність реалізації загроз оцінювалась на основі аналізу статистичних даних, типових сценаріїв атак та особливостей функціонування ІКС.

Загрози класифіковані за типом інформації якій вони загрожують: конфіденційна, технологічна та відкрита. Так, як критичність захисту конфіденційності, доступності та цілісності для різних типів інформації різна, то вагові коефіцієнти цих параметрів були визначені окремо для кожного типу та розраховані за методом AHP аналогічно до розрахунку важливості коефіцієнтів в моделі порушника (Таблиця 3.4). Матриці попарних порівнянь для кожного типу інформації представлені в Додатку С.

Загальна формула розрахунку оцінки ризику:

$$R = P(\omega_c C + \omega_I I + \omega_A A), \tag{3.2}$$

де R— підсумковий ризик, P— ймовірність реалізації загрози, C,I,A— експертні оцінки впливу загрози на конфіденційність, цілісність, доступність, ω_C, ω_I, ω_A, — вагові коефіцієнти, отримані методом AHP.

Таблиця 3.4

Вагові коефіцієнти для параметрів конфіденційності, цілісності та доступності в залежності від типу інформації.

Тип інформації	ω_C	ω_I	ω_A
Конфіденційна	0,5	0,3	0,2
Технологічна	0,2	0,4	0,4
Відкрита	0,2	0,3	0,5

Крім того, для кожної загрози був встановлений зв'язок із потенційними порушниками. Також вказано, які загрози можуть виникати внаслідок зовнішніх випадкових подій.

Повний список загроз з оцінкою ризику та потенційними порушниками наведено в таблиці у Додатку В.

3.4. Аналіз результатів та формування вимог та рекомендацій до КЗЗ ІКС

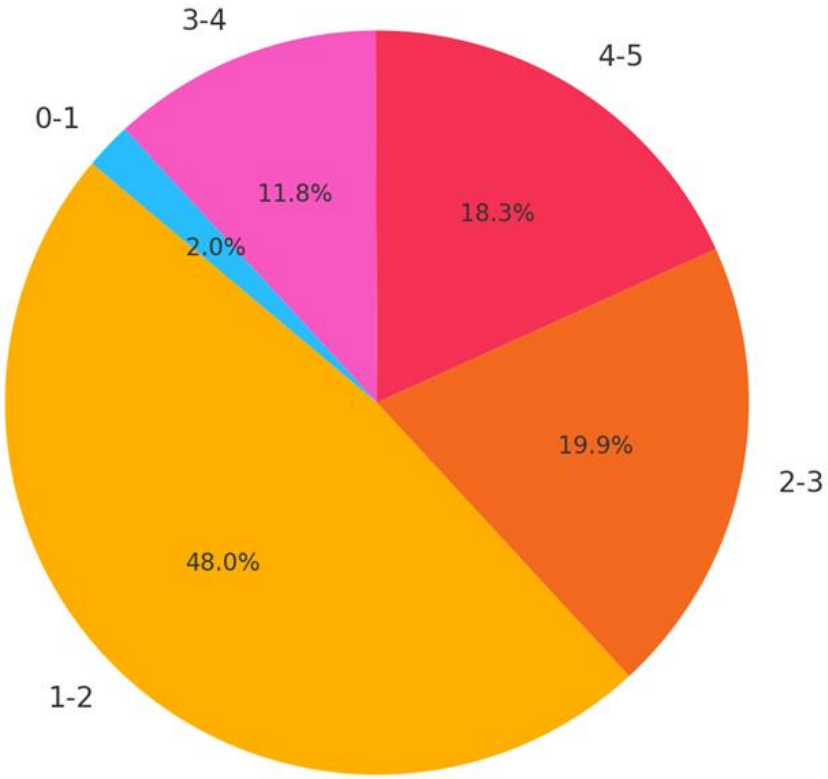
3.4.1. Графічний аналіз результатів

З метою візуалізації результатів оцінки ризиків були побудовані аналітичні графіки, що дозволяють оцінити загальну ситуацію щодо безпеки інформаційної системи веб-сайту УЦОЯО.

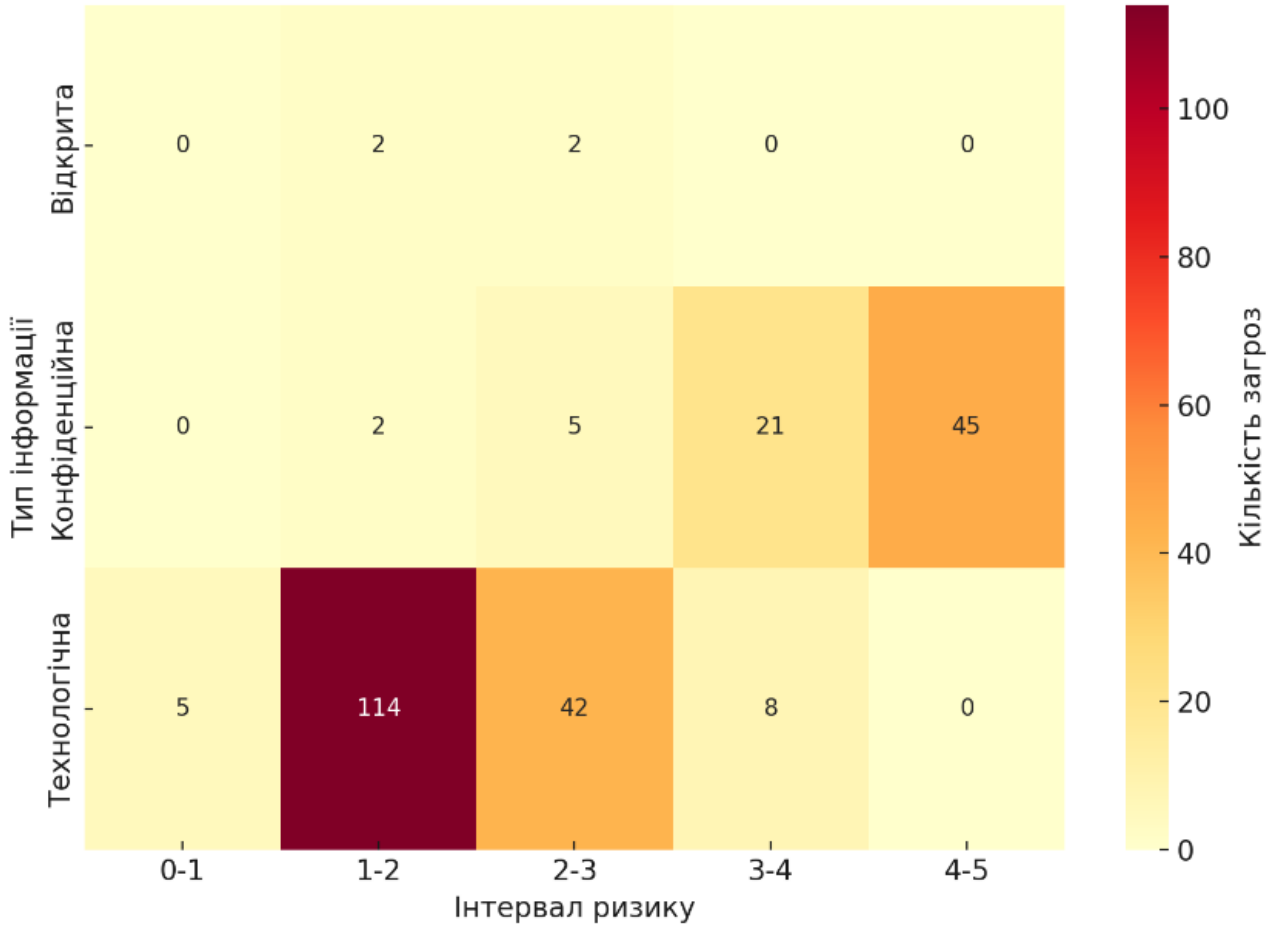
На рисунку 3.1 (а) зображено розподіл загроз за інтервалами ризику. Найбільша кількість загроз (48%) має низьку оцінку ризику в інтервалі 1-2, проте значна частина загроз зосереджена в інтервалах з оцінкою ризику 3-4 (11.8%) та 4-5 (18.3%) що вимагає посиленої уваги та реалізації заходів захисту.

