Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Метод оцінювання ризиків інформаційної безпеки для медичної установи»

Виконала: студентка 2 курсу, групи 1БС-20м
спеціальності 125 Кібербезпека
_____Ясінська Я. О.

Керівник: к. т. н., доц. каф. ЗІ
_____Куперштейн Л. М.
«___» _____ 2021 р.

Опонент:
к. т. н., доц., доц. каф. ОТ
_____Савицька Л. А.
«___» _____ 2021 р.

Допущено до захисту
Завідувач кафедри ЗІ, д.т.н., проф.
_____ Лужецький В.А.
«___» _____ 2021 р.

Вінниця ВНТУ – 2021 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійно програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д. т. н., проф.
_____В. А. Лужецький
_____ _____2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Ясінській Яні Олександрівні

1. Тема роботи: «Метод оцінювання ризиків інформаційної безпеки для медичної установи», керівник роботи: Куперштейн Леонід Михайлович, к. т. н., доцент, затверджені наказом ВНТУ від 9 вересня 2021 року №207.
2. Строк подання студентом роботи – 23 грудня 2021 р.
3. Вихідні дані до роботи:
   - тип медичної установа – міська клінічна лікарня;
   - стандарт ISO 27005;
   - перелік інформаційних ресурсів.
4. Зміст розрахунково-пояснювальної записки: Техніко-економічне та науково-технічне обґрунтування доцільності досліджень. Вступ. Аналіз методів та засобів оцінки ризиків інформаційної безпеки. Розробка методу оцінювання ризиків інформаційної безпеки. Розрахунок ризиків інформаційної безпеки медичної установи. Економічна частина. Висновки. Перелік використаних джерел. Додатки.
5. Перелік графічного матеріалу.

Загальна модель процесу оцінки ризиків інформаційної безпеки запропонованого методу (плакат, А4). Графічна формалізація першої стадії методу оцінювання ризиків ІБ (плакат, А4). Загальний вигляд логіко-ймовірнісної моделі для МКЛ (плакат, А4). Гілка «Конфіденційність» (плакат, А4). Гілка «Цілісність» (плакат, А4). Гілка «Доступність» (плакат, А4). Загальна схема зв'язків бази даних (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Куперштейн Л. М., доц. кафедри ЗІ		
2	Куперштейн Л. М., доц. кафедри ЗІ		
3	Куперштейн Л. М., доц. кафедри ЗІ		
4	Лесько О. Й., к. е. н., проф., зав. каф. ЕПВМ		

7. Дата видачі завдання – 9 вересня 2021 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	09.09.2021-13.09.2021	
2	Розробка технічного завдання	14.09.2021-16.09.2021	
3	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	17.09.2021-21.09.2021	
4	Розробка рішень	21.09.2021-27.09.2021	
5	Практична реалізація, моделювання, експериментування, результати	28.09.2021-18.10.2021	
6	Розробка розділу економічного обґрунтування доцільності розробки	19.10.2021-27.10.2021	
7	Аналіз виконання ТЗ, висновки	28.10.2021-01.11.2021	
8	Оформлення пояснювальної записки	02.11.2021-23.11.2021	
9	Попередній захист та доопрацювання МКР	24.11.2021-14.12.2021	
10	Перевірка магістерської роботи на наявність плагіату	14.12.2021-16.12.2021	
11	Представлення МКР до захисту, рецензування	16.12.2021-20.12.2021	
12	Захист МКР	21.12.2021-23.11.2021	

Студент_____Ясінська Я.О.

(підпис)

Керівник роботи_____Куперштейн Л.М.

(підпис)

АНОТАЦІЯ

УДК 004.056

Ясінська Я.О. Метод оцінювання ризиків інформаційної безпеки для медичної установи. Магістерська кваліфікаційна робота зі спеціальності 125 – кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2021. 92 с.

На укр. мові. Бібліогр.: 25 назв; рис.: 9; табл. 38.

Магістерська кваліфікаційна робота присвячена розробці методу оцінювання ризиків інформаційної безпеки для медичної установи. В рамках цієї роботи було проведено аналіз існуючих методів ризиків інформаційної безпеки. На основі існуючих методів було запропоновано вдосконалений комплексний підхід до оцінювання ризиків. Застосовано запропонований метод для медичної установи задля оцінки його ефективності.

Ілюстративна частина складається з 7 плакатів з демонстрацією результатів моделювання і проведених досліджень.

В економічному розділі здійснено оцінку витрат на розробку методу.

Ключові слова: інформаційна безпека, оцінка ризиків, ризик інформаційної безпеки, медицина.

ABSTRACT

Yasinska Y.O. Method of assessing information security risks for a medical institution. Master's thesis in the specialty 125 – cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2021. 92 p.

In Ukrainian. Bibliographer: 25 titles; fig .: 9; table. 38.

The master's qualification work is devoted to the development of a method for assessing information security risks for a medical institution. As part of this work, an analysis of existing methods of information security risks was conducted. Based on existing methods, an improved integrated approach to risk assessment has been proposed. The proposed method is used for a medical institution to assess its effectiveness.

The graphic part consists of 7 posters demonstrating the results of modeling and research.

In the economic section, the cost of developing the method is estimated.

Key words: information security, risk assessment, information security risk, medicine.

ЗМІСТ

ВСТУП

На сьогоднішній день інформаційна безпека (ІБ) відіграє все важливішу роль у діяльності будь-якої установи. Величезна кількість витоку даних, втрати доступу до інформаційних систем і т. д. відбувається по всьому світу і до того ж щодня. Медичні установи стають ще більш вразливими через перенесення великої частини роботи у цифровий простір. Тому **актуальним** способом забезпечення інформаційної безпеки є оцінка ризиків задля їх подальшого усунення або щонайменше зниження.

Досить значного поширення набуло оцінювання ризиків інформаційної безпеки за вимогами стандарту ISO 27005 . Даний метод враховує важливі фактори щодо ризиків ІБ, а саме: цінність актива, рівень вразливості, ймовірність реалізації загрози. Проте використання одного цього методу не допоможе визначити вплив загроз на напрями ІБ і на стан ІБ установи в цілому. Задля цієї потреби необхідно використати ще один метод оцінювання ризиків, а саме: логіко-ймовірнісне моделювання.

Значний внесок у розвиток методів оцінювання ризиків інформаційної безпеки було внесенно наступними вченими: Милославська Н.Г., Сенаторів М.Ю., Толстой А.І., Кабулов А.В., Варісов А., Каландаров І.

Об’єктом дослідження є процеси оцінювання ризиків інформаційної безпеки.

Предметом дослідження є методи та засоби оцінювання ризиків інформаційної безпеки.

Метою магістерської кваліфікаційної роботи є підвищення рівня інформаційної безпеки медичної установи шляхом оцінки її ризиків ІБ задля подальшого їх усунення або зниження.

Для досягнення поставленої мети необхідно реалізувати низку задач, а саме:

– проаналізувати існуючі відомі методи і засоби оцінювання ризиків ІБ;

– розробити алгоритм запропонованого методу оцінювання ризиків ІБ;

– розробити модель оцінювання ризиків ІБ;

– виконати аналіз досліджуваного об’єкта;

– виконати розрахунки оцінки ризиків ІБ досліджуваного об’єкта за допомогою запропонованого методу;

Наукова новизна дослідження полягає у вдосконаленні методу оцінки ризиків інформаційної безпеки, який полягає у застосуванні модифікованої методики стандарту ISO 27005 із врахуванням показника порушника та наступним логіко-ймовірнісним моделюванням загроз, що дозволить більш чітко оцінити недоліки в захисті установи та визначити для неї величину ризику в цілому.

Практична цінність полягає у тому, що спроектовано реляційну базу даних, яка в повній мірі реалізує запропонований метод оцінки ризиків інформаційної безпеки медичної установи. Запропонована база даних є універсальною і може бути використана будь-якою організацією для розробки власного програмного забезпечення. В структурі бази даних передбачено можливість додавання своїх активів та загроз.

Результати магістерської кваліфікаційної роботи доповідались на молодіжній науково-практичній інтернет-конференції студентів аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2021)» відбулась 1-14 травня 2021 р. [1].

Окремі результати магістерської кваліфікаційної роботи публіковані у фаховому виданні «Вимірювальна та обчислювальна техніка в технологічних процесах» [2].

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття оцінки ризиків інформаційної безпеки

Оцінка ризиків, як частина напрямку інформаційної безпеки є необхідним та важливим інструментом в побудові захисту. Даний процес призначений для виявлення ризиків бізнесу організацій, а також для визначення заходів безпеки, які потрібно вжити для зниження ризику. Оцінка ризиків дає необхідну інформацію для прийняття певних рішень, а також дає можливість керувати.

Під ризиком зазвичай мається на увазі ймовірність реалізації загрози інформаційній безпеці [3]. Оцінка ризиків зазвичай полягає в моделюванні ситуації настання несприятливих умов з використанням обліку всіх можливих факторів, які визначають ризик. Дивлячись з математичної точки зору (при аналізі ризиків) такі чинники слід вважати, як вхідні параметри. Хоча при цьому необхідно враховувати безліч джерел інформації і те, що ця інформація є невизначеною.

Ризик інформаційної безпеки визначається як добуток фінансових втрат, пов'язаних з інцидентами інформаційної безпеки, а також ймовірності того, що вони будуть реалізовані. Дане визначення підходить при розгляді різних архітектур інформаційних систем [4].

Інформація існує в різних формах: може бути написана на папері, може зберігатися в електронному вигляді або пересилатися поштою або ж транслюватися на екрані з використанням електронних засобів, також може обговорюватися в розмові. Якого б вигляду інформація не набувала, вона обов’язково повинна бути захищена відповідним чином.

Оцінка ризиків ІБ, з точки зору управління ризиками, аналіз науковими методами і засобами, інформаційних систем і технологій, які систематично піддаються загрозам і існуючим вразливостям. Проведена оцінка

потенційного збитку в разі загрозливих подій, а також висунуті контрзаходи проти загроз для запобігання і врегулювання ризиків ІБ, наявний контроль ризиків на прийнятному рівні так, щоб максимально забезпечити інформаційну безпеку.

Оцінка ризиків ІБ складається з трьох основних етапів, а саме (рис 1.1):

- ідентифікація загроз;
- ідентифікація вразливостей;
- ідентифікація активів [4].

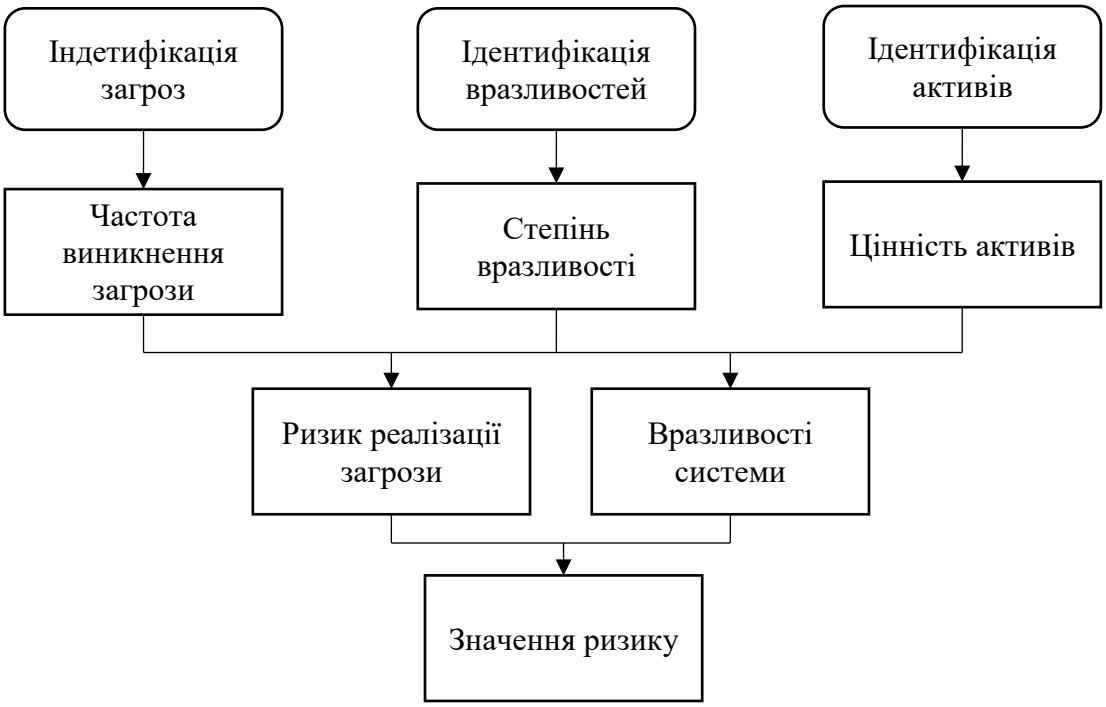


Рисунок 1.1 – Елементи оцінки ризиків інформаційної безпеки

Звичайно при оцінці ризиків найбільший інтерес представляють безпосередньо: формули, а також вхідні дані для розрахунку значення ризику.

Ризик інформаційної безпеки зазвичай визначається, як функція трьох змінних, а саме [3]:

- ймовірність існування загрози;
- ймовірність існування вразливості (незахищеності);
- потенційні наслідки.

Кожна з цих змінних повинна наближатись до нуля, відповідно і загальний ризик також наближається до 0.

Оцінка ризиків містить в собі:

1. визначення й оцінку ймовірності наявних можливих загроз та вразливостей;

2. розрахунок потенційних наслідків і впливу, які може мати загроза на кожен окремий актив;

3. визначення кількісної (вимірної) або якісної (описуваної) вартості ризику.

Також потрібно враховувати те, що ці три змінні рідко коли є незалежними одна від одної. В області інформаційної безпеки, завжди є зв'язок між ймовірністю виникнення загроз, впливом на активи, а також вартістю активів. Наприклад, більш імовірно, що зловмисник буде використовувати саме ту вразливість, яка викличе більший вплив, ніж вразливість з нижчим рівнем впливу. Ця ж схема працює і з більш цінними активами, зловмисник також вибере їх на перевагу менш цінним.

Таким чином, в даній області приймається до уваги більше, ніж просто випадкові дії. Завжди слід враховувати, що при наявності достатнього часу, рішучості та зацікавленості, зловмисники завжди мають можливість обійти практично всі наявні заходи безпеки. Вони можуть бути неймовірно креативими та творчими, коли мають для цього мотивацію. Таким чином, цей фактор повинен бути детально та серйозно розглянутий в процесі оцінки ризиків інформаційної безпеки.

1.2 Підходи до оцінки ризиків

Існує декілька підходів до оцінки ризиків інформаційної безпеки, на рис. 1.2 представлені три загальні підходи, за допомогою яких можна провести оцінку ризиків інформаційної безпеки, це:

- методи;

– управляючі документи;

– засоби [5].