На рисунку 3.1 (б) наведена теплова карта, яка демонструє співвідношення між типами інформації та інтервалами ризику загроз. Це дозволяє ідентифікувати найбільш критичні зони загроз. Найбільша концентрація загроз із низьким ризиком

спостерігається для технологічної інформації. Це пояснюється тим що технологічні процеси здебільшого автоматизовані та мають вбудовані захисні механізми. Конфіденційна інформація має найбільшу концентрацію загроз з оцінкою ризику в інтервалі 4-5, що говорить про потребу посилення заходів захисту для персональних даних та інформації обмеженого доступу. Відкрита інформація має найменше загроз, і всі вони зосереджені у нижчих інтервалах ризику.



А

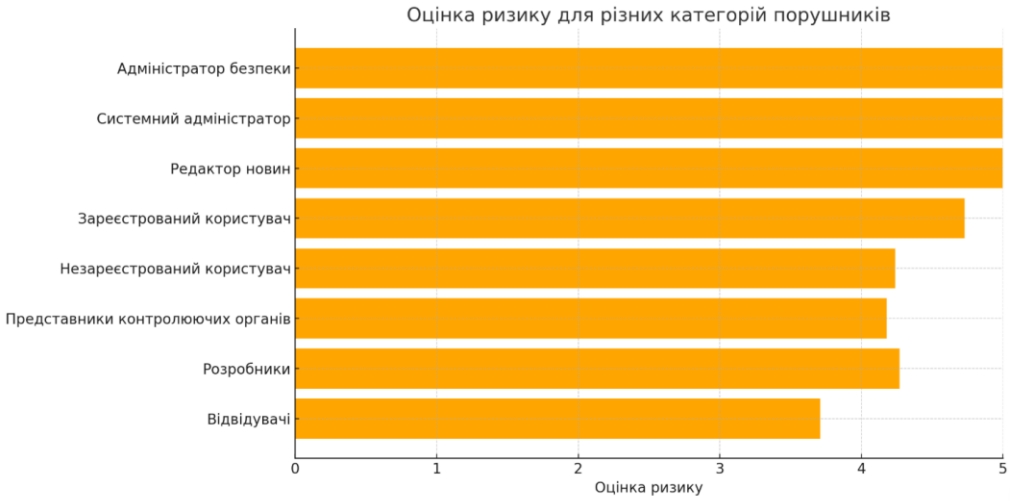


Б

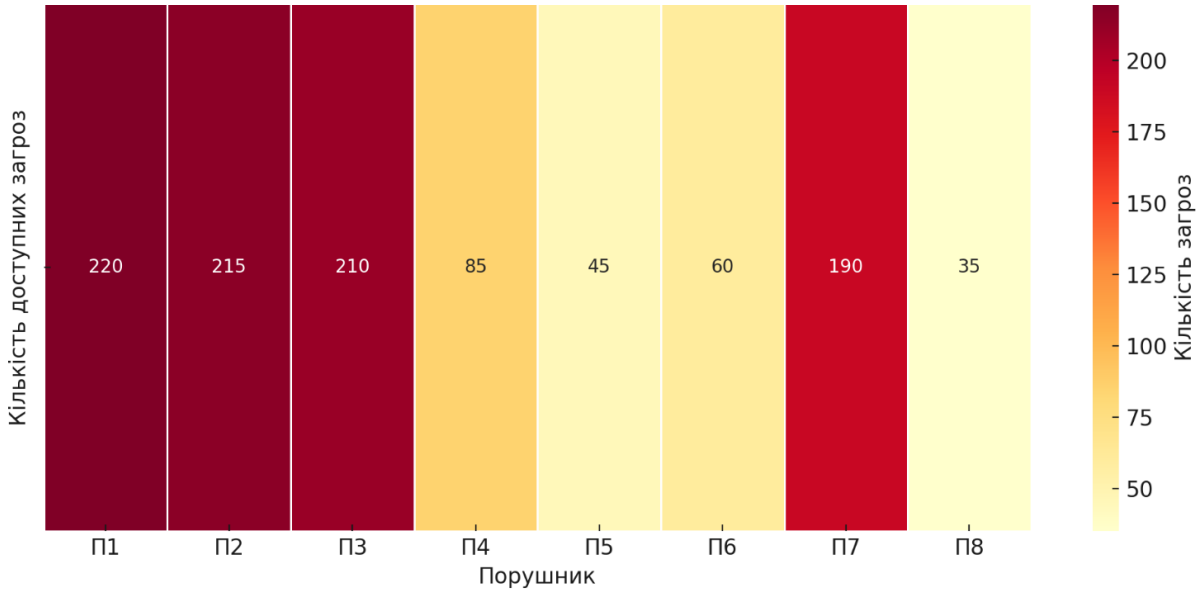
Рис. 3.1 Діаграма розподілу загроз за рівнями ризику (А) Теплова карта розподілу загроз за типом інформації та рівнем ризику (Б)

Також були побудовані окремі графіки на основі моделі порушників. Рисунок 3.2 (А) демонструє рівень ризику, що асоціюється з кожним типом порушника. Порушники П1-П3 (адміністратор безпеки, системний адміністратор, редактор новин) мають найвищі показники ризику, це пов’язано з їхнім високим рівнем доступу до ресурсів ІКС та глибокими знаннями системи. Порівняно низький рівень ризику у П8 (відвідувачі) обумовлений відсутністю авторизованого доступу та обмеженими можливостями.

На рисунку 3.2 (Б) зображена теплова карта доступності загроз для різних категорій порушників. Найбільше доступних загроз у категорій із найвищим рівнем ризику (П1-П3), що є очікуваним, найменше загроз доступно для реалізації незареєстрованому користувачу (П5).



А



Б

Рис. 3.2 Діаграма оцінки ризику для різних категорій порушників (А) Теплова карта доступних загроз для різних категорій порушників (Б)

Результати графічного аналізу дозволяють дійти таких висновків:

1. Найбільш критичними є загрози конфіденційної інформації. Вони повинні стати пріоритетною метою впровадження додаткових заходів безпеки.

2. Найбільшу небезпеку для системи становлять адміністратори та розробники, їм треба приділяти основну уваги при розробці організаційних заходів захисту та контролю повноважень.

3. Значна кількість загроз має ризик на рівні 3–5, тому поточний рівень захисту в ІКС ВЕБ САЙТ потребує зміцнення.

В цілому, отримані результати дозволяють здійснити обґрунтовану оцінку поточного стану безпеки та надають чітку основу для формування вимог до комплексної системи захисту ІКС ВЕБ САЙТ УЦОЯО.

3.4.2. Формування вимог до КЗЗ для ІКС ВЕБ САЙТ УЦОЯО

На основі проведеного аналізу інформаційної системи та оцінки ризиків інформаційної безпеки було сформовано вимоги до комплексів засобів захисту інформації (КЗЗ) для ІКС ВЕБ САЙТ УЦОЯО. При формуванні вимог враховувалися характеристики системи, її структурні компоненти, типи загроз, оцінки ризику, наявні заходи безпеки, а також чинні нормативні документи (ISO/IEC 27005:2018, НД ТЗІ 2.5-010-03, тощо).

Формування вимог до КЗЗ здійснювалося на основі низки ключових принципів, що забезпечують ефективність, актуальність та відповідність нормативним вимогам. Передусім першочергова увага приділялась загрозам із найвищою оцінкою ризику (>4), це дозволяє фокусуватися на найбільш критичних вразливостях системи. Кожна з вимог пов’язана із конкретною загрозою або групою загроз, реалізація якої дозволить зменшити ризики. Також враховується узгодженість вимог з вже впровадженими заходами захисту (наприклад, FortiGate 60E, Barrier-301). Рекомендовані заходи захисту охоплюють апаратні, програмні, організаційні та процедурні компоненти. Всі засоби, що передбачаються до

впровадження в рамках КЗЗ, повинні бути сертифікованими відповідно до чинного законодавства України, що гарантує їх офіційну відповідність вимогам безпеки.

Апаратні засоби захисту:

- Встановити міжмережеві екрани із DPI-функціоналом (Deep Packet Inspection) для контролю мережевого трафіку на периметрі системи.
- Інтегрувати засоби інтелектуального виявлення вторгнень (IDS/IPS) на рівні сегментів внутрішньої мережі.
- Забезпечити ізольоване розміщення серверів БД з логічною та фізичною сегментацією.
- Забезпечити джерела безперебійного живлення для серверного обладнання і критично важливих вузлів обробки інформації.

Програмні засоби:

- Оновити та централізувати засоби антивірусного захисту (ESET Server Security, Suricata).
- Впровадити систему моніторингу безпеки (SIEM) для виявлення інцидентів у реальному часі.
- Налаштувати контроль цілісності системних файлів і конфігураційних даних за допомогою audit-libs.
- Використовувати VPN/SSH із криптографічним захистом (наприклад ІІТ Захист з’єднань 2) для адміністративного доступу.

Організаційні заходи:

- Розробити та впровадити регламент безпечної роботи з ІКС та персональними даними.
- Переглянути політику паролів: мінімальна довжина, складність, ротація, блокування при переборі.
- Впровадити процедури навчання персоналу із соціальної інженерії та політик доступу.
- Регулярно проводити аудит безпеки конфігурацій та журналів подій.

Процедури управління ризиками:

- Визначити порогові значення ризику, що вимагають негайної реакції.
- Розробити процедури реагування на інциденти та тестування планів відновлення.
- Здійснювати щоквартальний перегляд оцінки ризиків з урахуванням змін в архітектурі ІКС.
- Забезпечити зберігання резервних копій відповідно до критичності інформації (3 рівні доступності).

ВИСНОВКИ

1. Проаналізовано архітектуру та особливості функціонування ІКС ВЕБ САЙТ УЦОЯО з урахуванням ролей користувачів та типів інформації, що обробляються в системі. Виділено три класи інформації (відкрита, технологічна, конфіденційна), для яких встановлено різні вимоги захисту. В результаті аналізу встановлено, що конфіденційна інформація є найбільш вразливою – на неї припадає понад 62% загроз із оцінкою ризику понад 4.0, що потребує пріоритетного захисту.
2. Побудовано модель загроз (247 загроз) та модель порушників (8 категорій),в яких проведено оцінку ефективного рівня загрози за критеріями впливу на конфіденційність, цілісність та доступність системи, а також поставлені оцінки вразливості та ймовірності реалізації загроз. Оцінювання здійснено на основі аналізу стандартів ISO/IEC 27005:2018, відомчих регламентів і типових інцидентів. У результаті моделювання найвищий ризик встановлено для адміністратора безпеки (R = 5.0), найнижчий — для випадкового відвідувача (R = 3.71).
3. Метод AHP дозволив формалізувати вагу критеріїв конфіденційності, цілісності та доступність залежно від типу інформації (наприклад, ωC=0.5 для конфіденційної інформації), що забезпечило адекватну агрегацію показників ризику. Така модель дозволила виконати повне ранжування загроз — понад 30% з них мають ризик понад 3.0, що свідчить про наявність критичних вразливостей та обмежену ефективність існуючих механізмів контролю.
4. Сформовано вимоги до КЗЗ, які охоплюють апаратні, програмні, організаційні та процедурні компоненти, з урахуванням реальної структури загроз і потенційних порушників. Особливу увагу приділено 41 загрозі з ризиком >4.0, з фокусом на посиленні контролю привілеїв, обмеженні доступу до конфіденційних ресурсів та впровадженні моніторингу безпеки відповідно до вимог ISO/IEC 27005.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шевченко С., Кравчук К., Жданова Ю. Information protection model based on information security risk assessment for small and medium-sized business // Cybersecurity Education Science Technique.
2. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). – Київ: ДП «УкрНДНЦ», 2013.
3. Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки // Моделі, методи та засоби захисту інформації в інформаційно-комунікаційних системах. – 2021.
4. Типове положення про службу захисту інформації в автоматизованій системі. – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 2000.
5. НД ТЗІ 1.1-002-99. Захист інформації. Терміни та визначення. – К.: Адміністрація Держспецзв'язку України, 1999.
6. Shevchenko H., Shevchenko Z., Zhdanova Y., Spasiteleva S., Negodenko O. Information Security Risk Analysis SWOT // Cybersecurity Education Science Technique.
7. Chang H.-H., Huang W.-C. Application of a quantification SWOT analytical method // Mathematical and Computer Modelling. – 2006.
8. Юдін О.Ю., Сидоренко В.М., Гнатюк С.О., Верховець О.С. Methods of information systems protection // Захист інформації. – 2021.
9. Хлапонін Ю.І. Комплексні системи захисту інформації. – Харків: ХНУРЕ, 2015.
10. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34.
11. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. – Geneva: International Organization for Standardization, 2018.

12. Stine J.F., Ross R. Guide for Conducting Risk Assessments (NIST SP 800-30 Rev.1). – Gaithersburg, MD: National Institute of Standards and Technology, 2012.

ДОДАТОК А

Таблиця Специфікація моделі порушника за мотивами здійснення порушень

Позначення	**Мотив порушення**	**Ефективний рівень загрози**
М1	Безвідповідальність (недбалість)	3
М2	Корисна цілеспрямованість	5

Таблиця Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС.

Позна-чення	**Основні кваліфікаційні ознаки порушника**	**Еф. рівень загрози**
К1	Не володіє знаннями та інформацією про порядок функціонування ІКС, не має навичок щодо користування штатними засобами системи.	1
К2	Має навики щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення та операційних систем, та практичними навичками роботи з засобами що реалізовані в ІКС.	4
К4	Володіє знаннями щодо функціонування засобів та механізмів захисту, що використовуються в ІКС та їх недоліки	5

Таблиця Специфікація моделі порушника за показником можливостей використання засобів ІКС для реалізації загроз

Позна-чення	**Характеристика можливостей порушника**	**Еф. рівень загрози**
З1	Має фізичний доступ до АРМ ІКС, але не є авторизованим користувачем ІКС	1
З2	Має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;	3
З3	Має можливість керування функціонуванням елементів ІКС, тобто конфігурує програмне забезпечення та КЗЗ ІКС	5
З4	Не має доступу фізичного доступу до ресурсів ІКС	1

Таблиця Специфікація моделі порушника за часом дії.

Позначення	**Характеристика можливостей порушника**	**Еф. рівень загрози**
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час).	4
Ч2	Під час функціонування ІКС	5

Ч3	Під час перерв у роботі для обслуговування та ремонту	3

Таблиця Специфікація моделі порушника за місцем дії.