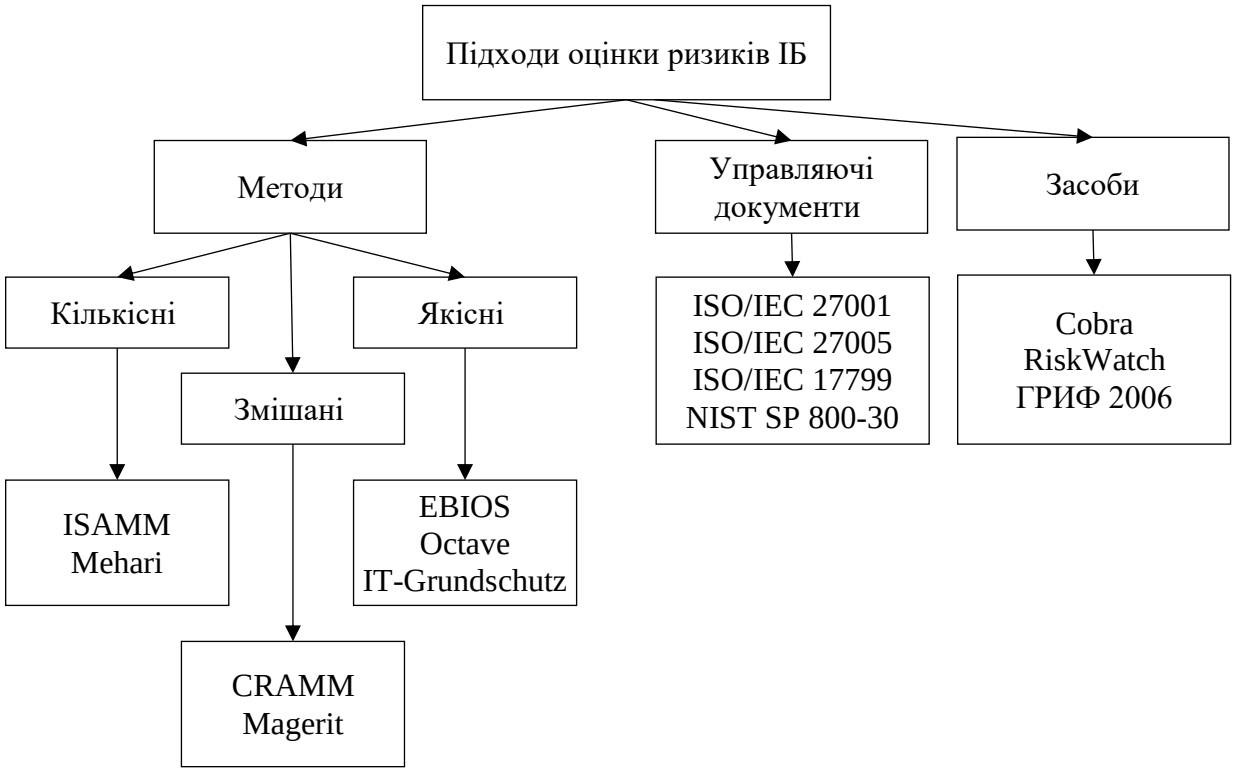


Рисунок 1.2 – Існуючі підходи оцінки ризиків інформаційної безпеки

Необхідно розглянути більш детально кожен з підходів оцінки ризиків інформаційної безпеки.

1.2.1 Методи оцінки ризиків інформаційної безпеки

Під методом розуміється систематизована сукупність кроків і дій, які необхідно зробити для досягнення поставленої мети чи вирішення певної задачі, тобто в даному випадку – провести оцінку ризиків. Тобто, під методом мається на увазі покрокова інструкція, а також засіб (програмний продукт) для проведення оцінки ризиків ІБ на підприємстві.

Всі методи оцінки ризику можна розділити на кількісні, якісні або змішані – комбінацію кількісних методів з якісними.

Кількісні методи використовують вимірні дані для визначення ймовірності втратиг. вартості активів та пов'язаних з ними ризиків. Мета

полягає в наступному: обчислення числових значень для кожного з компонентів, що зібрані в ході оцінки ризиків ІБ та аналізу витрат і переваг [5].

Якісні методи, в свою чергу, використовують відносний показник ймовірності справдження ризику або вартості активу на основі певного рейтингу або поділу на категорії, наприклад: низький, середній, вище середнього, високий, критичний або за шкалою від 1 до 10. Якісна модель оцінює ймовірності та дії виявлених ризиків досить швидким і економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику можуть послужити основою для цілеспрямованої кількісної оцінки [5].

Раніше частіше використовувалися кількісні підходи. Однак, останнім часом використання тільки кількісних методів оцінки ризиків ІБ часто призводить до важкої, тривалої роботи, і до того ж цей метод немає великих переваг перед якісним методом оцінки ризиків ІБ. Проте було знайдено альтернативне рішення – комбінація кількісного і якісного методу, так виник змішаний метод оцінки ризиків ІБ, який об’єднав в собі два вищезгадані метода. В таблиці 1.1 наведено переваги та недоліки для кількісного та якісного методів, змішаний метод відповідно має сукупність цих переваг та недоліків [3].

Таблиця 1.1 – Переваги та недоліки для кількісного та якісного методів

	Кількісний	Якісний
Переваги	– Ризики є пріоритетнішими за фінансові наслідки; – активи є пріоритетнішими за фінансові цінності; – отримання більш спрощених результатів оцінки ризиків ІБ та поверненням інвестицій у забезпечення безпеки; – результати можуть бути виражені в певній управлінській специфічній термінології	– Забезпечує прозорість і легше розуміння класифікації ризиків; – можливість досягнення консенсусу; – не потрібно визначати фінансову вартість активів; – можливість залучення людей, які не є експертами в області інформаційної безпеки.

Продовження таблиці 1.1

	Кількісний	Якісний
	(наприклад, грошові значення, ймовірність реалізації загрози виражаютьться у вигляді певного відсотка); – збільшення точності – це відбувається з плином часу, так, як організація постійно веде записи даних.	
Недоліки	– Вплив значення, які привласнені ризикам на підставі суб'єктивних думок експертів (учасників); – занадто довгий процес досягнення надійних результатів і консенсусу; – часто розрахунок є складним і трудомістким; – результати представлені тільки виключно в грошовому еквіваленті і їх складно інтерпретувати для «нетехнічних людей»; – процес вимагає спеціальної компетентності та знань, тому складно навчити персонал.	– Недостатня відмінність між критичними ризиками; – важко виправдати інвестиції в контроль реалізації, тому що немає підстав для аналізу витрат і переваг; – результати в більшій мірі залежать від якості тієї команди управління ризиками ІБ, яка буде створена.

Слід розглянути більш детально наявні практики методів оцінки ризиків.

Бельгійський метод оцінки ризиків інформаційної безпеки ISAMM. Метод був розроблений на основі Telindus. Це кількісний тип методології управління ризиками ІБ, де ризики оцінюються наступним чином: виражаючи ризики інформаційної безпеки через щорічні очікувані збитки в грошових одиницях. Тобто формула буде виглядати так [6]:

Щорічні очікувані збитки (ALE) = [ймовірність] × [середній вплив] (1.1)

Метод ISAMM дозволяє показувати, а також моделювати зниження ризиків ІБ для кожного поліпшеного контролю і порівнювати з вартістю його реалізації. Ефективність методу полягає в тому, що він дозволяє виконувати

обґрунтовану оцінку ризиків ІБ в заданих рамках, з мінімальними зусиллями та витратами часу. Останньою еволюцією в даній методології є уявлення активів. Це означає, що він може бути використаний для оцінки ризиків інформаційної безпеки щодо активів або щодо згрупованого набору активів. Метод ISAMM складається з трьох основних частин [6]:

– огляду;
– оцінки;
– результату розрахунків та звітності.

Даний метод немає наявності допоміжних програмних засобів, проте має хорошу керівну документацію.

Французький метод оцінки ризиків інформаційної безпеки Mehari являє собою модель управління ризиками ІБ, з модульними компонентами і процесами. Модуль оцінки охоплює, окрім інформаційної системи, ще саму організацію в цілому та її місця розташування, а також умови роботи, правові та нормативні аспекти. Це якісний метод оцінки ризиків ІБ. Також для нього наявні допоміжні програмні засоби [5].

Французький метод оцінки ризиків ІБ EBIOS являє собою набір вимог стандартів ISO/IEC 27001, ISO 31000 та ISO/IEC 27005. Процес аналізу та оцінки ризиків ІБ реалізується за допомогою наступних модулів:

1) Модуль 1 – дослідження контексту. Тут за допомогою трьох заходів реалізується збір інформації щодо об'єктів оцінювання, а саме:

– Захід 1 – визначення сфери управління ризиками.
– Захід 2 – підготовка метрики (критерії безпеки (табл. 1.2), рівні опасності (табл. 1.3) і ймовірності (табл. 1.4) і критерії управління ризиками)).
– Захід 3 – ідентифікація ресурсів інформаційних систем (далі – РІС).

2) Модуль 2 – дослідження небажаних подій. Тут реалізується визначення важливих РІС (з точки зору доступності, цілістності,

конфіденційності) та всіх загроз, які можуть спричинити порушення інформаційної безпеки (їх джерела та ймовірності).

3) Модуль 3 – дослідження сценаріїв загроз, які орієнтовані на виявлення і оцінку сценаріїв, які можуть викликати описані події, що відображають ризики. З цією метою досліджуються джерела наявних загроз і вразливості.

4) Модуль 4 – дослідження ризиків. Тут оцінюються ризики реалізації сценаріїв загроз, які були досліджені в модулі 3.

5) Модуль 5 – дослідження заходів безпеки. Тут орієнтація спрямована на визначення заходів безпеки і на реалізацію їх тестування [5].

Таблиця 1.2 – Приклад критеріїв безпеки

Критерії безпеки	Визначення	Шкала рівня	Детальний опис шкали
Доступність	Доступність РІС, своєчасність РІС першої необхідності	[72 год; ∞]	РІС не доступні більше 72 годин
		[24 год; 72 год]	РІС доступні протягом 72 годин
		[4 год; 24 год]	РІС доступні протягом 24 години
		[0 год; 4 год]	РІС доступні в За 4 години
Цілісність	Точність і повнота основних РІС	Ті, що виявляються	Зміни РІС ідентифікуються
		Визначені	Зміни РІС ідентифікуються і визначаються (локалізуються)
		Цілісні	Зміни РІС не здійснюються
Конфіденційність	Основні РІС доступні тільки зареєстрованим користувачам	Відкриті	Публічні
		Обмежені	Доступ тільки для співробітників і партнерів
		Службові	Доступ мають тільки персонал, який бере участь в розробці
		Персоналізовані	Доступ тільки для конкретних осіб

Таблиця 1.3 – Приклад шкали небезпеки

Шкала рівня	Опис
1. Незначна	Подолання наслідків без будь-яких труднощів
2. Середня	Подолання наслідків незважаючи на ряд труднощів
3. Висока	Подолання наслідків з серйозними труднощами
4. Критична	Непереборні наслідки

Таблиця 1.4 – Приклад ймовірнісної шкали реалізації сценаріїв загроз

Шкала рівня	Опис
1. Мінімальна	Не повинно відбутися
2. Середня	Може трапитись
3. Висока	Можливо чи справді станеться через день-два
4. Максимальна	Відбудеться найближчим часом

EBIOS містить повний набір посібників. Виробляються кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як в державному, так і приватному секторі. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні об'єкти (програмне і апаратне забезпечення, мережі) і нетехнічні об'єкти (організації, людські аспекти, фізична безпека) [7].

Це якісний метод оцінки ризиків інформаційної безпеки, який має наявність допоміжних програмних засобів.

Американський метод оцінки ризиків інформаційної безпеки OCTAVE являє собою самостійний підхід, що вказує на те, що персонал несе відповідальність за встановлення стратегії інформаційної безпеки організації. OCTAVE вимагає аналізу в межах взаємозв’язків між критичними активами, наявними загрозами для цих активів та вразливостями. Даний метод визначає важливі для організації інформаційні активи, і зосереджує діяльність на ці активи, так як для організації вони мають найбільш важливе значення (акцент на кількох важливих активів, проте не більше п'яти). Також існує декілька різних OCTAVE методів, які засновані на OCTAVE критеріях, а саме [8]:

- OCTAVE;
- OCTAVE-S;
- OCTAVE Allegro.

Це якісний метод оцінки ризиків інформаційної безпеки, який має наявність допоміжних програмних засобів.

Німецький метод оцінки ризиків інформаційної безпеки IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою

(далі – СУІБ). Вона включає в себе загальні рекомендації по забезпеченню безпеки ІТ та допоміжні технічні рекомендації для досягнення необхідного рівня ІТ безпеки для конкретного домену [9].

У методі IT-Grundschutz представлені каталоги:

1) модулі;
2) каталоги загроз;
3) каталоги захисту.

Це якісний метод оцінки ризиків інформаційної безпеки, який має наявність допоміжних програмних засобів.

Британський метод CRAMM є досить складним в використанні без засобу, який має таку ж назву, як сам засіб – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, який поєднує кількісні та якісні методи оцінки ризиків ІБ. Даний метод є універсальним, тому він підходить як для малих, так і для великих організацій, як для урядового, так і комерційного сектора. Грамотне використання даного методу оцінки ризиків ІБ дозволяє отримувати досить ефективні результати, найважливішим з яких є можливість економічного обґрунтування витрат на забезпечення інформаційної безпеки та безперервності бізнесу організації. Економічно обґрунтована стратегія управління ризиками інформаційної безпеки дозволяє заощаджувати кошти, уникаючи невиправданих витрат, в кінцевому підсумку [10].

Іспанський метод оцінки ризиків ІБ Magerit є відкритою методологією управління ризиками пропонованої в якості основи і керівництва [5]:

– для того, щоб особи відповідальні за інформаційні системи знали про існування ризиків і необхідність розглядати їх своєчасно;
– для пропозиції систематичного методу аналізу цих ризиків;
– для опису і планування відповідних заходів по утриманню ризику під контролем;

– для підготовки організації по процесу оцінки, аудиту, сертифікації та акредитації.

Це змішаний метод оцінки ризиків інформаційної безпеки, який передбачає наявність допоміжних програмних засобів.

1.2.2 Управляючі документи для оцінки ризиків інформаційної безпеки

Крім методів оцінки ризиків також використовуються управляючі документи, де описуються теоретично і даються методичні вказівки процесу оцінки ризиків інформаційної безпеки, але не дається конкретних технологій та кроків. Найвідомішими стандартами для оцінки ризиків ІБ на території України:

– ISO 27001;
– ISO 27005;
– ISO 17799;
– NIST SP 800-30.

Міжнародний стандарт ISO/IEC 27001 визначає процеси, які представляють можливість для бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки. Стандарт регламентує вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес ризиків організації. Вище зазначені вимоги реалізуються в рамках документованих процесів менеджменту інформаційної безпеки, які структуровані по моделі PDCA (Plan-Do-Check-Act). Стандарт ISO/IEC 27001 являє собою наочну модель управління, яка дозволяє здійснювати оцінку ризиків ІБ, проектування і реалізацію системи ІБ, її менеджмент і переоцінку [11].

Даний стандарт немає явних формул для розрахунку ризиків інформаційної безпеки проте він передбачає наступні вимоги щодо оцінки ризиків ІБ, а саме:

– під час оцінки ризиків повинні бути встановлені критерії щодо оцінки ризиків а також критерії щодо прийняття ризиків;

– необхідна ідентифікація ризиків інформаційної безпеки що направлені на Такі профілі інформаційних ресурсів як конфіденційність цілісність та доступність;

– необхідна ідентифікація власника ризику;

– під час аналізу ризиків потрібно виконати оцінку потенційних втрат у випадку реалізації ризику;

– повинна бути також оцінена ймовірність реалізації ризику.

Стандарт ISO/IEC 27005 призначений для визначення в організації підходу до управління ризиками в залежності, як приклад, від області дії СУІБ, області застосування управління ризиками або ж сектора промисловості. Цей стандарт забезпечує рекомендації для управління ризиками ІБ, які включають інформацію і управління ризиками безпеки технологій телекомунікації. Документ також підтримує загальні концепції, визначені в ISO/IEC 27001 та призначений для сприяння адекватного забезпечення ІБ на основі підходу, який пов'язаний з управлінням ризиком. Він може застосовуватись для усіх типів організацій (наприклад, державних установ, некомерційних організацій, комерційних підприємств), які планують та будуть здійснювати управління ризиками, для компрометації ІБ організації [12].

Згідно зі стандартом ISO 17799, при розробці ефективної системи безпеки слід приділити особливу увагу комплексному підходу до управління інформаційною безпекою [13]. Випливаючи з цього, в якості елементів управління розглядаються технічні, а також організаційно-адміністративні заходи, спрямовані на забезпечення наступних вимог до інформації:

1) конфіденційність;

2) цілісність;

3) достовірність;

4) доступність.

Порушення будь-якої з вищеперелічених вимог може спричинити за собою значні втрати у вигляді збитків і у вигляді неотриманого доходу.