Позна-чення	**Характеристика місця дії порушника**	**Еф. рівень загрози**
Д1	Усередині будівлі та приміщень, але без доступу до технічних засобів ІКС	1
Д2	З робочих місць користувачів	5
Д3	З інших об’єктів ІКС, в тому числі каналів зв’язку	2

ДОДАТОК В

Таблиця оцінки ризиків загроз

№	Загрози	Тип інформації	C	I	A	Вразливість	Ймовірність	Ризик	Заходи протидії	Порушники
1	Пожежа	Технологічна	3	3	4	Середня	0.3 (Низька)	0.93	Відповідно обладнане серверне приміщення Контроль функціонування	Випадкова подія
2	Забруднення, пил, корозія	Технологічна	2	3	3	Низька	0.3 (Низька)	0.82	Регулярне технічне обслуговування	Адміністратори Випадкова подія Обслуговуючий персонал
	Екологічні катастрофи	Технологічна	3	3	4	Середня	0.3 (Низька)	0.93	Відповідно обладнане серверне приміщення Інструктаж персоналу на випадок надзвичайної ситуації	Випадкова подія
4	Важливі події в навколишньому середовищі	Технологічна	2	3	3	Середня	0.3 (Низька)	0.82	Відповідно обладнане серверне приміщення Інструктаж персоналу на випадок надзвичайної ситуації	Випадкова подія
5	Відсутність або збій електропостачання	Технологічна	2	2	5	Середня	0.3 (Низька)	0.7	Відповідно обладнане серверне приміщення Наявність робочих джерел безперебійного живлення Виконання затверджених інструкцій Контроль за станом функціонування	Випадкова подія Стороння особа
6	Відмова або збій в роботі мережі живлення	Технологічна	2	2	5	Низька	0.6 (Середня)	1.39	Відповідно обладнане серверне приміщення	Випадкова подія Стороння особа

									Наявність робочих джерел безперебійного живлення	
7	Відмова або збій в роботі постачальників послуг	Технологічна	2	2	4	Низька	0.6 (Середня)	1.33	Наявність декількох операторів зв'язку	Випадкова подія Стороння особа
8	Відмова або збій мереж зв'язку	Технологічна	2	2	4	Середня	0.6 (Середня)	1.33	Контроль функціонування ПЗ моніторингу Наявність декількох операторів зв'язку	Адміністратори Випадкова подія Стороння особа
9	Перехоплення інформації / Шпигунство	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Розмежування прав доступу Реєстрація подій Періодичний інструктаж та контроль персоналу	Адміністратори Користувачі Обслуговуючий персонал Стороння особа
10	Викрадення пристроїв, носіїв інформації та документів	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Обмеження фізичного доступу до приміщень Періодичний інструктаж та контроль персоналу	Адміністратори Обслуговуючий персонал Стороння особа
11	Втрата пристроїв, носіїв інформації та документів	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Обмеження фізичного доступу до приміщень Заходи з організації безпечного зберігання та використання носіїв інформації Розмежування прав доступу Реєстрація подій	Адміністратори
12	Розголошення конфіденційної інформації	Конфіденційна	5	4	2	Середня	0.6 (Середня)	2.73	Розмежування прав доступу Реєстрація подій Періодичний інструктаж та	Адміністратори

									контроль персоналу	
13	Маніпуляція апаратним або програмним забезпеченням	Технологічна	4	5	2	Середня	0.6 (Середня)	2.65	Розмежування прав доступу Реєстрація подій Персональна відповідальність Періодичний інструктаж та контроль персоналу ПЗ антивірусного захисту ПЗ моніторингу	Адміністратори Обслуговуючий персонал Стороння особа
14	Маніпуляція інформацією	Конфіденційна	4	5	2	Середня	1.0 (Висока)	4.03	Розмежування прав доступу Реєстрація подій Персональна відповідальність Періодичний інструктаж та контроль персоналу	Адміністратори Обслуговуючий персонал Стороння особа
15	Несанкціонований доступ до ІТ-систем	Технологічна	5	5	2	Низька	0.6 (Середня)	2.81	Ідентифікація та автентифікація користувачів Сегментація мережі Розмежування прав доступу	Обслуговуючий персонал Стороння особа
16	Знищення пристроїв або носіїв інформації	Технологічна	4	4	2	Низька	0.6 (Середня)	2.27	Обмеження фізичного доступу до приміщень Заходи з організації безпечного зберігання та використання носіїв інформації	Адміністратори Стороння особа Випадкова подія
17	Відмова пристроїв або систем	Технологічна	3	4	3	Низька	0.6 (Середня)	2.18	Наявність у критичних частинах ІКС ВЕБ САЙТ дублювання компонентів	Адміністратори Випадкова подія

									та обладнання	
18	Несправність пристроїв або систем	Технологічна	3	3	3	Середня	0.6 (Середня)	1.8	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Реєстрація подій ПЗ моніторингу	Адміністратори
19	Відсутність ресурсів	Технологічна	2	3	3	Середня	0.6 (Середня)	1.64	Виконання затверджений інструкцій Контроль функціонування Коректна робота системного та функціонального ПЗ Періодичне тестування навантажень	Адміністратори
20	Уразливості або помилки програмного забезпечення	Технологічна	3	4	2	Низька	0.6 (Середня)	2.12	Тестування вебдодатків та БД (виконання необхідних випробувань при розробці) Розробка спеціального ПЗ відповідно до сучасних тенденцій Використання ліцензійного ПЗ Використання ПЗ, рекомендованого Адміністрацією Держспецзв'язку ПЗ антивірусного захисту Розмежування прав доступу	Випадкова подія
21	Порушення	Конфіденційн	3	2	2	Середня	1.0 (Висока)	2.72	Персональна	Адміністратор

	законів або правил	а							відповідальність Виконання затверджений інструкцій Контроль функціонування	и Користувачі Обслуговуючий персонал Стороння особа
22	Несанкціоноване використання або адміністрування пристроїв та систем	Технологічна	4	3	2	Середня	0.6 (Середня)	1.89	Ідентифікація та автентифікація користувачів Розмежування прав доступу Реєстрація подій	Адміністратори Користувачі Обслуговуючий персонал Стороння особа
23	Неправильне використання або адміністрування пристроїв та систем	Технологічна	3	4	3	Середня	0.6 (Середня)	2.18	Виконання затверджений інструкцій Розмежування прав доступу Реєстрація подій Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Кваліфікований персонал	Адміністратори
24	Зловживання повноваженнями	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Персональна відповідальність Реєстрація подій Періодичний інструктаж та контроль персоналу	Адміністратори Користувачі Обслуговуючий персонал Стороння особа Обслуговуючий персонал
25	Викрадення особистості	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Інструктаж персоналу Заходи фізичної охорони	Випадкова подія
26	Напад	Конфіденційна	3	2	3	Середня	1.0 (Висока)	2.81	Інструктаж персоналу Заходи фізичної охорони	Випадкова подія
27	Примус, здирництво або	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Персональна відповідальні	Адміністратори Користувачі

	корупція								сть Реєстрація подій Періодичний інструктаж та контроль персоналу	Обслуговуючий персонал
28	Відмова від дій	Конфіденційна	2	3	2	Середня	1.0 (Висока)	2.19	Персональна відповідальність Реєстрація подій Періодичний інструктаж та контроль персоналу	Адміністратори Користувачі Обслуговуючий персонал
29	Зловживання персональними даними	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Персональна відповідальність Реєстрація подій Періодичний інструктаж та контроль персоналу	Адміністратори Користувачі Обслуговуючий персонал
30	Шкідливе програмне забезпечення	Технологічна	3	4	2	Середня	0.6 (Середня)	2.12	ПЗ антивірусного захисту Періодичний інструктаж та контроль персоналу	Стороння особа Випадкова подія
31	Відмова в обслуговуванні	Технологічна	2	3	5	Низька	0.6 (Середня)	1.77	Налаштування міжмережевого екрану Коректна робота системного та функціонального ПЗ Періодичне тестування навантажень Використання системи IPS/IDS Розробка спеціального ПЗ відповідно до сучасних тенденцій	Стороння особа Випадкова подія
32	Соціальна інженерія	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Реєстрація подій Періодичний інструктаж та контроль	Адміністратори Користувачі Обслуговуючий персонал Стороння

									персоналу Розмежування доступу Багаторівневий захист інформації (комплексний підхід)	особа
33	Повтор повідомлень	Технологічна	2	3	3	Середня	0.6 (Середня)	1.64	Реєстрація подій Періодичний інструктаж та контроль персоналу Розмежування доступу Багаторівневий захист інформації (комплексний підхід)	Адміністратори Користувачі Обслуговуючий персонал Стороння особа Випадкова подія
34	Втрата даних	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Резервне копіювання критичної інформації Розмежування прав доступу Реєстрація подій	Адміністратори Випадкова подія
35	Втрата цілісності конфіденційної інформації	Конфіденційна	5	5	2	Середня	1.0 (Висока)	4.75	Резервне копіювання критичної інформації Розмежування прав доступу Реєстрація подій	Адміністратори Випадкова подія
36	Втрата особистості	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Реєстрація подій Періодичний інструктаж та контроль персоналу Розмежування доступу Багаторівневий захист інформації (комплексний підхід)	Адміністратори Користувачі Обслуговуючий персонал Стороння особа Випадкова подія
37	Відмова IT-системи	Технологічна	3	3	5	Середня	0.6 (Середня)	1.93	Резервне копіювання критичної інформації Можливість відновлення	Адміністратори Випадкова подія

									налаштувань на певний момент часу ПЗ моніторингу Наявність кластерів та задубльованих компонентів Контроль функціонування	
38	Займання кабелів	Технологічна	2	3	4	Середня	0.6 (Середня)	1.71	Відповідно обладнане серверне приміщення Контроль функціонування	Випадкова подія
39	Неприйнятна температура та вологість	Технологічна	2	3	3	Середня	0.6 (Середня)	1.64	Відповідно обладнане серверне приміщення Контроль функціонування Регулярне технічне обслуговування	Випадкова подія
40	Відмова глобальної мережі	Технологічна	2	2	4	Низька	0.6 (Середня)	1.33	Використання двох провайдерів послуг	Випадкова подія
41	Наслідки катастроф в навколишньому середовищі	Технологічна	3	3	4	Низька	0.6 (Середня)	1.86	Дотримання інструкцій	Випадкова подія
42	Проблеми, викликані великими публічними подіями	Технологічна	2	2	3	Низька	0.6 (Середня)	1.26	Дотримання інструкцій	Випадкова подія
43	Відмова патч-панелей через пожежу	Технологічна	3	3	4	Середня	0.6 (Середня)	1.86	Контроль функціонування Наявність резервного обладнання Регулярне технічне обслуговування	Випадкова подія
44	Відмова постачальника послуг	Технологічна	2	2	4	Низька	0.6 (Середня)	1.33	Використання двох провайдерів послуг	Випадкова подія Стороння особа
45	Відсутність,	Технологічна	2	3	4	Середня	0.6 (Середня)	1.71	Коректна	Адміністратор

	неналежність, несумісність ресурсів								робота системного та функціонального ПЗ Контроль функціонування Виконання затверджених інструкцій	и
46	Недостатній контроль гарантій безпеки	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	СА (АБ)
47	Неконтрольоване використання ресурсів	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Ідентифікація та аутентифікація користувачів Розмежування прав доступу Реєстрація подій Контроль за станом функціонування	Адміністратори
48	Погана адаптація до змін у використанні ІТ	Технологічна	2	2	3	Низька	0.6 (Середня)	1.26	Заходи з організації ремонту та модернізації Інструкції користувачам та адміністраторам	Адміністратори
49	Носії даних не доступні у випадку необхідності	Технологічна	2	3	3	Низька	0.6 (Середня)	1.64	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори
50	Неналежне керування ключами шифрування	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Виконання затверджених інструкцій Реєстрація подій	Адміністратори
51	Відсутня або недостатня	Конфіденційна	2	2	2	Низька	1.0 (Висока)	2.0	Виконання затверджених	Адміністратори

	оцінка даних аудиту								інструкцій Кваліфікований персонал	
52	Втрата конфіденційності чутливої інформації захищеної мережі	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Виконання затверджених інструкцій Розмежування прав доступу Реєстрація подій Контроль за станом функціонування	Адміністратори
53	Несанкціоноване використання прав	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Ідентифікація та аутентифікація користувачів Розмежування прав доступу Реєстрація подій	Адміністратори
54	Порушення авторських прав	Конфіденційна	2	2	2	Низька	1.0 (Висока)	2.0	Виконання затверджених інструкцій Централізоване придбання обладнання та ПЗ	Адміністратори Користувачі
55	Тестування програмного забезпечення з використанням виробничих даних	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Виконання затверджених інструкцій	Адміністратори
56	Неналежна пропускна здатність лінії	Технологічна	2	2	3	Середня	0.6 (Середня)	1.26	Виконання затверджених інструкцій Розмежування прав доступу Реєстрація подій Контроль за станом функціонування	Випадкова подія
57	Неприпустиме обмеження	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених	Адміністратори

	середовища користувача								інструкцій	
58	Відсутність, або неналежне, впровадження механізмів забезпечення безпеки БД	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених інструкцій Кваліфікований персонал Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ Контроль та тестування налаштувань	Адміністратори
59	Складність СКБД	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ	СА (АБ)
60	Складність доступу до БД	Технологічна	2	3	2	Середня	0.6 (Середня)	1.58	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	СА (АБ)
61	Погана організація обміну користувачів БД	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
62	Незахищене переміщення файлів і носіїв даних	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори Користувачі

63	Втрата конфіденційності через приховані фрагменти даних	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори Користувачі Обслуговуючий персонал Стороння особа Випадкова подія
64	Неналежне зберігання носіїв інформації в разі виникнення надзвичайної ситуації	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Сегментація мережі Обмеження фізичного доступу до приміщень	Адміністратори
65	Експлуатація незареєстрованих компонентів	Технологічна	3	4	2	Середня	1.0 (Висока)	3.53	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за станом функціонування	Адміністратори Обслуговуючий персонал Стороння особа
66	Концепція для мережної системи та системи управління не впроваджена або недостатня	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	Адміністратори
67	Несанкціонований збір даних, пов'язаних з фізичними особами	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Адміністратори Користувачі Обслуговуючий персонал Стороння особа
68	Невідповідне поводження з інцидентами безпеки	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Виконання затверджених інструкцій Контроль за станом функціонування Реєстрація подій Розмежуванн	СА (АБ)

									я доступу Періодичний інструктаж та контроль персоналу	
69	Неправильне адміністрування прав доступу до сайту та даних	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори
70	Неналежне переміщення архівних систем	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Адміністратори
71	Неадекватне управління безпекою	Технологічна	2	3	2	Низька	0.6 (Середня)	1.58	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	СА (АБ)
72	Неналежний журнал аудиту архівних систем	Технологічна	2	3	2	Низька	0.6 (Середня)	1.58	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
73	Неадекватні ключі індексування для архівів	Технологічна	2	2	2	Низька	1.0 (Висока)	2.0	Кваліфікований персонал	Адміністратори
74	Недостатня документація щодо доступу до архіву	Технологічна	2	3	2	Середня	0.6 (Середня)	1.58	Контроль за станом функціонування Періодичне тестування архівних копій	Адміністратори
75	Неефективне відновлення даних при архівації	Технологічна	2	3	2	Низька	0.6 (Середня)	1.58	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Адміністратори
76	Неефективне відновлення цифрових	Технологічна	2	3	2	Низька	0.6 (Середня)	1.58	Виконання затверджених інструкцій	Адміністратори Користувачі