Спеціальна публікація NIST SP 800-30 Guide for Conducting Risk Assessments (посібник з проведення оцінок ризику) присвячена процедурі проведення оцінки ризиків, яка є фундаментальним компонентом процесу управління ризиками в організації відповідно до NIST SP 800-39 та стоїть поряд з визначенням, обробкою та моніторингом ризиків [14]. Процедури оцінки ризиків використовуються для ідентифікації, оцінювання та пріорітизації ризиків, що породжуються використанням інформаційних систем, для операційної діяльності організації, її активів та працівників. Цілями оцінки ризиків є інформування осіб, які приймають рішення щодо них, та підтримка процесу реагування на ризик шляхом ідентифікації:

– актуальних загроз як самої організації, так і опосередковано інших організацій;

– внутрішніх та зовнішніх вразливостей;

– потенційних збитків організації з урахуванням можливостей експлуатації вразливостей загрозами;

– ймовірності виникнення цієї шкоди.

Кінцевим результатом є обчислення детермінанти (значення) ризику, тобто функції від розміру шкоди та ймовірності виникнення шкоди. Оцінку ризиків можна проводити на всіх трьох рівнях управління ризиками (рівні організації, цілі, інформаційних систем) за аналогією з підходом, що застосовується в NIST SP 800-39 та NIST SP 800-37. Підкреслюється, що оцінка ризиків – це безперервний процес, що стосується всіх рівнів управління ризиками в організації, а також вимагає включення в життєвий цикл розробки систем (SDLC) і проводиться з частотою, адекватною цілям і обсягу оцінки [14].

Процес оцінки ризиків включає:

– підготовку до оцінки ризиків;

– проведення оцінки ризиків;

– комунікування результатів оцінки та передачу інформації всередині організації;

– підтримка досягнутих результатів.

У документі йдеться про важливість розробки методології оцінки ризиків, що розробляється організацією ще на етапі визначення ризиків. Вказано, що організація може вибрати одну або кілька методологій оцінки ризиків, залежно від наявних ресурсів, фази SDLC, складності та зрілості бізнес-процесів, критичності/важливості інформації, що обробляється. У цьому створенням коректної методології організація підвищує якість і відтворюваність оцінок ризику, що реалізуються. Методологія оцінки ризику зазвичай включає [14]:

– опис процесу оцінки ризиків;

– модель ризиків, що описує оцінювані фактори ризику та взаємозв'язки між ними;

– спосіб оцінки ризиків (наприклад, якісний або кількісний), що описує значення, які можуть набувати фактори ризику, і те, як комбінації цих факторів можуть бути оброблені;

– спосіб аналізу (наприклад, загрозливо-центричний, орієнтований на активи або вразливості), що описує, як ідентифікуються та аналізуються комбінації факторів ризику.

Модель ризиків визначає оцінювані фактори ризику та взаємозв'язки між ними. Фактори ризику – це характеристики, що використовуються в моделях ризиків, як вхідні дані для визначення рівнів ризиків під час оцінки ризиків. Крім цього, фактори ризику використовуються при комунікуванні ризиків для виділення тих факторів, які відчутно впливають на рівні ризиків у певних ситуаціях та контекстах. Типові фактори ризику включають:

– загрози;

– вразливості;

- негативний вплив;
- ймовірність;
- попередні умови.

При цьому деякі фактори ризику можуть бути декомпозовані до більш детальних характеристик, наприклад, загрози можна декомпозувати до джерел загроз і подій загроз.

1.2.3 Засоби для оцінки ризиків інформаційної безпеки

Окрім методів та управляючих документів для оцінки ризиків інформаційної безпеки використовують засоби для оцінки ризиків. Під засобами розуміється програмне забезпечення з документацією, де описано правила використання. Найбільш відомими засобами, які існують без методики з покроковою інструкцією є:

- Cobra;
- RiskWatch;
- ГРИФ 2006.

Британський програмний засіб Cobra дозволяє проводити оцінку ризиків ІБ. Він працює наступним чином: оцінює відносну важливість усіх загроз і вразливостей, і згідно цього генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики ІБ з потенційними наслідками для певної бізнес-одиниці. Крім того конкретне питання може бути розглянуте «самостійно», без будь-яких наслідків для організації [15].

Американський RiskWatch являє собою певне сімейство програмних продуктів, реалізованих на загальному програмному ядрі, які призначені для управління різними видами ризиків, а також підтримки достаньо великого різновиду стандартів. У даному ПЗ в якості критеріїв для оцінки та управління ризиками беруться річні очікувані втрати (Annual Loss Expectancy, ALE), а також оцінка повернення інвестицій (Return on Investment, ROI). RiskWatch орієнтований на точну кількісну оцінку співвідношення втрат від реалізації загроз безпеки і затрат на створення системи захисту [16].

Російська система ГРИФ 2006 являє собою потужний і зручний засіб [17]. Він призначений для аналізу захищеності ресурсів інформаційних систем та ефективного управління ризиками. Він також дозволяє провести повний аналіз ризиків тобто отримати повну та детальну картину всіх загроз, актуальних для певної інформаційної системи. Дозволяє оцінити, наскільки критичними є вразливості, а також до яких втрат вони можуть привести. Окрім аналізу ризиків тут є можливість управління ризиками. Алгоритм системи «полягає в наступному: він аналізує побудовану модель і далі генерує звіт, який містить значення ризику для кожного окремого ресурсу. Конфігурація звіту може бути будь-якою, таким чином, є можливість створювати, як короткі звіти для керівництва, так і більш детальні звіти для подальшої роботи з результатами.

1.3 Формалізація вимог та постановка задачі

Оцінка ризиків інформаційної безпеки є важливим аспектом для будь якої установи, не є виключенням і медичні установи. На сьогоднішній день вони потребують все більшого захисту. Такі установи мають дуже цінний актив – медичні дані, які є конфіденційними та місять лікарську таємницю. Вимоги до обробки, збереження, передавання та використання медичної інформації описано у Законі України №2801-XII від 23.04.2021 «Основи законодавства України про охорону здоров'я».

У сучасному світі IT-інфраструктура медустанови зазвичай є розгалуженою мережею, яка містить, як правило, основні три складові. По-перше, це звісно робочі місця співробітників установи тобто комп'ютери лікарів, секретарів на рецепції, бухгалтерів і так далі. По-друге, це актуальні медичні інформаційні системи (МІС), які являють собою комплексні автоматизовані інформаційні системи та в яких об'єднані [18]:

- електронні медичні записи про пацієнтів;
- дані медичних досліджень в цифровій формі;

– дані моніторингу стану пацієнта з медичних приладів;
– засоби спілкування між співробітниками;
– фінансова та адміністративна інформація.

По-третє, це важливе сучасне медичне обладнання, (як приклад томографи), яке являє собою якийсь певний медичний прилад або набір таких приладів, який також поєднаний з комп'ютером, де встановлено спеціалізоване ПЗ, а також з іншими пристроями для передачі інформації (наприклад принтером).

Інфраструктура, яка складається з таких пристроїв є схильною до ризиків інформаційної безпеки, так як має низку загроз, наприклад: націлені атаки, зломи медичної інформаційної системи, витік медичної інформації, шкідливі дії власних співробітників. Шкідливі дії співробітників, в свою чергу, діляться на дві категорії: перша – це використання комп'ютерів некомпетентними людьми, з точки зору застосування інформаційних технологій, які можуть заподіяти шкоду для системи ненавмисним чином; друга – це зловмисні дії інсайдерів задля планованої крадіжки або модифікації окремих даних, або ж до повного знищення системи.

Сучасні медичні інформаційні системи не захищені від дій будь-якого співробітника, який володіє суто мінімальною технічною грамотністю в поводженні з комп'ютерами. А більш обширні медичні інформаційні системи, які передбачають досить мінімальний рівень захисту від власних співробітників, ще більше вразливі перед адміністраторами ІТ-інфраструктури установи.

Виходячи з цих даних, медичні заклади є вразливими до загроз пов’язаних з ІБ, тому для усунення цих загроз необхідно періодично виконувати аналіз та оцінку ризиків з подальшим їх управлінням.

Медична інформація повинна бути захищена від усіх типів загроз. Вона є дуже важливою, так як може впливати на людські життя. Постійний моніторинг та оцінка ризиків щодо загроз ІБ підвищує рівень інформаційної

безпеки установи. Оцінивши ризики можна побачити найбільш критичні та суттєві загрози, які слід усувати в першу чергу. Наявні методи оцінки ризиків є не досконалими, так, як можуть оцінювати тільки окремі загрози, але важливо знати загальний рівень інформаційної безпеки установи. Згідно з вищесказаних проблем, необхідно запропонувати метод оцінювання ризиків інформаційної безпеки для медичної установи. Важливим етапом також є створення загальної бази даних загроз, вразливостей та активів медичної установи. Це допоможе в майбутньому автоматизувати процес оцінки ризиків за запропонованим методом. На шляху до цього необхідно виконати наступні кроки:

- аналіз існуючих методів та засобів оцінки ризиків ІБ;
- порівняння наявних методів та засобів оцінки ризиків ІБ;
- підбір основних факторів для оцінки ризиків;
- розробка методу оцінки ризиків ІБ;
- застосування методу на практиці;
- розробка бази даних загроз, вразливостей та активів медичних установ;
- оцінка економічної ефективності методу.

2 РОЗРОБКА МЕТОДУ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Загальний опис методу оцінки ризиків ІБ для медичної установи

Задля підвищення ефективності та результативності оцінки ризиків інформаційної безпеки для запропонованого метода оцінки ризиків інформаційної безпеки для медичної установи (Метод) пропонується поєднання двох методів, а саме: оцінка ризиків за ISO 27005 та оцінка загального рівня ІБ за допомогою логіко-ймовірнісного моделювання.

При оцінці ризиків інформаційної безпеки згідно ISO 27005 враховуються наступні фактори, а саме:

- цінність активу (ЦА);
- рівень вразливості для співвідношення загроз та активів (РВ);
- ймовірність реалізації загрози для кожного активу (ЙЗ).

Метод враховує дані фактори, а також пропонує враховувати такий фактор, як показник порушника (ПП). Даний фактор допомагає визначити вплив знань, навичок, та інших можливостей порушника, на реалізацію загроз та на наслідки від такої реалізації.

Метод оцінювання ризиків інформаційної безпеки для медичної установи передбачає 2 основні стадії:

1) Оцінка загального рівня ризику всіх наявних активів.
2) Оцінка впливу загроз на напрями ІБ та на загальний рівень ІБ установи.

Кожна стадія має свої етапи. Загальний процес оцінки ризиків ІБ для медичної установи має наступні етапи:

1) загальний аналіз установи;
2) ідентифікація активів та визначення їх цінності;

3) ідентифікація вразливостей і загроз та визначення рівня вразливостей у відношенні до кожної загрози;

4) визначення ймовірності реалізації загрози;

5) визначення показника порушника;

6) обчислення загального рівня ризику;

7) приведення оцінки загального рівня ризику до нечіткого вигляду;

8) оцінка впливу загроз на напрями ІБ та загальний рівень ІБ.

Загальна модель процесу оцінки ризиків інформаційної безпеки запропонованого методу зображена на рис. 2.1.

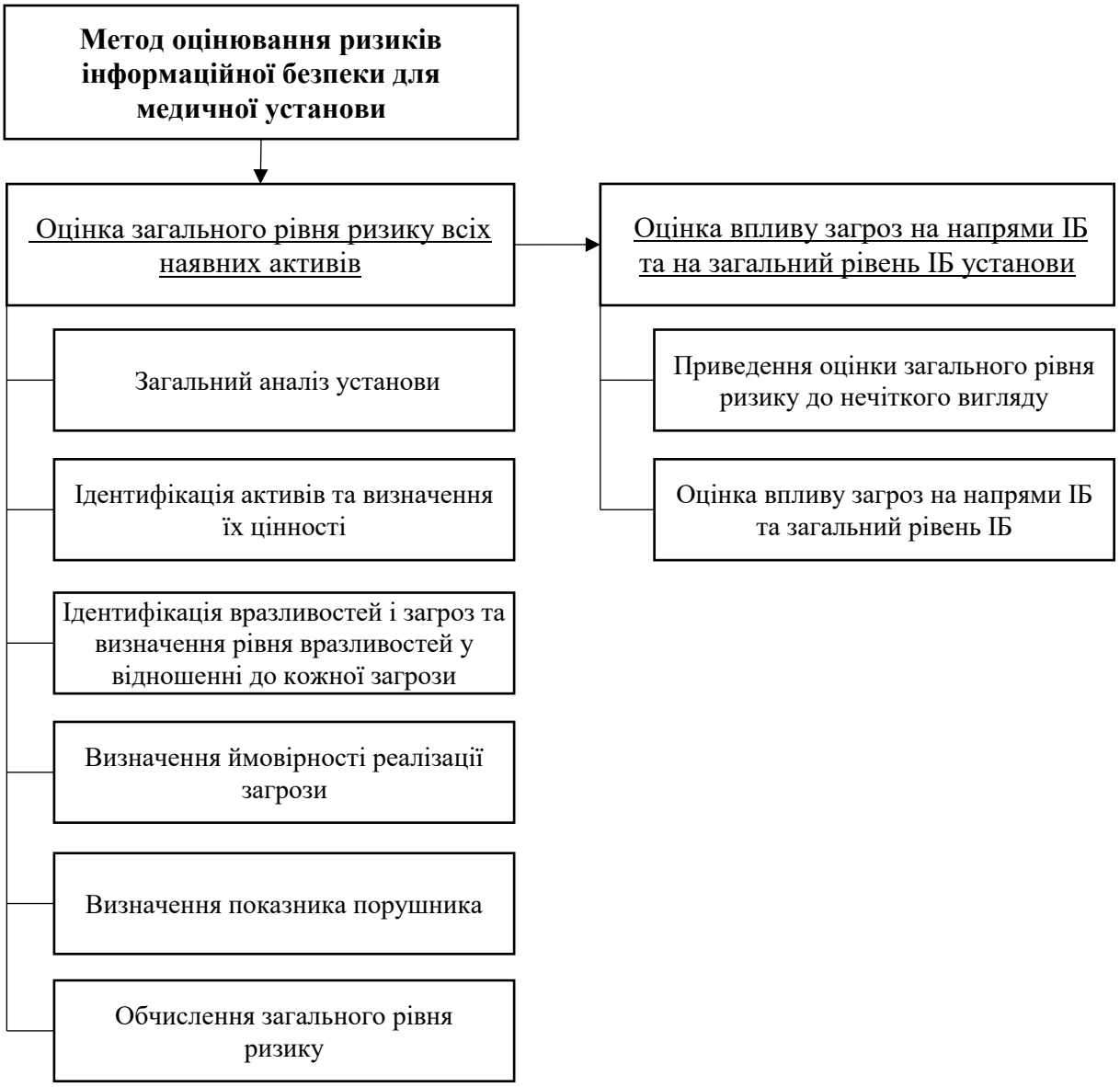


Рисунок 2.1 – Загальна модель процесу оцінки ризиків інформаційної безпеки запропонованого методу

Необхідно розглянути більш детально стадії методу та кожен з етапів методу.

2.2 Оцінка загального рівня ризику всіх наявних активів

Стадія «Оцінка загального рівня ризику всіх наявних активів» включає шість перших етапів з загального переліку. Першим етапом даної стадії є загальний аналіз установи. Даний етап передбачає проведення аналізу установи, а саме:

- визначення організаційної структури;
- визначення топології мережі;
- визначення наявності нормативної документації;
- опис бізнес-процесів;
- визначення наявних засобів та заходів захисту інформаційної безпеки.

Наступним етапом є ідентифікація активів та визначення їх цінності. Активи визначаються у відповідності до ISO 27005 та поділяються на основні та допоміжні. Цінність активу оцінюється за 4-х бальною шкалою.

Наступним кроком є ідентифікація вразливостей і загроз. На даному етапі визначаються всі можливі загрози та наявні вразливості установи. Кожна загроза може мати вплив на один чи декілька активів. Оцінка рівня вразливості визначається за парою загроза-актив за 3-х бальною шкалою.