	підписів при архівації								Впровадження автоматизованих методів архівування	
77	Неефективний аудит процедур архівування	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	СА (АБ)
78	Погане планування розташування архівної системи	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Адміністратори
79	Використання небезпечних протоколів в мережах загального користування	Відкрита	3	2	2	Середня	1.0 (Висока)	2.09	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
80	Застаріла або некоректна інформація на вебсайті	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій	Редактор новин
81	Неналежне планування на випадок надзвичайних ситуацій	Технологічна	2	3	2	Середня	1.0 (Висока)	2.63	Кваліфікований персонал Виконання затверджених інструкцій Зовнішній аудит	СА (АБ)
82	Неекономічне використання ресурсів в результаті неадекватного управління безпекою	Технологічна	2	3	2	Середня	0.6 (Середня)	1.58	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Адміністратори
83	Недостатня ємність архівних носіїв	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій	Адміністратори
84	Порушення нормативних положень та договірних угод	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Резервне копіювання критичної інформації Можливість	Адміністратори Користувачі Обслуговуючий персонал Стороння

									відновлення налаштувань на певний момент часу Заходи з контролю функціонування	особа
85	Порушення бізнес-процесів в результаті інцидентів з безпекою	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори Користувачі Обслуговуючий персонал
86	Відсутнє або недостатнє планування системи зберігання даних	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Адміністратори
87	Неналежна організація оновлення та перенесення БД	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Резервне копіювання критичної інформації	СА (АБ)
88	Неадекватне планування методів резервного копіювання даних для контролерів домену	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
89	Недостатній аналіз бізнес-процесів при керуванні виправленнями та змінами	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
90	Недостатньо ресурсів для керування виправленнями та змінами	Технологічна	2	3	2	Середня	0.6 (Середня)	1.58	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	Адміністратори

91	Погана комунікація при керуванні виправленнями та змінами	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
92	Невиявлені інциденти інформаційної безпеки	Технологічна	2	3	2	Середня	1.0 (Висока)	2.63	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
93	Відсутність або неадекватне планування використання DNS	Відкрита	3	3	2	Низька	0.6 (Середня)	1.62	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори
94	Поганий вибір або концепція вебдодатків	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Сегментація мережі Обмеження фізичного доступу до приміщень	Адміністратори
95	Відсутнє або недостатнє уникання даних від сторонніх осіб при обробці персональних даних	Відкрита	3	3	2	Середня	1.0 (Висока)	2.7	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за станом функціонування	Адміністратори Користувачі Обслуговуючий персонал Стороння особа
96	Недоліки в розробці і розширенні вебдодатків	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	Адміністратори
97	Неадекватний захист персональних	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій	Адміністратори

	даних у вебдодатках								Кваліфікований персонал Періодичні курси підвищення кваліфікації	
98	Відсутність або недостатній аудит інцидентів інформаційної безпеки	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених інструкцій Контроль за станом функціонування Реєстрація подій Розмежування доступу Періодичний інструктаж та контроль персоналу	Адміністратори
99	Втрата конфіденційності та цілісності зареєстрованих даних аудиту	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори Випадкова подія
100	Порушення обмеженого використання персональних даних при їх обробці	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	
101	Відсутність дозволів для обробки персональних даних	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
102	Порушення принципу необхідності при обробці персональних даних	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
103	Порушення конфіденційності при обробці персональних даних	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Кваліфікований персонал	Адміністратори
104	Відсутня або неналежна	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Контроль за станом	Адміністратори

	попередня перевірка								функціонування Періодичне тестування архівних копій	
105	Порушення прав зацікавлених осіб при обробці персональних даних	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Адміністратори
106	Відсутній або неналежний захист персональних даних при обробці даних за замовленням	Конфіденційна	4	4	2	Низька	1.0 (Висока)	3.83	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
107	Відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист даних	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
108	Погіршення заданих цілей контролю при обробці персональних даних	Конфіденційна	5	3	2	Низька	1.0 (Висока)	4.36	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Адміністратори
109	Відсутній або неналежний захист при обробці персональних даних за кордоном	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
110	Неприйнятні автоматизовані рішення для окремих випадків або результати обробки персональних даних	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори
11	Відсутній або	Конфіденційн	4	3	2	Середня	1.0 (Висока)	3.64	Кваліфікован	Адміністратор

1	недостатній контроль захисту даних	а							ий персонал Виконання затверджених інструкцій Зовнішній аудит	и
112	Втрата конфіденційності даних або цілісності в результаті помилки користувача	Технологічна	2	2	2	Середня	0.6 (Середня)	1.2	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Користувачі Випадкова подія
113	Необережне знищення обладнання або даних	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій	Адміністратори Обслуговуючий персонал
114	Недотримання правил IT-безпеки	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Заходи з контролю функціонування	Адміністратори Користувачі
115	Несанкціоноване підключення кабелів	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори
116	Ненавмисне пошкодження кабелів	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
117	Неправильне використання IT-системи	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Резервне копіювання критичної інформації	Адміністратори
118	Неправильне адміністрування IT-систем	Технологічна	2	2	2	Середня	0.6 (Середня)	1.2	Виконання затверджених інструкцій Зовнішній	Адміністратори

									аудит	
119	Неправильний експорт файлових систем під UNIX	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	Адміністратори
120	Передача помилкової або внутрішньої інформації	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
121	Неправильне адміністрування прав доступу до сайту і даних	Конфіденційна	5	3	2	Середня	1.0 (Висока)	4.36	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
122	Неправильне внесення змін до реєстру	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори
123	Неправильне керування СКБД	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Виконання затверджених інструкцій Сегментація мережі Обмеження фізичного доступу до приміщень	Адміністратори
124	Недбала обробка даних	Технологічна	3	2	2	Середня	1.0 (Висока)	2.26	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за	Адміністратори

									станом функціонування	
125	Неправильна синхронізація часу	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	Адміністратори
126	Неправильна конфігурація активних мережних компонентів	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Адміністратори
127	Відсутня або невідповідна сегментація	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених інструкцій Контроль за станом функціонування Реєстрація подій Розмежування доступу Періодичний інструктаж та контроль персоналу	Адміністратори
128	Порушення основних правових умов використання криптографічних перетворень	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори Сторонні особи
129	Неправильне використання криптомодулів	Технологічна	2	2	2	Низька	1.0 (Висока)	2.0	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Адміністратори
130	Відключення сервера під час роботи	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Обслуговуючий персонал
13	Невірне	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання	СА (АБ)

1	тлумачення події інформаційної безпеки								затверджених інструкцій Впровадження автоматизованих методів архівування	
132	Непродуктивні пошуки	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Кваліфікований персонал	Адміністратори
133	Помилки в конфігурації і роботі	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Контроль за станом функціонування Періодичне тестування архівних копій	Адміністратори
134	Неправильне поводження з паролями	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Адміністратори Користувачі
135	Недбалість в обробці інформації	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Користувачі
136	Порушення вимог законодавства щодо використання архівних систем	Технологічна	3	2	2	Низька	0.6 (Середня)	1.36	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
137	Неправильне налаштування маршрутизаторів та комутаторів	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Адміністратори
138	Неправильне адміністрування маршрутизаторів та комутаторів	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання	Адміністратори

									системи	
139	Недостатнє прийняття інформаційної безпеки	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій	Адміністратори
140	Відкриті кабелі	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Кваліфікований персонал Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
141	Помилки при синхронізації БД	Технологічна	3	2	2	Середня	0.6 (Середня)	1.36	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Адміністратори
142	Погіршення протипожежного захисту	Конфіденційна	5	3	2	Низька	1.0 (Висока)	4.36	Виконання затверджених інструкцій	Адміністратори Обслуговуючий персонал Випадкова подія
143	Помилки при передачі прав доступу	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Заходи з контролю функціонування	Адміністратори
144	Недооцінення актуальності виправлень і змін	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори
145	Неправильне налаштування DNS-сервера	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Адміністратори
146	Несанкціоноване використання	Конфіденційна	3	2	2	Низька	1.0 (Висока)	2.72	Виконання затверджених	Адміністратори

	зовнішніх послуг								інструкцій Резервне копіювання критичної інформації	
147	Неналежна поведінка при використанні Інтернету	Технологічна	2	2	2	Середня	0.6 (Середня)	1.2	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
148	Невірна інформація про домен	Відкрита	3	2	2	Середня	0.6 (Середня)	1.25	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
149	Пошкодження репутації	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
150	Неправильне адміністрування аудиту	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
151	Неправильний вибір відповідних даних аудиту	Технологічна	2	2	2	Середня	1.0 (Висока)	2.0	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
152	Відсутність синхронізації часу під час аналізу даних аудиту	Технологічна	2	3	2	Низька	0.6 (Середня)	1.58	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори
153	Збій електропостачання	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Сегментація мережі Обмеження	Випадкова подія

									фізичного доступу до приміщень	
154	Відмова внутрішніх мереж	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за станом функціонування	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
155	Відмова існуючих пристроїв безпеки	Технологічна	2	2	2	Середня	1.0 (Висока)	2.0	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
156	Перехресні перешкоди	Технологічна	2	2	2	Низька	1.0 (Висока)	2.0	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Випадкова подія
157	Погіршення характеристик ліній через фактори навколишнього середовища	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Контроль за станом функціонування Реєстрація подій Розмежування доступу Періодичний інструктаж та контроль персоналу	Випадкова подія
158	Дефектні носії даних	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
15	Втрата даних,	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання	Адміністратор

9	що зберігаються								затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	и Випадкова подія
160	Перевантажені інформаційні системи	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Випадкова подія
161	Уразливості або помилки у програмному забезпеченні	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Випадкова подія
162	Автоматичне розпізнавання з'ємних носіїв даних	Технологічна	4	4	2	Низька	1.0 (Висока)	3.79	Кваліфікований персонал	Адміністратори
163	Відмова БД	Технологічна	4	4	2	Середня	0.6 (Середня)	2.27	Контроль за станом функціонування Періодичне тестування архівних копій	Адміністратори Випадкова подія
164	Обхід контролю доступу через ODBC	Технологічна	4	4	2	Низька	0.6 (Середня)	2.27	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Адміністратори
165	Втрата даних в БД	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
166	Втрата цілісності/ несуперечності БД	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження	Адміністратори Випадкова подія

									автоматизованих методів архівування	
167	Відмова або несправність мережевого компонента	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
168	Неякісна або відсутня автентифікація	Технологічна	4	3	2	Середня	1.0 (Висока)	3.15	Дотримання інструкцій Персональна відповідальність Контроль використання системи	СА (АБ)
169	Відмова криптомодулю	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Випадкова подія
170	Нестійкі криптографічні алгоритми	Технологічна	4	3	2	Середня	1.0 (Висока)	3.15	Кваліфікований персонал Виконання затверджених інструкцій Зовнішній аудит	Випадкова подія
171	Помилки в зашифрованих даних	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Випадкова подія
172	Відмова компонентів системи управління мережею або системи управління системою	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
173	Помилки проектування програмного забезпечення	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Заходи з контролю	Випадкова подія

									функціонування	
174	Недокументовані функції	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Випадкова подія
175	Затримка доступу до архівної інформації	Технологічна	2	2	2	Низька	0.6 (Середня)	1.2	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Адміністратори Випадкова подія
176	Погана синхронізація індексних даних під час архівування	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Резервне копіювання критичної інформації	Адміністратори
177	Застаріння криптографічних методів	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Виконання затверджених інструкцій Зовнішній аудит	Випадкова подія
178	Небезпечні налаштування за замовчанням на маршрутизаторах і комутаторах	Технологічна	2	2	2	Середня	0.6 (Середня)	1.2	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
179	Запилені вентилятори	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	Адміністратори Обслуговуючий персонал
180	Проблеми при автоматизації поширення виправлень і змін	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
181	Неадекватна перевірка вхідних та вихідних даних	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальні	Адміністратори

	у вебпрограмах								сть Контроль використання системи	
182	Відсутність або погана обробка помилок вебпрограмами	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	Адміністратори
183	Неадекватне відстеження подій, пов'язаних з безпекою у вебпрограмах	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Сегментація мережі Обмеження фізичного доступу до приміщень	СА (АБ)
184	Розголошення конфіденційної інформації в вебпрограмах	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за станом функціонування	Адміністратори
185	Відсутність або недостатнє оповіщення при виникненні інцидентів безпеки	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	СА (АБ)
186	Маніпуляція або руйнування обладнання чи деталей	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Адміністратори Обслуговуючий персонал Стороння особа Випадкова подія
187	Маніпуляція інформацією або програмним забезпеченням	Технологічна	2	2	2	Середня	1.0 (Висока)	2.0	Виконання затверджених інструкцій Контроль за станом функціонуван	Адміністратори

									ня Реєстрація подій Розмежування доступу Періодичний інструктаж та контроль персоналу	
188	Вандалізм	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Випадкова подія
189	Прослуховування лінії	Технологічна	4	3	2	Низька	1.0 (Висока)	3.15	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Випадкова подія
190	Несанкціоноване використання IT-систем	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Обслуговуючий персонал Стороння особа
191	Систематичний перебір паролів	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
192	Зловживання портами для віддаленого обслуговування	Технологічна	2	2	2	Низька	1.0 (Висока)	2.0	Кваліфікований персонал	Адміністратори
193	Загроза при виконанні технічного обслуговування / адміністрування	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.64	Контроль за станом функціонування Періодичне тестування архівних копій	Адміністратори
194	Зловживання правами користувачів	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Користувачі

195	Зловживання правами адміністратора	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
196	Троянський кінь	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори
197	Неправильне використання системи UNIX за допомогою UUCP	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Адміністратори Користувачі
198	IP-спуфінг	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Стороння особа
199	Зловживання маршрутизацією джерела	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Стороння особа
200	Зловживання протоколом ICMP	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Кваліфікований персонал Виконання затверджених інструкцій Зовнішній аудит	Стороння особа
201	Зловживання протоколами маршрутизації	Технологічна	2	2	2	Середня	0.6 (Середня)	1.2	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Стороння особа
202	Інструменти аналізу мережі	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори
203	Неправильне використання віддаленого	Технологічна	5	3	2	Низька	0.6 (Середня)	2.05	Резервне копіювання критичної	Адміністратори

	доступу до функцій управління маршрутизаторами								інформації Можливість відновлення налаштувань на певний момент часу Заходи з контролю функціонування	
204	Маніпуляція даними або програмним забезпеченням в системах БД	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори
205	Відмова від послуг в системі БД	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Адміністратори
206	Несанкціоноване підключення інформаційних систем до мережі	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Резервне копіювання критичної інформації	Адміністратори Обслуговуючий персонал Стороння особа
207	Неавторизоване виконання функцій керування мережею	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори Стороння особа
208	DNS-спуфінг	Технологічна	4	3	2	Середня	0.6 (Середня)	1.89	Виконання затверджених інструкцій Зовнішній аудит	Стороння особа
209	Несанкціоноване використання криптомодулів	Технологічна	3	3	2	Середня	0.6 (Середня)	1.74	Розробка спеціального ПЗ та налаштування СКБД відповідно НД та конкретних потреб ІКС ВЕБ САЙТ ПЗ моніторингу	Адміністратори Користувачі
210	Маніпуляції криптомодулем	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Дотримання інструкцій	Адміністратори