Наступним етапом оцінювання ризиків інформаційної безпеки медичної установи є визначення ймовірності реалізації загрози. Оцінка ймовірності загроз має враховувати загрози різних груп. Ймовірність реалізації загрози оцінюється за 4-х бальною шкалою.

Показник порушника оцінюється за відповідною шкалою та може бути використаний, як додатковий фактор. Це означає, що даний фактор може враховуватися або не враховуватися. Цей показник зручно використовувати коли більше відомо про самого порушника, а коли необхідно визначити саме

оцінку ризику певної загрози його можна упустити. Показник порушника оцінюється за 4-х бальною шкалою.

Останнім етапом даної стадії є обчислення загального рівня ризику (ЗРР). Після отримання оцінок всіх факторів можна оцінити загальний рівень ризику. Математична формалізація оцінки загального рівня ризику має вигляд:

$$ЗРР = f(ЦА, РВ, ЙЗ, ПП), \quad (2.1)$$

де $ЦА = \{ЦА_1, ЦА_2, ЦА_3, \ldots, ЦА_n\}$;

$РВ = \{РВ_1, РВ_2, РВ_3, \ldots, РВ_k\}$;

$ЙЗ = \{ЙЗ_1, ЙЗ_2, ЙЗ_3, \ldots, ЙЗ_i\}$;

$ПП = \{ПП_1, ПП_2, ПП_3, \ldots, ПП_j\}$.

Графічна формалізація методу оцінювання ризиків ІБ для медичної установи зображена на рис. 2.2.

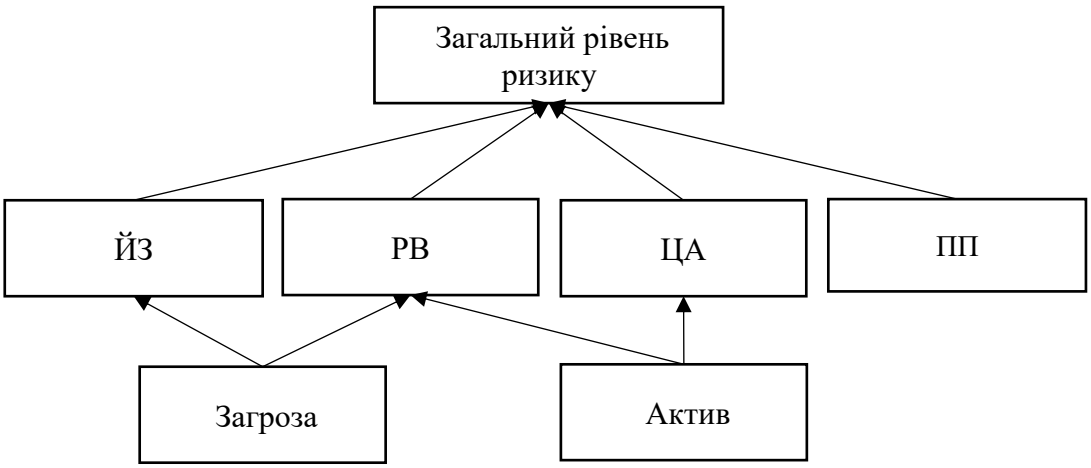


Рисунок 2.2 – Графічна формалізація першої стадії методу оцінювання ризиків ІБ

Обчислення загального рівня ризику виконується за формулою, де враховуються всі фактори:

$$ЗРР_{w,m} = ЦА \cdot РВ \cdot ЙЗ \cdot (ПП), \quad (2.2)$$

де w – актив за яким відбуваються розрахунки;

m – загроза за якою відбуваються розрахунки;

ЦА приймає значення від 1 до 4;

РВ приймає значення від 1 до 3;

ЙЗ приймає значення від 1 до 4;

ПП приймає значення від 1 до 4.

ЗРР без врахування ПП та з врахуванням знаходяться в межах від 1 до 48 (у разі найвищих оцінок по всім факторам буде отримано 48, шкали оцінок описані в наступних підрозділах) та від 1 до 192 (у разі найвищих оцінок по всім факторам буде отримано 192, шкали оцінок описані в наступних підрозділах) відповідно і мають певний показник критичності (табл. 2.1 та табл. 2.2).

Таблиця 2.1 – Показник критичності для ЗРР без ПП

Загальний рівень загроз (без ПП)	Показник критичності
(1-8)	Низький
(9-16)	Нижче середнього
(17-24)	Середній
(25-36)	Вище середнього
(37-48)	Високий

Таблиця 2.2 – Показник критичності для ЗРР з ПП

Загальний рівень загроз (з ПП)	Показник критичності
(1-33)	Низький
(34-64)	Нижче середнього
(65-96)	Середній
(97-144)	Вище середнього
(145-192)	Високий

Слід розглянути більш детально кожен з факторів: цінність активу, рівень вразливості для співвідношення загроз та активів, ймовірність реалізації загрози для кожного активу та показник порушника.

2.2.1 Визначення цінності активів

Відповідності до ISO 27005 активи організації можна поділити на основні та допоміжні. До основних активів належать:

– бізнес-процеси;

– інформація.

Під бізнес-процесами розуміється сукупність різних окремих видів діяльності, в результаті яких створюються продукти або послуги, які можуть представляти інтерес для споживачів. Група «Інформація» містить під собою відомості, які є предметом власності, які підлягають захисту від порушення конфіденційності, цілісності та доступності, відповідно до норм правових документів та вимог власників інформації, незалежно від форми представлення. Відомості, компрометація яких не призведе до втрат та ніяким чином не вплине на діяльність організації, не розглядаються, як цінний актив.

До допоміжних активів належать наступні групи:

– апаратно-програмні комплекси;
– носії даних;
– мережа;
– персонал;
– місце функціонування установи.

Група «Апаратно-програмний комплекс» являє собою сукупність технічних та програмних засобів, які призначені для виконання взаємопов'язаних експлуатаційних функцій щодо обробки інформації з обмеженим доступом, яка також включає активну апаратне забезпечення обробки даних, стаціонарне апаратне забезпечення, периферійні пристрої обробки, операційні системи, а також прикладне програмне забезпечення.

Група «Носії даних» являють собою носії для зберігання даних, включаючи електронні носії та аналогові.

Група «Мережа» містить під собою сукупність телекомунікаційних пристроїв, які використовуються для з'єднання декількох фізично віддалених сегментів інформаційної системи.

Під персоналом маються на увазі всі суб'єкти, що мають легітимний доступ до меж контрольованої зони та можуть бути потенційними внутрішніми порушниками.

Остання група допоміжних активів «Місце функціонування установи» описує межі контрольованої зони, де функціонує інформаційна система.

Для медичних установ типу міська клінічна лікарня обов'язковими групами активів є інформація та бізнес-процеси, а з допоміжних груп можна обрати, ті які більш стосуються установи, наприклад: апаратно-програмний комплекс, носії даних та персонал.

Цінність активу оцінюється за тим, які збитки установа отримає від реалізації ризику ІБ спрямованого на конфіденційність, цілісність та/або доступність такого активу.

На основі цих даних створюється таблиця цінності активів. Дана таблиця містить ідентифікатор для кожного активу, групу активу та оцінку її впливу на конфіденційність, цілісність та доступність. Виходячи з цих оцінок визначається загальна цінність активу. Цей показник визначається шляхом обрання найбільшої оцінки впливу активу на один з напрямів.

Цінність активу математично можна описати наступним кортежем:

$$\text{ЦА} = (\text{ВК}, \text{ВЦ}, \text{ВД}), \tag{2.3}$$

де ВК – вплив реалізації ризику ІБ на конфіденційність активу;

ВЦ – вплив реалізації ризику ІБ на цілісність активу;

ВД – вплив реалізації ризику ІБ на доступність активу.

Оцінки впливу на кожен з напрямів задаються згідно з шкалою, де:

– 1 – реалізація ризику ІБ, спрямованого на конфіденційність, цілісність та/або доступність активу не буде мати жодних наслідків, як для окремих бізнес-процесів, так для організації в цілому.

– 2 – реалізація ризику ІБ, спрямованого на конфіденційність, цілісність та/або доступність активу може призвести до незначних втрат для установи, при умові, коли відновлення попереднього стану системи можливе без зупинки бізнес-процесів.

– 3 – реалізація ризику ІБ, спрямованого на конфіденційність, цілісність та/або доступність активу приведе, як до значних фінансових втрат,

так і/або чинитиме суттєвий негативний вплив на престиж організації, при умові, коли відновлення попереднього стану системи є можливим, але потребує тимчасових великих та/або фінансових ресурсів.

– 4 – реалізація ризику ІБ, спрямованого на конфіденційність, цілісність та/або доступність активу може призвести до повної зупинки бізнес-процесів, до великих фінансових втрат та/або може вплинути на престиж організації.

2.2.2 Визначення рівня вразливості кожного активу

Наступним кроком є визначення рівня вразливості для співвідношення загроз та активів організації. Вразливість інформаційної системи в інформаційній безпеці визначається, як певна властивість такої системи, яка може зумовлювати реалізацію загроз безпеці інформації, яка обробляється в системі [19]. Умовою для реалізації загрози безпеці, інформації, що оброблюється в інформаційній системі може бути якесь слабке місце в такій системі. Чим вищий рівень вразливості – тим вищий загальний рівень загрози.

Рівень вразливості визначається з аналізу наскільки певний актив вразливий до певної загрози (тобто чи існують заходи/засоби захисту активу до певної загрози, схильність активу до загроз певного типу і т.д).

Даний фактор визначається за допомогою надання оцінки кожній парі загроза-актив. Тобто, мається на увазі, що для кожної загрози визначається індивідуальна оцінка рівня вразливості по відношенню до певного активу. І навпаки, для кожного активу визначається окрема оцінка рівня вразливості по відношенню до певної загрози.

Рівень вразливості математично можна описати наступною наступним кортежем:

$$РВ = (РВК, РВЦ, РВД), \quad (2.4)$$

де РВК – рівень вразливості порушення конфіденційності активу;

РВЦ – рівень вразливості порушення цілісності активу;

РВД – рівень вразливості порушення доступності активу.

Оцінки визначення рівня вразливості визначаються за трьох бальною шкалою, де:

– 1 – рівень вразливості є низьким щодо конфіденційності, цілісності та/або доступності одного з цінних активів організації;

– 2 – рівень вразливості є середнім щодо конфіденційності, цілісності та/або доступності одного з цінних активів організації;

– 3 – рівень вразливості є високим щодо конфіденційності, цілісності та/або доступності одного з цінних активів організації.

Такі результати записуються в таблицю, приклад такої таблиці представлено в табл. 2.3.

Таблиця 2.3 – Приклад матриці рівня вразливості активів

Загрози інформаційної безпеки	Цінні активи установи			
	Актив 1	Актив 2	…	Актив w
Загроза 1	1	2	…	3
Загроза 2	3	1	…	2
…	…	…	…	…
Загроза m	2	3	…	–

Існують загрози, які не впливають на той чи інший актив, в такому разі цей фактор упускається, а у відповідне місце в таблиці ставиться прочерк.

2.2.3 Визначення ймовірності реалізації загроз

Наступним етапом оцінювання ризиків інформаційної безпеки медичної установи є визначення ймовірності реалізації загрози. Оцінка ймовірності загроз має враховувати загрози, які мають різну природу та особливості, що властиві різним групам, наприклад [20]:

– Навмисні загрози – ймовірність таких загроз залежить від мотивації зловмисника, від наявних у нього знань, компетенції та доступних йому ресурсів, а також цінності та привабливості активів для реалізації атак.

– Випадкові загрози – ймовірність випадкових загроз оцінюється за допомогою використання статистики та минулого досвіду. Ймовірність таких загроз також залежить від близькості розташування установи до джерел небезпеки, наприклад таких, як залізничні колії, автомагістралі, а також заводи, які в своїй діяльності мають справу з хімічними речовинами, небезпечними матеріалами і т.д. Також слід враховувати географічне розташування установи, яке може вплинути на можливість виникнення екстремальних погодних умов. Ще одним дуже важливим фактором є ймовірність людських помилок та раптові поломки обладнання, що також має бути врахованим.

– Попередні інциденти – інциденти, які вже відбувалися у минулому, ілюструють у теперішньому часі проблеми у існуючих заходах захисту.

– Нові розробки та тенденції – включають різні звіти, тенденції та новини, отримані з Інтернету, інших установ, новин в т.д.

Ймовірність реалізації загроз показує, наскільки ймовірно, те що загроза не просто існує, а може відбутись в реальності.

Ймовірність реалізації загроз математично можна описати наступною залежністю:

$$ЙЗ = (ЧВУ, ЧВС), \quad (2.5)$$

де ЧВУ – частота виникнення загрози в установі;

ЧВС – частота виникнення загрози у даній сфері.

Оцінка ймовірності визначається відповідно до кожної загрози й записується в таблицю (табл. 2.4), за відповідною шкалою, де:

– 1 – загроза існує, проте ще не зустрічалася у даній сфері;

– 2 – загроза існує та виникає у даній сфері 2-3 рази на рік;

– 3 – загроза існує та була раніше реалізована в установі;

– 4 – загроза існує та виникає періодично (2-3) рази на рік в установі.

Таблиця 2.4 – Ймовірність реалізації загроз

Загроза ІБ	Загроза 1	Загроза 2	…	Загроза m
Ймовірність	2	1	…	2

Цей етап може бути фінальним у визначенні оцінок факторів для оцінки ризиків інформаційної безпеки медичної установи, а можна врахувати ще один фактор, який надасть більш точний результат.

2.2.4 Визначення показника порушника

Для визначення показника порушника використовується модель порушника, яка являє собою сукупність припущень про можливості зловмисника, які він може використовувати при розробці та проведені атак.

Модель ймовірного порушника включає [21]:

– опис можливих порушників;

– припущення про наявну інформацію у порушника про об'єкт атаки;

– припущення про наявні у порушника засоби для проведення атаки;

– опис об'єктів та цілей атаки порушником;

– опис каналів атаки.

Усі порушники поділяються на дві групи, а саме:

– зовнішні порушники – фізичні особи, які не мають права перебування на території контрольованої зони;

– внутрішні порушники – фізичні особи, які мають право перебування на території контрольованої зони.

Як зовнішній порушник інформаційної безпеки розглядається порушник, який не має безпосереднього доступу до технічних засобів та ресурсів системи, що знаходяться в межах контрольованої зони.

Можливості внутрішнього порушника суттєвим чином залежать від діючих у межах контрольованої зони обмежувальних факторів, основним з яких є реалізація комплексу режимних та організаційно-технічних заходів, у

тому числі підбір, розстановка та забезпечення високої професійної підготовки кадрів, допуск фізичних осіб всередину до контрольованої зони та контролю за порядком проведення робіт, спрямованих на запобігання та уникнення несанкціонованих дій.

До внутрішніх порушників можуть належати:

– адміністратори інформаційних систем (ІС);

– технічний персонал інформаційних систем;

– підрозділи, які здійснюють технічний супровід обладнання, програмного забезпечення та засобів захисту інформації;

– користувачі ІТС;

– співробітники, які мають санкціонований доступ до службових приміщень, в яких розміщуються активи ІТС, але не мають права на доступ до самих активів;

– обслуговуючий персонал (охорона, працівники інженерно-технічних служб тощо);

– уповноважений персонал розробників ІТС;

– та інші.

Показник порушника визначається за наступними критеріями: мотив порушення, рівень обізнаності та кваліфікації порушника щодо ІТС установи (РК), наявність можливості використання методів та засобів подолання систем захисту (МВЗ), специфікація порушника за часом дії (ЧД), специфікація порушника за місцем дії (МД) і в результаті загальне значення фактора записується у показник порушника (табл. 2.5).

Кожен критерій має оцінку ефективності від 1 до 4, де 1 – низька оцінка, 2 – середня оцінка, 3 – вище середньої оцінка та 4 – висока оцінка [22]. Така оцінка показує наскільки даний критерій може вплинути на реалізацію загроз.

Показник порушника математично можна описати наступним кортежем:

$$ПП = (МП, РК, МВЗ, ЧД, МД), \quad (2.6)$$

де МП приймає значення від 1 до 4;

РК приймає значення від 1 до 4;

МВЗ приймає значення від 1 до 4;

ЧД приймає значення від 1 до 4;

МД приймає значення від 1 до 4.

Мотивом порушника може бути: отримання певної інформації; досягнення можливості вносити власні зміни в інформаційні потоки установи; нанесення збитків установі шляхом знищення матеріальних та інформаційних цінностей.

Наявність можливості використання методів та засобів подолання систем захисту визначається за 4-х бальною шкалою, де [22]:

1 – показує низький рівень можливостей щодо ведення діалогу з ІТС. Порушник має можливість запуску фіксованого набору певних завдань та програм.

2 – визначається наявною можливістю створення, розробки і запуску власних програм з певними новими функціями обробки інформації.

3 – визначається наявною можливістю керування функціонуванням ІТС, тобто можливістю впливу на програмне забезпечення системи, на її склад та конфігурацію устаткування.

4 – визначається наявністю повного обсягу можливостей (можливість здійснення проектування, реалізації, впровадження і т.д. програмного та апаратного забезпечення ІТС).

РК оцінюється за 4-х бальною шкалою, де:

1 – порушник володіє інформацією про певні функціональні особливості ІТС та вміє користуватися деякими штатними засобами;

2 – включає попередні знання та можливості, а також володіє високим рівнем знань та має досвід роботи з технічними засобами системи та розуміє принцип їхнього обслуговування;

3 – включає попередні знання та можливості, а також володіє високим рівнем знань у галузі проектування та експлуатації ІТС, програмуванні та обчислювальної техніки;

4 – включає попередні знання та можливості, а також володіє інформацією щодо функцій та механізмів дії засобів захисту.

МД визначається за 4-х бальною шкалою, де:

– 1 – без доступу на контрольовану територію установи (ІТС);

– 2 – з доступом на контрольовану територію, але без наявності доступу до певних технічних засобів ІТС;

– 3 – з доступом до робочих місць користувачів ІТС;

– 4 – з доступом до засобів певних адміністрування ІТС установи.

Таблиця 2.5 – Модель порушника

Визначення категорії	МП	РК	МВЗ	ЧД	МД	Показник порушника
Внутрішні по відношенню до установи						
Персонал, який обслуговує технічні засоби (інженери, техніки)	3	1	4	2	1	4
Зовнішні по відношенню до установи						
Відвідувачі	3	2	2	1	3	3

Показник порушника визначається шляхом вибору максимальної оцінки критеріїв. Формалізувавши визначення всіх факторів та алгоритм методу оцінювання ризиків інформаційної безпеки слід перевірити його на практичному застосуванні.

2.3 Оцінка впливу загроз на напрями ІБ та на загальний рівень ІБ установи

Наступна стадія «Оцінка впливу загроз на напрями ІБ та на загальний рівень ІБ установи» включає два останніх етапи з загального переліку етапів. Оцінивши загальний рівень ризику по кожному активу слід визначити вплив реалізації таких загроз на напрями інформаційної безпеки, а саме: конфіденційність цілісність та доступність, а також вплив на загальний рівень інформаційної безпеки установи. Це буде виконуватись за допомогою

використання методу логіко-ймовірнісного моделювання. Даний метод допомагає графічно та математично формалізувати та оцінити вплив загроз.

Одна загроза може мати певний вплив, як на всі профілі безпеки так і на один чи два з них. Проте ці впливи будуть різнитись, так як будуть мати різні оцінки рівня вразливості та ймовірності реалізації загроз. Тобто наприклад загроза «Навмисні дії працівників» може впливати, як на конфіденційність так і на цілісність та доступність, а, наприклад, загроза «Пересилання інформації з обмеженим доступом через загальнодоступну мережу» буде впливати тільки на конфіденційність та цілісність.

Для дослідження питань надійності та безпеки інформаційно-телекомунікаційних систем часто застосовуються логіко-ймовірнісні методи моделювання, при яких: структура інформаційно-телекомунікаційної системи описується за допомогою засобів математичної логіки, а саме кількісне оцінювання надійності та безпеки такої системи здійснюється за допомогою теорії ймовірностей [23].

Пропонується виконати розрахунки логіко-ймовірнісного моделювання за допомогою обчисленого загального рівня ризику загроз. Даний показник буде взятий у якості загальної ймовірності виникнення загрози для логіко-ймовірнісного моделювання. Для цього потрібно виконати перетворення бальних оцінок ЗРР у наближені оцінки ймовірностей. Це відбувається за шкалою, що наведена у табл. 2.6.

Таблиця 2.6 – Відповідність показника критичності загальній ймовірності виникнення для логіко-ймовірнісного моделювання

Показник критичності	Загальний ймовірність виникнення для логіко-ймовірнісного моделювання
Низький	[0-0,05]
Нижче середнього	(0,05-0,15]
Середній	(0,15-0,30]
Вище середнього	(0,30-0,60]
Високий	(0,60-1]

Після перетворення експертом задається близька оцінка ймовірності виникнення загрози з певного діапазону. Формалізація такої оцінки передбачає два етапи: – фазифікацію (розмиття) та дефазифікацію (отримання найбільш достовірного значення). Етап дефазифікації виконується методом центру ваги [24].

$$\tilde{X} = \frac{\sum_i x_i * \mu_i}{\sum_i \mu_i}, \tag{2.7}$$

де x_i - наближена ймовірність;

μ_i - значення функції належності.

Даний метод передбачає побудову логіко-ймовірнісної моделі загроз у вигляді базових та проміжних подій, які зв’язуються між собою за допомогою логічних функцій «І» та «АБО».

Щоб оцінити загальний вплив загроз на один з напрямів ІБ та на загальний рівень інформаційної безпеки необхідно використати формулу для незалежних або залежних базових подій (якщо події зв’язані логічною функцією «І» – вираз 2, якщо події зв’язані логічною функцією «АБО» – вираз 3) [25]:

$$P = \prod_{j=1}^{k} \text{ЗРР}_j, \tag{2.8}$$

$$P = 1 - \prod_{j=1}^{k} (1 - \text{ЗРР}_j), \tag{2.9}$$

де ЗРР_j – загальний рівень j-тої загрози (події), які є причинами появи вихідної події;

k – кількість подій, що впливають на появу вихідної події.

Необхідно перевірити застосування запропонованого методу оцінки ризиків інформаційної безпеки для медичних установ на практиці.

3 РОЗРАХУНОК РИЗИКІВ ІБ МЕДИЧНОЇ УСТАНОВИ

3.1 Загальний аналіз установи

Досліджуваним об’єктом для оцінки ризиків було обрано медичний заклад типу «міська клінічна лікарня» (далі – МКЛ). Такі лікарні зазвичай є не досить великими (містять штат близько 200 людей), але досить розвиненими в сфері інформаційних технологій. На теперішній час практично вся медична інформація зберігається в цифровому просторі. Прихід медичних інформаційних систем значно полегшив процес комунікації лікаря з пацієнтом для обох сторін: заведення електронних карток, видача електронних лікарняних і т.д. Проте це також спричинило появі великій кількості нових вразливостей, а з ними і загроз ІБ.

Типова міська лікарня має у своєму функціонуванні низку активів (табл. 3.1).

Таблиця 3.1 – Перелік активів типової медичної установи

№	Група	Актив
1	Інформація	БД інформаційно-телекомунікаційної системи
2		Технологічний процес зберігання, обробки, збору та передачі інформації
3		Електронні звіти
4		Паперові звіти
5		Паперові картки хворих
6		Електронні історії хвороб
7		Паперові історії хвороб
8		Паперові журнали ведення
9	Бізнес-процеси	Процес прийому пацієнтів
10		Внесення даних до МІС
11		Наради
12	Персонал	Керівництво
13		Лікарі/Медичні сестри
17		Санітари
18		Технічний персонал
19		Бухгалтер

Продовження таблиці 3.1

№	Група	Актив
20	Носії інформації	Флешки-ЕЦП персоналу
21		Жорсткі диски
22		Паперова документація
23	Апаратно-програмний комплекс	Апаратне забезпечення
24		Програмне забезпечення

Загрози установи виникають внаслідок наявних вразливостей, існуючих заходів захисту та типових загроз даної сфери [26]. Загальний перелік загроз для медичної установи типу «міська клінічна лікарня» наведено у табл. 3.2.

Таблиця 3.2 – Перелік загроз типової медичної установи

№	Загроза
1	Пошкодження інформації внаслідок стихійних лих
2	Пошкодження інформації внаслідок некомпетентності персоналу
3	Пошкодження інформації внаслідок ШПЗ
4	Пошкодження інформації внаслідок навмисних помилок персоналу
5	Пошкодження інформації внаслідок ненавмисних помилок персоналу
6	Пошкодження інформації внаслідок вільного доступу до неї
7	Пошкодження інформації внаслідок збоїв
8	Пошкодження інформації внаслідок поломок
9	Пошкодження інформації внаслідок зламу/компроментації паролів
10	Розкриття інформації внаслідок ШПЗ
11	Розкриття інформації внаслідок вішингу
12	Розкриття інформації внаслідок фішингу
13	Розкриття інформації внаслідок зламу/компроментації паролів
14	Розкриття інформації внаслідок підслуховування
15	Розкриття інформації внаслідок вільного доступу до неї
16	Розкриття інформації внаслідок навмисних помилок персоналу
17	Розкриття інформації внаслідок ненавмисних помилок персоналу
18	Розкриття інформації внаслідок її викрадення
19	Втрата доступу до інформації внаслідок Ddos-атак
20	Втрата доступу до інформації внаслідок ШПЗ
21	Втрата доступу до інформації внаслідок навмисних помилок персоналу
22	Втрата доступу до інформації внаслідок ненавмисних помилок персоналу
23	Втрата доступу до інформації внаслідок збоїв
24	Втрата доступу до інформації внаслідок поломок
25	Втрата доступу до інформації внаслідок стихійних лих
26	Втрата доступу до інформації внаслідок некомпетентності персоналу

Слід розглянути першопричини кожної загрози. Загроза «Пошкодження інформації внаслідок стихійних лих» та «Втрата доступу до інформації внаслідок стихійних лих» є випадковими загрозами. Вони залежать від особливостей розташування будівлі установи, від погодних умов і т.д. Зазвичай в простих медичних установах відсутні резервні копії інформації, щоб в разі реалізації загрози, інформацію можна було відновити до попереднього стану. На щастя, такі загрози не так часто трапляються.

Загрози «Пошкодження інформації внаслідок некомпетентності персоналу» та «Втрата доступу до інформації внаслідок некомпетентності персоналу» є випадковими загрозами. Вони безпосередньо залежать від рівня знань та навичок персоналу. Медичні установи стрімко перейшли до цифрового простору, проте персонал не встигає за цим швидким рухом. Працівники потребують навчання, проте це потребує витрат, тому не все керівництво розуміє його необхідність.

Загрози «Пошкодження інформації внаслідок ШПЗ», «Розкриття інформації внаслідок ШПЗ» та «Втрата доступу до інформації внаслідок ШПЗ» можуть бути, як навмисними, так і випадковими. Більшість невеликих медичних установ не встановлюють на робочих станціях антивірусний захист та обмеження на завантаження та встановлення програмного забезпечення, це призводить до потрапляння ШПЗ в мережу установи. Загрози є дуже поширеними та небезпечними.

Загрози «Пошкодження інформації внаслідок навмисних помилок персоналу», «Пошкодження інформації внаслідок ненавмисних помилок персоналу», «Розкриття інформації внаслідок навмисних помилок персоналу», «Розкриття інформації внаслідок ненавмисних помилок персоналу», «Втрата доступу до інформації внаслідок навмисних помилок персоналу» та «Втрата доступу до інформації внаслідок ненавмисних помилок персоналу» є схожими між собою результатами їхньої реалізації, але різними за причинами виникнення. Основними причинами виникнення таких загроз є необізнаність персоналу у сфері ІБ та інсайдери. Загрози дуже поширені та часті.

Загрози «Пошкодження інформації внаслідок вільного доступу до неї» та «Розкриття інформації внаслідок вільного доступу до неї» виникають внаслідок відсутності автоматичного блокування робочих екранів комп'ютерів, залишання інформації з обмеженим доступом на видних місцях, відсутності обмеження доступу до критичних приміщень.

Загрози «Пошкодження інформації внаслідок збоїв» та «Втрата доступу до інформації внаслідок збоїв» є випадковими та виникають внаслідок різких змін напруги і т.д.

Загрози «Пошкодження інформації внаслідок поломок» та «Втрата доступу до інформації внаслідок поломок» виникають внаслідок застарілого або бракованого апаратного забезпечення та обладнання.

Загрози «Пошкодження інформації внаслідок зламу/компроментації паролів» та «Розкриття інформації внаслідок зламу/компроментації паролів» виникають внаслідок вибраних користувачами нестійких паролів та неправильного зберігання паролів.

Загрози «Розкриття інформації внаслідок вішингу» та «Розкриття інформації внаслідок фішингу» є частими загрозами. Вони виникають внаслідок відсутності навчання персоналу інформаційній безпеці. Зловмисники використовують дану вразливість та дізнаються важливу інформацію.

Загроза «Розкриття інформації внаслідок підслуховування» виникає внаслідок відсутності окремих шумоізолюючих кабінетів для проведення нарад, прийому пацієнтів в кабінетах з відчиненими вікнами, дверима і т.д.

Загроза «Розкриття інформації внаслідок її викрадення» виникає внаслідок зберігання носіїв інформації в вільнодоступних, незахищених місцях.

Загроза «Втрата доступу до інформації внаслідок Ddos-атак» виникає внаслідок відсутності захисту від атак такого роду.

3.2 Визначення оцінок факторів

Задля розрахунку загального рівня ризику необхідно оцінити 4 фактора впливу. Перший фактор цінність активу оцінюється по кожному активу в межах від 1 до 4. Він враховує наступні критерії: вплив реалізації ризику ІБ на конфіденційність активу, вплив реалізації ризику ІБ на цілісність активу та вплив реалізації ризику ІБ на доступність активу. Для прикладу визначення цінності розглянемо актив «БД інформаційно-телекомунікаційної системи». Актив має високий вплив по всім критеріям, так, як тут містяться персональні дані пацієнтів, працівників, а також діагнози – що є медичною таємницею. Тому цінність такого активу буде найвищою, тобто 4. Результати всіх оцінок наведені в таблиці 3.3.

Таблиця 3.3 – Визначення цінності активів

№	Група	Актив	Конфіденційність	Цілісність	Доступність	Цінність актива
а	б	в	г	ґ	д	ж
1	Інформація	БД інформаційно-телекомунікаційної системи	4	4	4	4
2		Технологічний процес зберігання, обробки, збору та передачі інформації	3	3	3	3
3		Електронні звіти	3	2	1	3
4		Паперові звіти	3	2	2	3
5		Паперові картки хворих	3	2	1	3
6		Електронні історії хвороб	2	2	1	2
7		Паперові історії хвороб	2	2	1	2
8		Паперові журнали ведення	1	1	1	1
9	Бізнес-процеси	Прийом пацієнтів	3	-	-	3
10		Внесення даних до МІС	4	3	1	4
11		Наради	2	-	-	2
12	Персонал	Керівництво	4	2	2	4
13		Лікарі/Медичні сестри	3	1	2	3

Продовження таблиці 3.3

а	б	в	г	ґ	д	ж
14		Санітари	1	1	1	1
15		Технічний персонал	1	1	1	1
16		Бухгалтер	2	2	2	2
17	Носії інформації	Флешки з ЕЦП працівників	3	2	2	3
18		Жорсткі диски	3	3	3	3
19		Паперова документація	2	2	2	2
20	Апаратно-програмний комплекс	Апаратне забезпечення	3	3	3	3
21		Програмне забезпечення	3	2	3	3

Наступним етапом є визначення другого фактору: рівня вразливості. Кожен актив має певний рівень вразливості для відповідної загрози. Наприклад, розглянемо актив 3 – «Електронні звіти» та загрозу 3 – «Пошкодження інформації внаслідок ШПЗ». Даний актив має великий рівень вразливості до даної загрози, так, як наприклад якщо на робочий комп’ютер працівника потрапить ШПЗ, в першу чергу постраждають файли такого комп’ютера. А наприклад, актив 4 – Паперові звіти взагалі не вразливий до такої атаки, тому доцільно взагалі не ставити оцінку для цієї пари. Всі оцінки рівня вразливостей по парам загроза-актив наведені в таблиці 3.4.