									Персональна відповідальність Контроль використання системи	Користувачі
211	Компрометація криптографічних ключів	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори Користувачі Стороння особа
212	Підробні сертифікати	Конфіденційна	4	5	2	Низька	1.0 (Висока)	4.03	Виконання затверджених інструкцій Наявність спеціально обладнаних місць для зберігання носіїв	СА (АБ) Адміністратори Користувач Обслуговуючий персонал Стороння особа Розробники / постачальники програмного і апаратного забезпечення
213	Втрата цілісності інформації, яка повинна бути захищена	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Виконання затверджених інструкцій Сегментація мережі Обмеження фізичного доступу до приміщень	Адміністратори
214	Маніпуляція параметрами керування	Технологічна	4	3	2	Середня	1.0 (Висока)	3.15	Виконання затверджених інструкцій Сегментація мережі Кваліфікований персонал Тестування навантажень в мережі Контроль за станом функціонування	Адміністратори
215	Web-спуфінг	Технологічна	4	3	2	Середня	1.0 (Висока)	3.15	Виконання затверджених інструкцій Періодичний інструктаж та контроль персоналу	Стороння особа
21	Зловживання	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання	Стороння

6	активним контентом								затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	особа
217	Перехоплення мережевого з’єднання	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Виконання затверджених інструкцій Контроль за станом функціонування Реєстрація подій Розмежування доступу Періодичний інструктаж та контроль персоналу	Стороння особа
218	Несанкціонований запис або видалення файлів архівування	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій	Адміністратори
219	Web-"закладки"	Технологічна	3	3	2	Низька	1.0 (Висока)	2.89	Виконання затверджених інструкцій Кваліфікований персонал Періодичні курси підвищення кваліфікації	Стороння особа
220	Маніпуляція ARP-таблицями	Технологічна	3	3	2	Низька	0.6 (Середня)	1.74	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Стороння особа
221	MAC-спуфінг	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Стороння особа
222	Несанкціоноване фотографування та фільмування портативними	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Кваліфікований персонал	Адміністратори Обслуговуючий персонал Стороння

	пристроями									особа
223	SQL-ін'єкція	Технологічна	4	4	2	Середня	0.6 (Середня)	2.27	Контроль за станом функціонування Періодичне тестування архівних копій	Стороння особа
224	Несанкціоноване використання вебінструментів адміністрування	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Періодичне тестування архівних копій Впровадження автоматизованих методів архівування	Адміністратори
225	SPIT та фішинг	Технологічна	5	4	2	Низька	0.6 (Середня)	2.43	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Стороння особа
226	Атака "Людина посередині"	Технологічна	4	3	2	Низька	0.6 (Середня)	1.89	Виконання затверджених інструкцій Впровадження автоматизованих методів архівування	Адміністратори Користувачі Стороння особа
227	Компрометація служб каталогів через НСД	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Налаштування міжмережевого екрану Сегментація мережі Виконання затверджених інструкцій	Стороння особа
228	Втрата конфіденційності через файли підкачки	Технологічна	3	3	2	Середня	1.0 (Висока)	2.89	Дотримання інструкцій Персональна відповідальність Контроль використання системи	Адміністратори
229	DNS-флудінг	Технологічна	4	4	2	Низька	0.6 (Середня)	2.27	Виконання затверджених інструкцій	Стороння особа
230	DNS-захоплення	Технологічна	4	4	2	Середня	1.0 (Висока)	3.79	Кваліфікований персонал Виконання затверджених	Стороння особа

									інструкцій Зовнішній аудит	
231	Посилення DNS-атаки	Технологічна	4	4	2	Середня	0.6 (Середня)	2.27	Виконання затверджених інструкцій ПЗ моніторингу Контроль за станом функціонування	Сторонняособа
232	Витоки інформації DNS	Технологічна	4	4	2	Низька	0.6 (Середня)	2.27	Виконання затверджених інструкцій	Адміністратори
233	Використання динамічних оновлень DNS	Конфіденційна	5	3	2	Низька	1.0 (Висока)	4.36	Резервне копіювання критичної інформації Можливість відновлення налаштувань на певний момент часу Заходи з контролю функціонування	Сторонняособа
234	Бот мережі	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій	Сторонняособа
235	Фішинг та фармінг	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Заходи з контролю функціонування Впровадження автоматизованих методів архівування	Сторонняособа
236	Несанкціонований доступ до даних для вебпрограм або їх обробка	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Резервне копіювання критичної інформації	Адміністратори
237	Неправильне використання вебдодатка через автоматичне використання	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених інструкцій Зовнішній аудит	Адміністратори
238	Помилки в логіці	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Виконання затверджених	Адміністратори

	вебпрограм								інструкцій Зовнішній аудит	
239	Обхід функцій безпеки вебпрограми, реалізованих на стороні клієнта	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Налаштування міжмережевого екрану ПЗ антивірусного захисту Тестування вебдодатків та БД (виконання необхідних випробувань при розробці) Розробка спеціального ПЗ відповідно до сучасних тенденцій Зовнішній аудит	Адміністратори
240	XSS-атака	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Тестування вебдодатків та БД (виконання необхідних випробувань при розробці) Розробка спеціального ПЗ відповідно до сучасних тенденцій Контроль функціонування	Стороння особа
241	Неадекватне управління сесіями вебпрограм	Конфіденційна	5	4	2	Низька	1.0 (Висока)	4.56	Виконання затверджених інструкцій Налаштування міжмережевого екрану ПЗ антивірусного захисту Тестування вебдодатків та БД (виконання необхідних	Адміністратори

									випробувань при розробці) Розробка спеціального ПЗ відповідно до сучасних тенденцій Зовнішній аудит Шифрування даних	
242	Атака "Міжсайтова підробка запиту" (CSRF, XSRF, Session Riding)	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Шифрування даних Розмежування доступу Реєстрація подій Резервне копіювання критичної інформації	Стороння особа
243	Обхід авторизації в вебпрограмах	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Шифрування даних Розмежування доступу Реєстрація подій Тестування вебдодатків та БД Зовнішній аудит Резервне копіювання критичної інформації	Стороння особа
244	Інтеграція сторонніх даних та зловмисного коду в вебпрограму	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Шифрування даних Розмежування доступу Реєстрація подій Тестування вебдодатків та БД Зовнішній аудит Виконання затверджених інструкцій Резервне копіювання критичної інформації	Стороння особа
245	Ін'єкційні атаки	Конфіденційна	5	4	2	Середня	1.0 (Висока)	4.56	Шифрування даних Розмежування доступу	Стороння особа

									Реєстрація подій Тестування вебдодатків та БД	
246	Атака Clickjacking	Конфіденційна	4	3	2	Низька	1.0 (Висока)	3.64	Виконання затверджених інструкцій Налаштування міжмережевого екрану ПЗ антивірусного захисту	Стороння особа
247	Зловживання короткими URL-адресами та QR-кодами	Конфіденційна	4	3	2	Середня	1.0 (Висока)	3.3	Виконання затверджених інструкцій Налаштування міжмережевого екрану ПЗ антивірусного захисту	Стороння особа

Примітка:

Адміністратори – системний адміністратор (Адміністратор безпеки) (СА (АБ)), користувачі –користувачі автоматизованого місця.

ДОДАТОК С

Матриця порівнянь для конфіденційної інформації

Параметр	**Конфіденційність (C)**	**Цілісність (I)**	**Доступність (A)**
C	1	3	5
I	1/3	1	3
A	1/5	1/3	1

Матриця порівнянь для технологічної інформації

Параметр	**Конфіденційність (C)**	**Цілісність (I)**	**Доступність (A)**
C	1	1/3	1/5
I	3	1	1
A	5	1	1

Матриця порівнянь для відкритої інформації

Параметр	**Конфіденційність (C)**	**Цілісність (I)**	**Доступність (A)**
C	1	1/2	1/5
I	2	1	1/3
A	5	3	1