Таблиця 3.4 – Визначення рівня вразливостей

Загрози ІБ	Активи установи																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
2	2	-	2	1	1	2	1	1	1	2	-	-	-	-	-	-	2	1	1	2	2
3	3	-	2	-	-	2	-	-	-	2	-	-	-	-	-	-	2	2	-	2	3
4	2	-	2	2	2	2	2	2	1	2	-	-	-	-	-	-	2	1	1	2	2
5	3	-	3	2	2	3	2	2	1	2	-	-	-	-	-	-	2	1	1	2	3
6	3	-	2	2	3	2	2	2	1	2	-	-	-	-	-	-	2	1	1	2	2
7	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
8	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
9	3	-	3	2	2	3	2	2	1	2	-	-	-	-	-	-	2	1	1	2	3
10	3	-	3	2	2	3	2	2	-	2	-	-	-	-	-	-	2	1	1	2	3
11	3	-	3	2	2	3	2	2	-	2	-	2	2	2	2	2	2	1	1	2	3

Продовження таблиці 3.4

Загрози ІБ	Активи установи																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
12	3	-	3	2	2	3	2	2	-	2	-	2	2	2	2	2	2	1	1	2	3
13	3	-	3	2	2	3	2	2	1	2	-	-	-	-	-	-	2	1	1	2	3
14	1	-	1	1	1	1	1	1	2	1	2	-	-	-	-	-	1	1	1	1	1
15	3	-	2	2	3	2	2	2	1	2	-	-	-	-	-	-	2	1	1	2	2
16	3	-	2	2	2	2	2	2	1	2	-	-	-	-	-	-	2	1	1	2	2
17	3	-	3	2	2	3	2	2	1	2	-	-	-	-	-	-	2	1	1	2	3
18	1	2	1	2	2	1	2	2	-	-	-	-	-	-	-	-	2	1	1	2	1
19	2	-	1	-	-	1	-	-	-	2	-	-	-	-	-	-	-	-	-	1	2
20	3	-	3	2	2	3	2	2	-	2	-	-	-	-	-	-	2	1	1	2	3
21	2	-	2	2	2	2	2	2	1	2	-	-	-	-	-	-	2	1	1	2	2
22	3	-	3	2	2	3	2	2	1	2	-	-	-	-	-	-	2	1	1	2	3
23	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
24	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
25	1	-	1	1	1	1	1	1	1	-	-	-	-	-	-	-	1	1	1	1	1
26	2	-	2	1	1	2	1	1	1	2	-	-	-	-	-	-	2	1	1	2	2

Наступним кроком є визначення третього фактору: ймовірностей реалізації загроз. Такий фактор визначається за двома критеріями: частота виникнення загрози в установі та частота виникнення загрози у даній сфері. Розглянемо загрозу 25 – «Втрата доступу до інформації внаслідок стихійних лих», така загроза існує в даній установі та сфері, проте раніше ще не була реалізована, а також вона не є частою, тому ЙЗ буде дорівнювати 1. Оцінки ймовірностей реалізації загроз наведені в таблиці 3.5.

Таблиця 3.5 – Визначення ймовірностей реалізації загроз

Загроза ІБ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Ймовірність	1	3	2	2	3	3	1	2	4	3	3	3	4	2	3	2	3	2	2	3	2	3	1	1	1	3

Наступним кроком є визначення четвертого фактору: показника порушника. Для даної установи існує 4 загальних типи порушника: внутрішній навмисний порушник, внутрішній ненавмисний порушник, зовнішній навмисний порушник та зовнішній ненавмисний порушник. Для певної загрози підбирається відповідний порушник, наприклад: для загрози «Пошкодження інформації внаслідок навмисних помилок персоналу» порушником може бути виключно внутрішній навмисний порушник. Існують загрози для яких врахування ПП є недоцільним, наприклад: «Пошкодження інформації внаслідок стихійних лих». Тому цей фактор враховується при потребі. Оцінки загальних 4-х показників порушників для МКЛ наведені в таблиці 3.6.

Таблиця 3.6 – Визначення показника порушника

Визначення категорії	МП	РК	МВЗ	ЧД	МД	Показник порушника
Внутрішні по відношенню до установи						
Внутрішній навмисний порушник	4	3	4	2	3	4
Внутрішній ненавмисний порушник	1	3	2	2	2	3
Зовнішні по відношенню до установи						
Зовнішній навмисний порушник	4	2	3	1	1	4
Зовнішній ненавмисний порушник	2	2	1	1	1	2

Визначивши оцінки кожного фактору потрібно обчислити загальний рівень ризиків.

3.3 Обчислення загального рівня ризику

Визначивши оцінки всіх факторів можна розрахувати загальний рівень ризику для кожного активу. Обчислення здійснюється за формулою (2.2). Розрахуємо загальний рівень ризику активу «БД інформаційно-телекомунікаційної системи» для загрози «Розкриття інформації внаслідок навмисних помилок персоналу». Для такого випадку цінність активу дорівнює

4, рівень вразливості дорівнює 3, ймовірність реалізації загрози дорівнює 2 та порушник відомий «Внутрішній навмисний порушник», показник якого дорівнює 4. Підставивши дані в формулу, буде отримано результат:

$$ЗРР_{1,16} = 4 \cdot 3 \cdot 2 \cdot 4 = 96$$

Згідно шкали критичності (див. табл. 2.2) показник критичності даного ризику є «Вище середнього». Це свідчить про необхідність негайного прийняття рішення щодо ризику та вживання відповідних заходів захисту задля усунення або зменшення даного ризику. Необхідно виконати обчислення аналогічним чином для кожного активу та загрози. Результати обрахунків загального рівня ризику для пар загроза-актив, для яких показник порушника є недоцільним та для яких слід врахувати показник порушника наведені в таблиці 3.7 та 3.8 відповідно.

Таблиця 3.7 – Результати обрахунку загального рівня ризиків без врахування ПП

Загрози ІБ	Активи установи																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	4	-	3	3	3	2	2	1	3	-	-	-	-	-	-	-	3	3	2	3	3
6	36	-	18	18	27	12	12	6	9	24	-	-	-	-	-	-	18	9	6	18	18
7	4	-	3	3	3	2	2	1	3	-	-	-	-	-	-	-	3	3	2	3	3
8	8	-	6	6	6	4	4	2	6	-	-	-	-	-	-	-	6	6	4	6	6
9	48	-	36	24	24	24	16	8	12	32	-	-	-	-	-	-	24	12	8	24	36
10	36	-	27	18	18	18	12	6	-	24	-	-	-	-	-	-	18	9	6	18	27
13	48	-	36	24	24	24	16	8	12	32	-	-	-	-	-	-	24	12	8	24	36
14	8	-	6	6	6	4	4	2	12	8	8	-	-	-	-	-	6	6	4	6	6
15	36	-	18	18	27	12	12	6	9	24	-	-	-	-	-	-	18	9	6	18	18
18	8	12	6	12	12	4	8	4	-	-	-	-	-	-	-	-	12	6	4	12	6
19	16	-	6	-	-	4	-	-	-	16	-	-	-	-	-	-	-	-	-	6	12
20	36	-	27	18	18	18	12	6	-	24	-	-	-	-	-	-	18	9	6	18	27
23	4	-	3	3	3	2	2	1	3	-	-	-	-	-	-	-	3	3	2	3	3
24	4	-	3	3	3	2	2	1	3	-	-	-	-	-	-	-	3	3	2	3	3
25	4	-	3	3	3	2	2	1	3	-	-	-	-	-	-	-	3	3	2	3	3

Таблиця 3.8 – Результати обрахунку загального рівня ризиків з врахуванням ПП

Загрози ІБ	Активи установи																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2	-	54	27	27	36	18	9	27	72	-	-	-	-	-	-	54	27	18	54	54	-
3	-	48	-	-	32	-	-	-	64	-	-	-	-	-	-	48	48	-	48	72	-
4	-	48	48	48	32	32	16	24	64	-	-	-	-	-	-	48	24	16	48	48	-
5	-	81	54	54	54	36	18	27	72	-	-	-	-	-	-	54	27	18	54	81	-
11	-	108	72	72	72	48	24	-	96	-	96	72	24	24	48	72	36	24	72	108	-
12	-	108	72	72	72	48	24	-	96	-	96	72	24	24	48	72	36	24	72	108	-
16	-	48	48	48	32	32	16	24	64	-	-	-	-	-	-	48	24	16	48	48	-
17	-	81	54	54	54	36	18	27	72	-	-	-	-	-	-	54	27	18	54	81	-
21	-	48	48	48	32	32	16	24	64	-	-	-	-	-	-	48	24	16	48	48	-
22	-	81	54	54	54	36	18	27	72	-	-	-	-	-	-	54	27	18	54	81	-
26	-	54	27	27	36	18	9	27	72	-	-	-	-	-	-	54	27	18	54	54	-

Розрахувавши загальний рівень ризику по кожній парі загроза-актив, можна визначити загальний рівень ризику кожної окремої загрози. Це відбувається шляхом вибору максимальної оцінки загального рівня ризику такої загрози по відношенню до активів. Наприклад, для першої загрози максимальна оцінка ЗРР є для першого активу – 4, то ЗРР для такої загрози буде 4. Результати оцінок без врахування ПП та з врахуванням ПП наведені в таблиці 3.9 та 3.10 відповідно.

Таблиця 3.9 – Визначення загального рівня ризику загроз без врахування ПП

№	Загроза	Загальний рівень ризику загрози
1	Пошкодження інформації внаслідок стихійних лих	4
6	Пошкодження інформації внаслідок вільного доступу до неї	36
7	Пошкодження інформації внаслідок збоїв	4
8	Пошкодження інформації внаслідок поломок	8
9	Пошкодження інформації внаслідок зламу/компрометації паролів	48

Продовження таблиці 3.9

10	Розкриття інформації внаслідок ШПЗ	36
13	Розкриття інформації внаслідок зламу/компроментації паролів	48
14	Розкриття інформації внаслідок підслуховування	12
15	Розкриття інформації внаслідок вільного доступу до неї	36
18	Розкриття інформації внаслідок її викрадення	12
19	Втрата доступу до інформації внаслідок Ddos-атак	16
20	Втрата доступу до інформації внаслідок ШПЗ	36
21	Втрата доступу до інформації внаслідок навмисних помилок персоналу	64
22	Втрата доступу до інформації внаслідок ненавмисних помилок персоналу	108
23	Втрата доступу до інформації внаслідок збоїв	4
24	Втрата доступу до інформації внаслідок поломок	4
25	Втрата доступу до інформації внаслідок стихійних лих	4

Таблиця 3.10 – Визначення загального рівня ризику загроз з врахуванням ПП

№	Загроза	Загальний рівень ризику загрози
2	Пошкодження інформації внаслідок некомпетентності персоналу	72
3	Пошкодження інформації внаслідок ШПЗ	96
4	Пошкодження інформації внаслідок навмисних помилок персоналу	64
5	Пошкодження інформації внаслідок ненавмисних помилок персоналу	108
11	Розкриття інформації внаслідок вішингу	144
12	Розкриття інформації внаслідок фішингу	144
16	Розкриття інформації внаслідок навмисних помилок персоналу	64
17	Розкриття інформації внаслідок ненавмисних помилок персоналу	108
21	Втрата доступу до інформації внаслідок навмисних помилок персоналу	64
22	Втрата доступу до інформації внаслідок ненавмисних помилок персоналу	108
26	Втрата доступу до інформації внаслідок некомпетентності персоналу	72

Згідно шкали критичності (див. табл. 2.1 та 2.2) необхідно визначити рівень критичності оцінки (табл. 3.11 та 3.12).

Таблиця 3.11 – Рівень критичності отриманих оцінок без врахування ПП

Загроза	Загальний рівень ризику загрози	Показник критичності
1	4	Низький
6	36	Вище середнього
7	4	Низький
8	8	Низький
9	48	Високий
10	36	Вище середнього
13	48	Високий
14	12	Нижче середнього
15	36	Вище середнього
18	12	Нижче середнього
19	16	Нижче середнього
20	36	Вище середнього
23	4	Низький
24	4	Низький
25	4	Низький

Таблиця 3.12 – Рівень критичності отриманих оцінок з врахуванням ПП

Загроза	Загальний рівень ризику загрози	Показник критичності
2	72	Середній
3	96	Середній
4	64	Нижче середнього
5	108	Вище середнього
11	144	Вище середнього
12	144	Вище середнього
16	64	Нижче середнього
17	108	Вище середнього
21	64	Нижче середнього
22	108	Вище середнього
26	72	Середній

Оцінивши загальний рівень ризику пар загроза-актив, а також загальний рівень ризику кожної загрози. Для визначення загального рівня інформаційної безпеки установи необхідно перейти до наступної стадії. Вона полягає у переведені бальних оцінок до нечітких значень та побудові логіко-ймовірнісної моделі.

3.4 Побудова логіко-ймовірнісної моделі та оцінка впливу на загальний рівень ІБ

Для переведення бальних оцінок до нечіткого вигляду залучається експерт. У відповідності до шкали (див. табл. 2.3) експерт обирає значення для певної загрози з відповідного діапазону. Наприклад, перша загроза має бальну оцінку 4 та показник критичності «Низький». Експерт обирає з діапазону ймовірностей для показника критичності близьку оцінку, наприклад 0,025. Результати такого переведення наведені в таблиці 3.13 та 3.14.

Таблиця 3.13 – Результати переведення бальних оцінок до вимог логіко-ймовірнісного моделювання без врахування ПП

Загроза	**Загальний рівень ризику загрози**	**Показник критичності**	**Близька оцінка загальної ймовірності виникнення для логіко-ймовірнісного моделювання**
1	4	Низький	0,014
6	36	Вище середнього	0,311
7	4	Низький	0,024
8	8	Низький	0,051
9	48	Високий	0,652
10	36	Вище середнього	0,368
13	48	Високий	0,639
14	12	Нижче середнього	0,061
15	36	Вище середнього	0,302
18	12	Нижче середнього	0,071
19	16	Нижче середнього	0,055
20	36	Вище середнього	0,396
23	4	Низький	0,011
24	4	Низький	0,012
25	4	Низький	0,013

Таблиця 3.14 – Результати переведення бальних оцінок до вимог логіко-ймовірнісного моделювання з врахуванням ПП

Загроза	**Загальний рівень ризику загрози**	**Показник критичності**	**Близька оцінка загальної ймовірності виникнення для логіко-ймовірнісного моделювання**
2	24	Середній	0,163
3	24	Середній	0,154
4	16	Нижче середнього	0,072
5	36	Вище середнього	0,346

Продовження таблиці 3.14

11	36	Вище середнього	0,410
12	36	Вище середнього	0,326
16	16	Нижче середнього	0,063
17	36	Вище середнього	0,336
21	16	Нижче середнього	0,111
22	36	Вище середнього	0,344
26	24	Середній	0,172

Наступним етапом є формалізація таких оцінок. Тут виконується фазифікація (розмиття) та дефазифікація (отримання найбільш достовірного значення). Етап дефазифікації виконується методом центру ваги за формулою (2.7). Всі отримані дані наведено в таблиці 3.15 та 3.16.

Таблиця 3.15 – Результати формалізації оцінок без врахування ПП

Загроза	**Загальна ймовірність виникнення для логіко-ймовірнісного моделювання**
1	0,015
6	0,312
7	0,024
8	0,053
9	0,655
10	0,366
13	0,638
14	0,062
15	0,302
18	0,071
19	0,055
20	0,397
23	0,012
24	0,013
25	0,012

Таблиця 3.16 – Результати формалізації оцінок без врахування ПП

Загроза	**Загальна ймовірність виникнення для логіко-ймовірнісного моделювання**
2	0,162
3	0,153
4	0,071
5	0,347
11	0,410

Продовження таблиці 3.16

12	0,326
16	0,061
17	0,337
21	0,112
22	0,346
26	0,174

Розрахувавши загрози можна будувати логіко-ймовірнісну модель та розраховувати вплив загроз на загальний рівень ІБ. На рис. 3.1 зображено загальний вигляд логіко-ймовірнісної моделі для МКЛ. Розгалуження гілок конфіденційності, цілісності та доступності представлено на рис. 3.2, 3.3 та 3.4 відповідно.

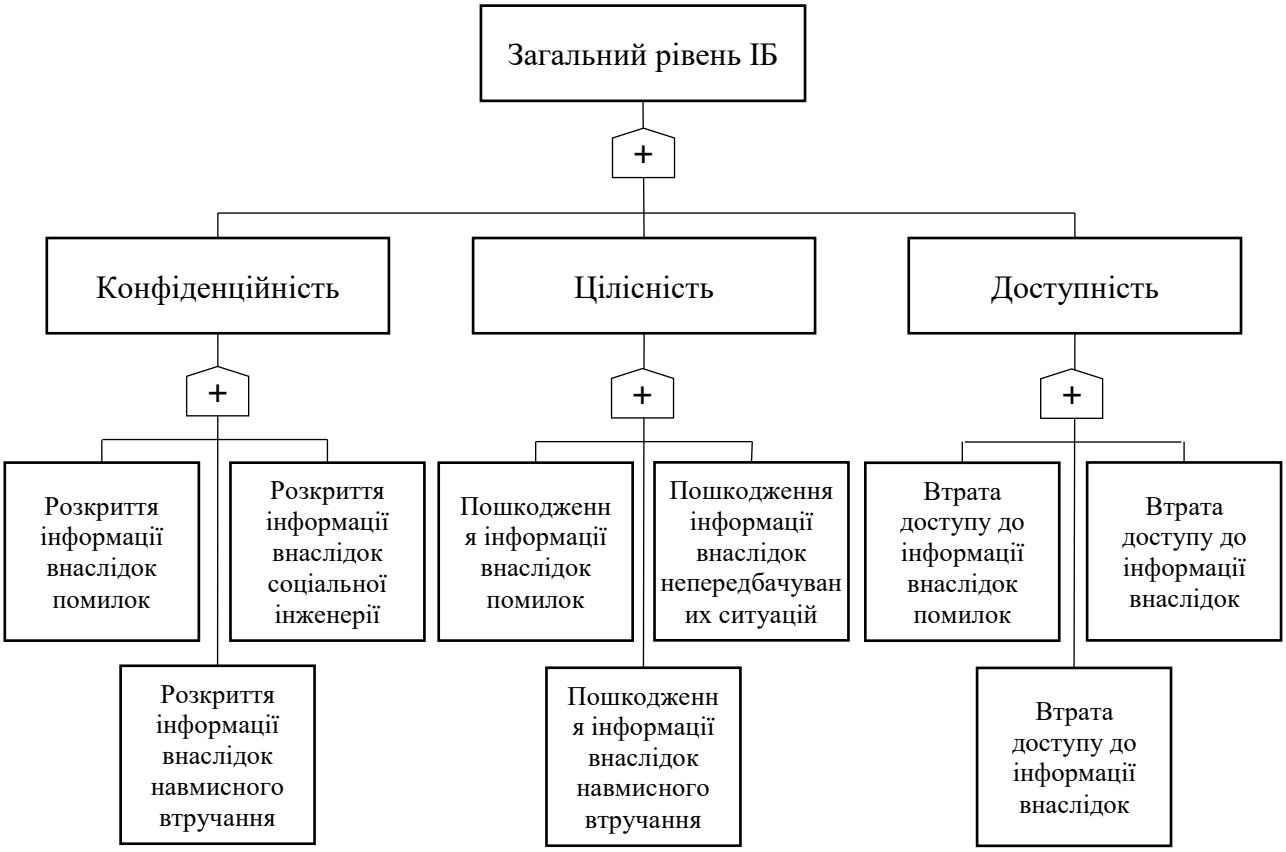


Рисунок 3.1 – Загальний вигляд логіко-ймовірнісної моделі для МКЛ

Загальна модель включає проміжні події всіх гілок, а кожна гілка має окремі базові події (загрози) ідентифіковані в табл. 3.2.

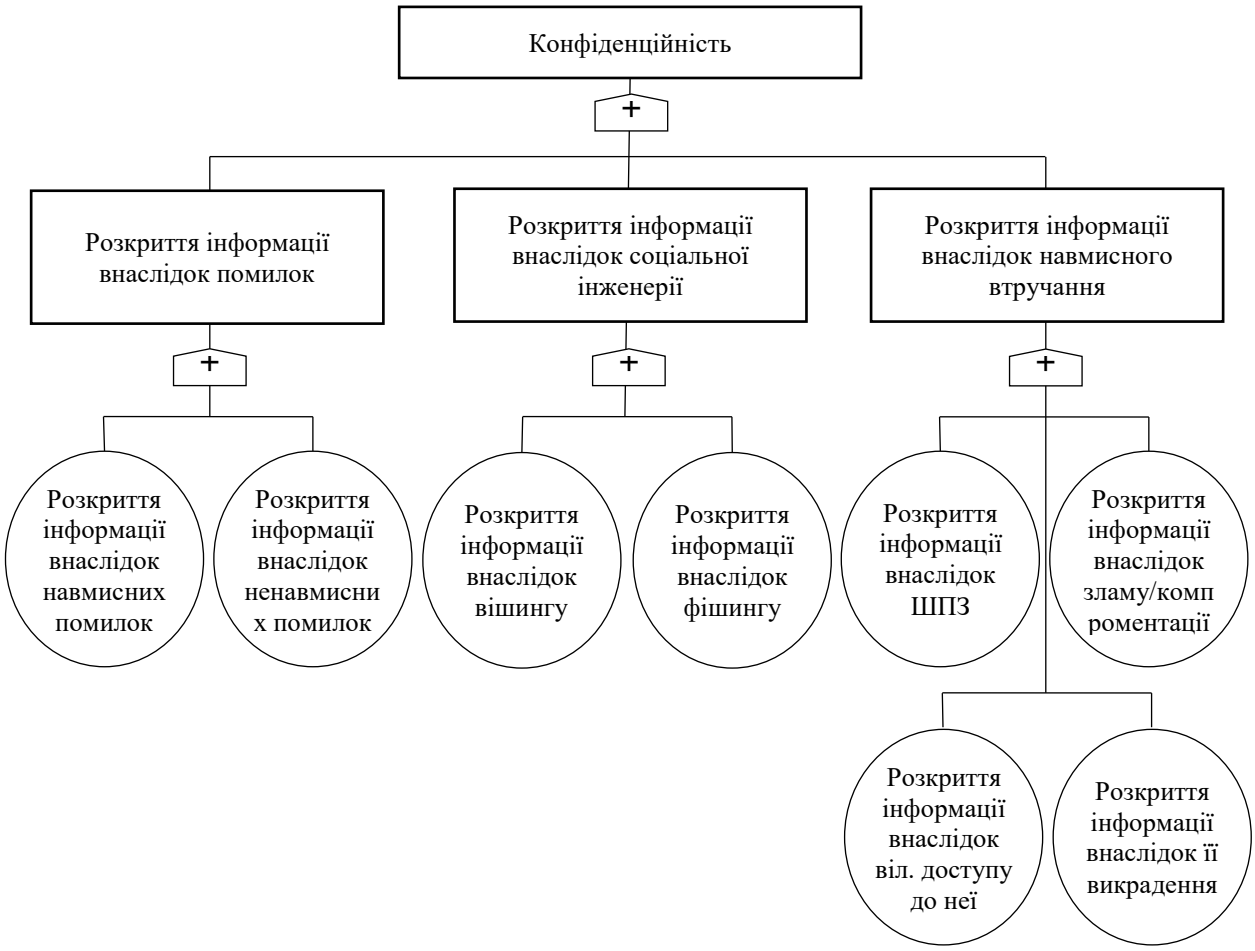


Рисунок 3.2 – Гілка «Конфіденційність»

Гілка «Конфіденційність» включає 3 проміжні події та 8 базових. Для розрахунку впливу таких подій на конфіденційність установи потрібно виконати розрахунки за формулою (2.9), так, як всі події є незалежними, тобто для виконання проміжної події має виконуватись хоча б одна з базових подій (загроз). Розрахунок ймовірності виникнення для проміжної події «Розкриття інформації внаслідок помилок» має вигляд:

$$P_{К1} = 1 - (1 - 0{,}061)(1 - 0{,}337) = 0{,}377$$

Так, як максимальне значення ймовірності виникнення є 1, то 0,377 є досить невисоким результатом. Тобто вплив загроз конфіденційність установи є на невисокому рівні, але потребує розгляду та обробки ризиків. Результати розрахунків ймовірності виникнення проміжних подій для гілки «Конфіденційність» наведені в таблиці 3.17.

Таблиця 3.17 – Результати розрахунків ймовірності виникнення проміжних подій для гілки «Конфіденційність»

Проміжна подія	Ймовірність виникнення
Розкриття інформації внаслідок помилок	0,377
Розкриття інформації внаслідок соціальної інженерії	0,482
Розкриття інформації внаслідок навмисного втручання	0,651

Розрахунок загального впливу загроз на конфіденційність:

$$P_{\text{К}} = 1 - (1 - 0{,}377)(1 - 0{,}482)(1 - 0{,}651) = 0{,}703$$

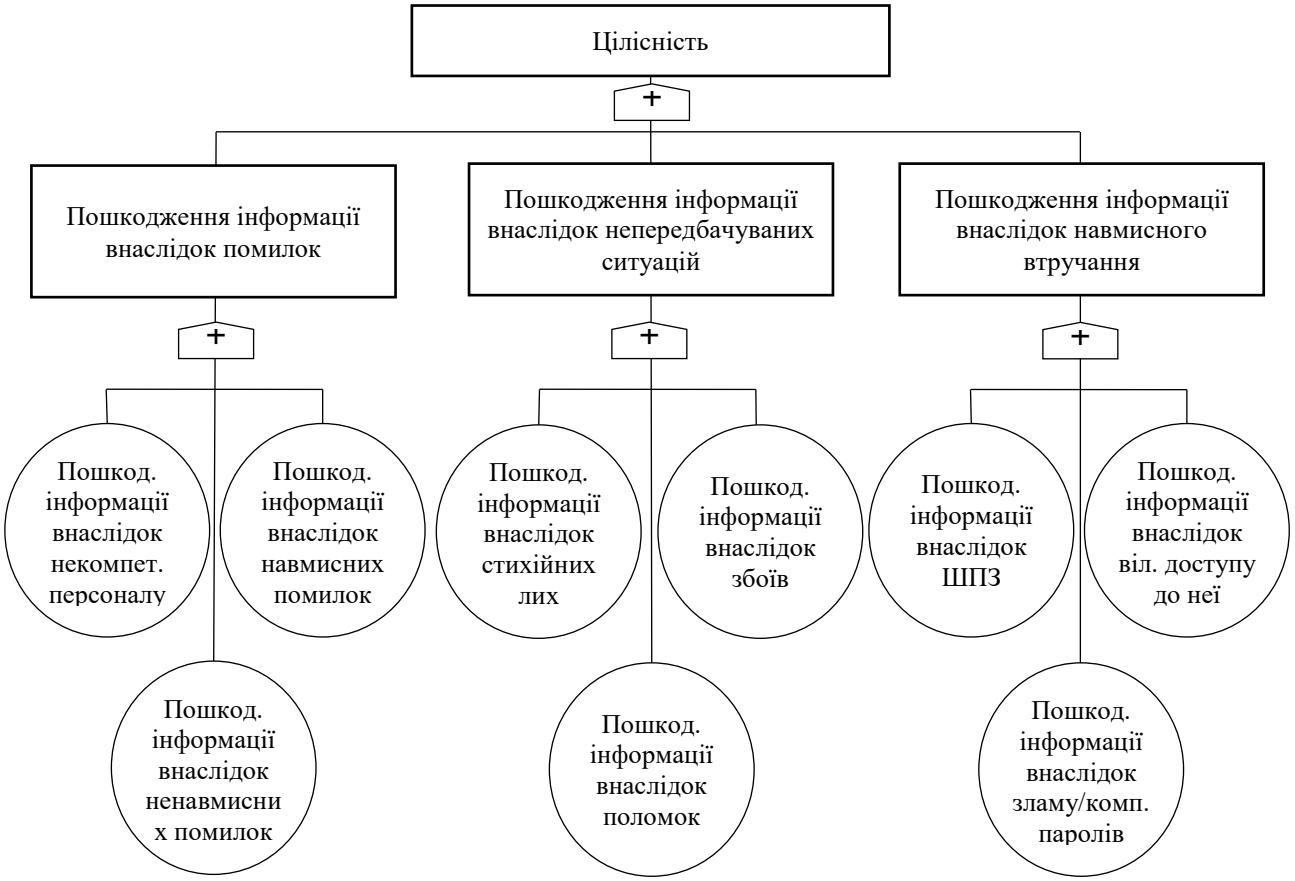


Рисунок 3.3 – Гілка «Цілісність»

Гілка «Цілісність» включає 3 проміжні події та 9 базових. Для розрахунку впливу таких подій на цілісність установи потрібно виконати розрахунки за формулою (2.9), так, як всі події є незалежними. Розрахунок ймовірності виникнення для проміжної події «Пошкодження інформації внаслідок непередбачуваних ситуацій» має вигляд:

$$P_{\text{Ц2}} = 1 - (1 - 0{,}015)(1 - 0{,}024)(1 - 0{,}053) = 0{,}089$$

Так, як максимальне значення ймовірності виникнення є 1, то 0,089 є дуже низьким результатом, що свідчить про малоймовірну реалізацію такого ризику. Результати розрахунків ймовірності виникнення проміжних подій для гілки «Цілісність» наведені в таблиці 3.18.

Таблиця 3.18 – Результати розрахунків ймовірності виникнення проміжних подій для гілки «Цілісність»

Проміжна подія	Ймовірність виникнення
Пошкодження інформації внаслідок помилок	0,491
Пошкодження інформації внаслідок непередбачуваних ситуацій	0,089
Пошкодження інформації внаслідок навмисного втручання	0,798

Розрахунок загального впливу загроз на цілісність:

$$P_{\text{Ц}} = 1 - (1 - 0{,}491)(1 - 0{,}089)(1 - 0{,}798) = 0{,}657$$

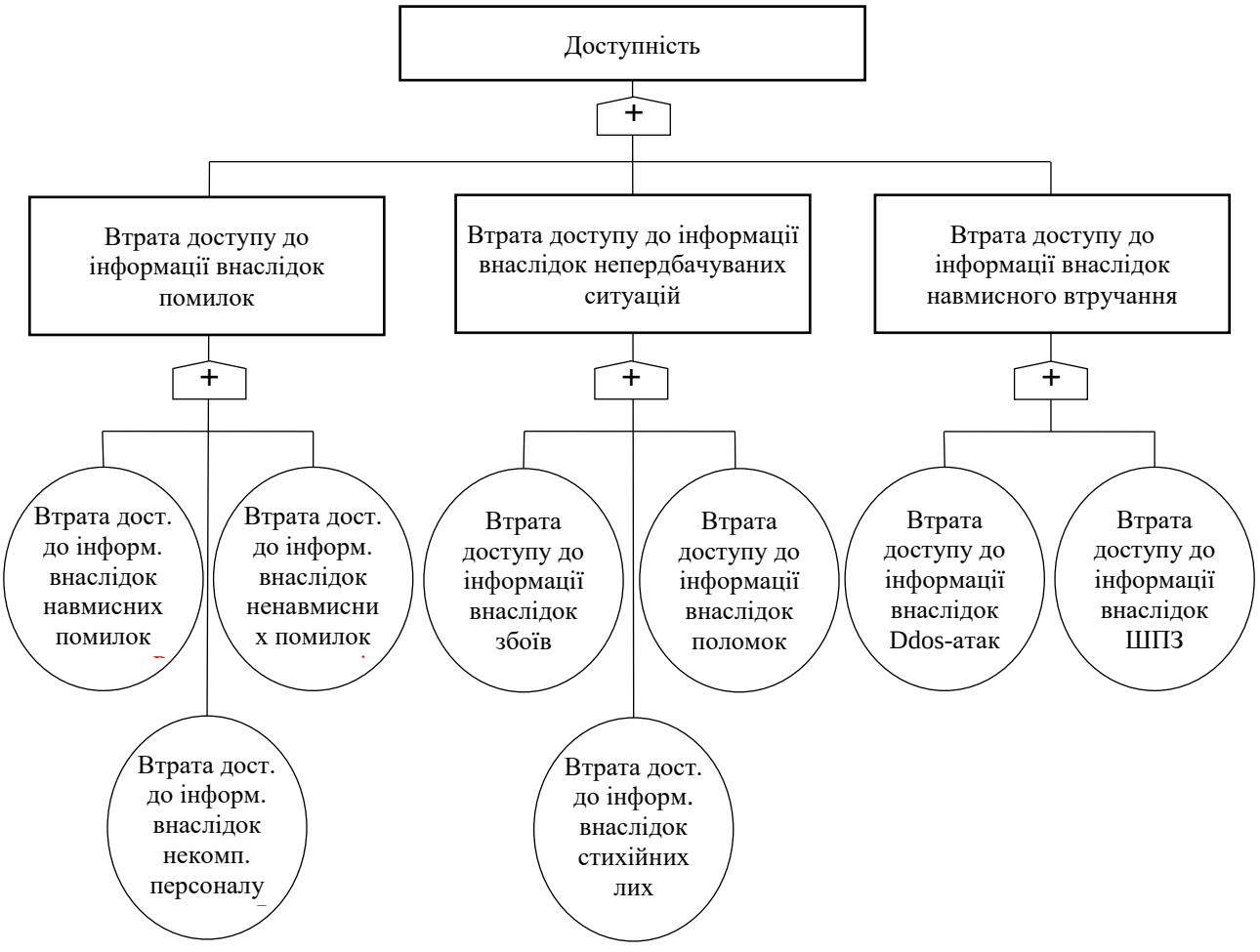


Рисунок 3.4 – Гілка «Доступність»

Гілка «Доступність» включає 3 проміжні події та 8 базових. Для розрахунку впливу таких подій на доступність установи потрібно виконати розрахунки за формулою (2.9), так, як всі події є незалежними. Розрахунок ймовірності виникнення для проміжної події «Втрата доступу до інформації внаслідок навмисного втручання» має вигляд:

$$P_{\text{ДЗ}} = 1 - (1 - 0{,}055)(1 - 0{,}397) = 0{,}430$$

Так, як максимальне значення ймовірності виникнення є 1, то 0,430 є не досить низьким результатом, що свідчить про середню ймовірність реалізації ризику. Результати розрахунків ймовірності виникнення проміжних подій для гілки «Доступність» наведені в таблиці 3.19.

Таблиця 3.19 – Результати розрахунків ймовірності виникнення проміжних подій для гілки «Доступність»

Проміжна подія	Ймовірність виникнення
Втрата доступу до інформації внаслідок помилок	0,520
Втрата доступу до інформації внаслідок непердбачуваних ситуацій	0,036
Втрата доступу до інформації внаслідок навмисного втручання	0,430

Розрахунок загального впливу загроз на доступність:

$$P_{\text{Д}} = 1 - (1 - 0{,}520)(1 - 0{,}036)(1 - 0{,}430) = \ 0{,}361$$

Розрахунок впливу загроз на загальний рівень інформаційної безпеки міської клінічної лікарні:

$$P_{\text{заг.}} = 1 - (1 - 0{,}703)(1 - 0{,}657)(1 - 0{,}361) = \ 0{,}834$$

Тобто наявні ризики інформаційної безпеки медичної установи мають дуже високу ймовірність реалізації, що може призвести до значного порушення рівня інформаційної безпеки, що в свою чергу призведе до матеріальних, репутаційних та інших втрат або й до зупинки функціонування установи. Оцінивши ризики видно, що найбільшу ймовірність реалізації

мають ризики за напрямом конфіденційності, на які слід звернути увагу в першу чергу.

За оцінкою ризиків згідно стандарту ISO 27005 найкритичнішими ризиками було виявлено: «Пошкодження інформації внаслідок зламу/компроментації паролів» та «Розкриття інформації внаслідок зламу/компроментації паролів». Це зв’язано з відсутністю в установі парольної політики, що призводить до вибору працівниками нестійких паролів, зберіганні їх в незахищених місцях та передачі паролів в відкритому вигляді загальнодоступними мережами. Запропонований метод оцінювання ризиків інформаційної безпеки для медичної установи допоміг визначити загальний рівень ІБ установи, а також слабкі місця, на які варто звернути увагу та прийняти необхідні міри задля підвищення рівня ІБ.

3.5 Розробка бази даних

База даних (БД) розроблюється задля подальшого впровадження її до програмних засобів для оцінки ризиків інформаційної безпеки медичної установи. БД містить наступні сутності:

1. companies – таблиця для зберігання компаній|, для яких виконується оцінка ризиків інформаційної безпеки. Така таблиця містить наступні властивості:
   - id – унільний ідентифікатор компанії;
   - name – ім’я компанії:
   - created_at – дата створення компанії;
2. assets – таблиця в якій містяться всі активи утанови. Активи в подальшому пов'язуються з компанією для цього використовується зведена таблиця: company_assets, тим самим реалізується відношення many-to-many. Додатково зведена таблиця містить в собі властиві score, цим самим дозволяючи встановити для кожного активу компанії його рівень критичності. Така таблиця містить наступні властивості:

– id – унільний ідентифікатор активу;

– name – назва активу:

– created_at – дата створення активу.

Проміжна таблиця ж складається з наступних властивостей:

– company_id – ідентифікатор компанії з таблиці companies;

– asset_id – ідентифікатор активу з таблиці assets;

– score – рівень критичності активу;

3. violators – така таблиця описує перелік можливих порушників. По аналогію з активами та компаніями використовує зведену таблицю company_violators з реалізацією відношення many-to-many. В зведеній таблиці такоє є можливість вказати відповідний score для кожного з порушників в контексті компанії. Така таблиця містить наступні властивості:

– id – унільний ідентифікатор порушника;

– name – ім’я порушника;

– type – тип порушника;

– created_at – дата запису порушника.

Проміжна таблиця складається з таких властивостей:

– violator_id – ідентифікатор порушника;

– company_id – ідентифікатор компанії;

– score – оцінка потенційного ризику.

4. threats – таблиця описує список можливих загроз. Загроза відповідно пов’язується з активами компаніями, що дозволяє встановити відповідний score зі сторони загрози до кожного активу компанії. Зв’язок по аналогії з попередніми таблицями реалізує many-to-many з використанням проміжної таблиці company_asset_threats. Така таблиця містить наступні властивості:

– id – унільний ідентифікатор загрози;

– name – загальна назва загрози;

– created_at – дата запису загрози.

Проміжна таблиця ж складається з наступних властивостей:

– company_asset_id – ідентифікатор активу в контексті компанії;

– threat_id – ідентифікатор загрози;

– score – оцінка загрози.

Загальна схема зв’язків бази даних зображена на рис. 3.5.

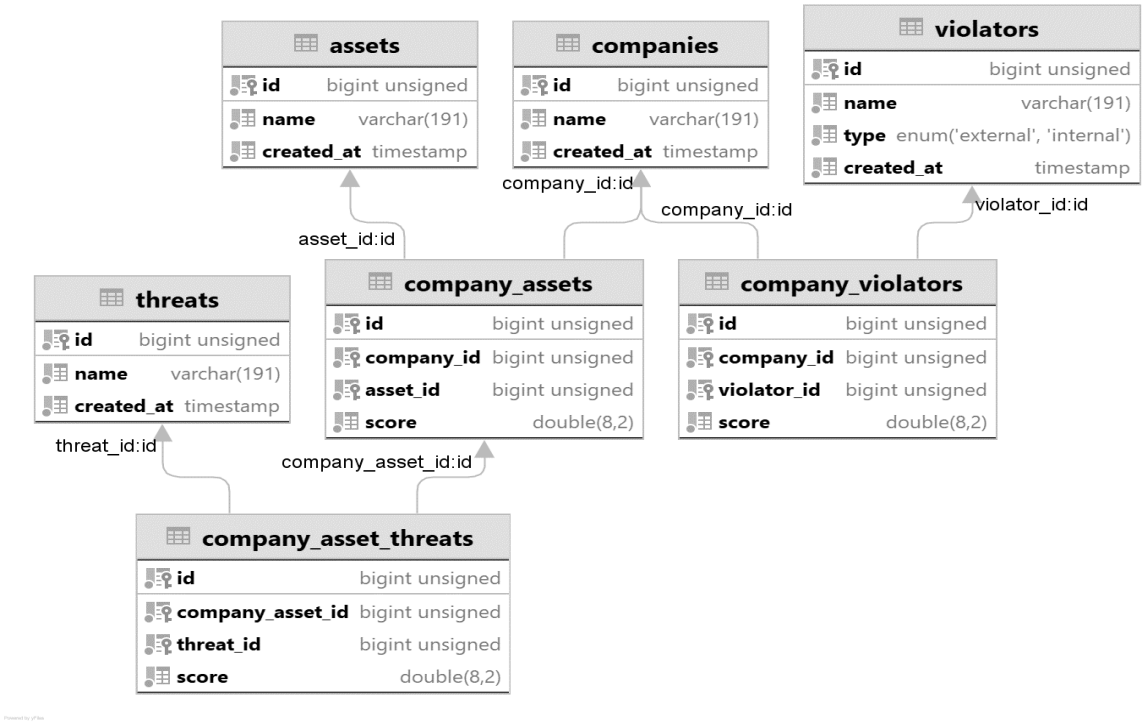


Рисунок 3.5 – Загальна схема зв’язків бази даних

Приклад опису схеми таблиць assets та companies разом з відношенням між ними в контексті СКБД MySQL:

```
CREATE TABLE `assets` (
  `id` bigint unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(191) COLLATE utf8mb4_unicode_ci NOT
NULL,
  `created_at` timestamp NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4
COLLATE=utf8mb4_unicode_ci;
CREATE TABLE `companies` (
  `id` bigint unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(191) COLLATE utf8mb4_unicode_ci NOT
NULL,
  `created_at` timestamp NOT NULL,
  PRIMARY KEY (`id`)
```

```
    )      ENGINE=InnoDB      DEFAULT      CHARSET=utf8mb4
COLLATE=utf8mb4_unicode_ci;
    CREATE TABLE `company_assets` (
      `id` bigint unsigned NOT NULL AUTO_INCREMENT,
      `company_id` bigint unsigned NOT NULL,
      `asset_id` bigint unsigned NOT NULL,
      `risk` double(8,2) NOT NULL DEFAULT '0.00',
      PRIMARY KEY (`id`),
     KEY`company_assets_company_id_foreign` (`company_id`),
      KEY `company_assets_asset_id_foreign` (`asset_id`),
      CONSTRAINT `company_assets_asset_id_foreign` FOREIGN
KEY (`asset_id`) REFERENCES `assets` (`id`) ON DELETE
CASCADE,
       CONSTRAINT        `company_assets_company_id_foreign`
FOREIGN KEY (`company_id`) REFERENCES `companies` (`id`) ON
DELETE CASCADE
    )      ENGINE=InnoDB      DEFAULT      CHARSET=utf8mb4
COLLATE=utf8mb4_unicode_ci;
```

Створення ролі “аудитор” в MySQL:

```
CREATE ROLE 'auditor';
```

Надання необхідних привілеїв (читання, записи, оновлення та видалення) для ролі «аудитор»:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON security_assestment.*
TO auditor';
```

Створення нового користувача з іменем “експерт”:

```
CREATE USER expert'@'localhost' IDENTIFIED BY ‘Exp3rToP!';
```

Надання ролі аудитора для експерта:

```
GRANT ‘auditor' TO 'expert'@'localhost';
```

Створивши базу даних, її можна використовувати в майбутньому для автоматизації оцінки ризиків. Це означає, що запропонована база даних є універсальною та може використовуватись для будь-якої організації задля розробки власного програмного забезпечення. Структура бази даних передбачає можливість додавання своїх активів та загроз, що робить її придатною для використання не лише конкретною установою.

Отже, виконавши розрахунки за запропонованим методом видно, що метод є ефективним для оцінки ризиків інформаційної безпеки медичної установи та оцінки її загального рівня в цілому. Необхідно визначити доцільність такої розробки за допомогою економічних розрахунків.

4 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини магістерської кваліфікаційної роботи є обґрунтування економічної доцільності методу оцінювання ризиків інформаційної безпеки для медичної установи. Для виконання поставленої мети необхідно: оцінити комерційний потенціал розробки; оцінити витрати на виконання та впровадження результатів наукової роботи; розрахувати ціну та чистий прибуток реалізації результатів розробки; розрахувати період окупності наукової роботи та результатів розробки.

4.1 Оцінювання комерційного потенціалу розробки (технологічний аудит розробки)

Провести технологічний аудит було залучено трьох незалежних експертів: Баришев Ю. В, Куперштейн Л. М., Войтович О. П. Кожен з експертів повинен ознайомитися з запропонованою розробкою та заповнити таблицю, яка визначає рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можливу оцінку в балах.

Після виконання цього, підраховується середньоарифметична сума балів та визначається який рівень комерційного потенціалу має нова розробка. Здійснюємо оцінювання комерційного потенціалу розробки за відповідними критеріями, наведеними в додатку Б. Результати оцінювання комерційного потенціалу розробки наведено в таблиці 4.1.

Таблиця 4.1 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали експерта		
	Баришев Ю. В,	Куперштейн Л. М.	Войтович О. П.
	Бали, виставлені експертами:		
1	2	3	3
2	2	2	2
3	4	3	3
4	3	2	2

Продовження таблиці 4.1

5	4	4	4
6	2	2	2
7	3	4	3
8	3	4	3
9	3	3	3
10	4	3	4
11	4	4	4
12	3	4	3
Сума балів	$СБ_1$=37	$СБ_2$=38	$СБ_3$=36
Середньоарифметична сума балів $\overline{СБ}$	$\overline{\text{СБ}} = \frac{\sum_1^i \text{СБ}_\text{i}}{i} = \frac{37 + 38 + 36}{3} = 37$		

За даними таблиці 4.1 робимо висновок щодо рівня комерційного потенціалу розробки методу оцінювання ризиків інформаційної безпеки для медичної установи. При цьому використано рекомендації, що наведено у таблиці 4.2.

Таблиця 4.2 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів	Рівень комерційного потенціалу
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-50	Високий

Отже, відповідно до результатів оцінювання експертами рівень комерційного потенціалу розробки методу оцінювання ризиків інформаційної безпеки для медичної установи становить вище середнього.

Оцінювання рівня якості розробки методу оцінювання ризиків інформаційної безпеки для медичної установи здійснюється з метою порівняльного аналізу та визначення найбільш ефективного, з технічної точки зору, варіанта інженерного рішення.

Рівень якості – кількісна характеристика міри придатності певного виду продукції для задоволення конкретного попиту на неї при порівнянні з відповідними базовими показниками за фіксованих умов споживання.

Абсолютний рівень якості розробки методу оцінювання ризиків інформаційної безпеки для медичної установи знаходимо обчисленням обраних для вимірювання показників, не порівнюючи їх із відповідними показниками аналогічних методів.

Для визначення рівня якості розробки обрано систему параметрів: кількість факторів впливу, складність розрахунків, кількість виконання необхідних етапів.

Визначаємо величину параметрів якості в балах та встановлюємо граничні значення (кращі, гірші, середні). Дані для кожного параметра представлено у таблиці 4.3.

Таблиця 4.3 – Основні параметри методу оцінювання ризиків інформаційної безпеки для медичної установи

Параметри	Абсолютне значення параметра			Коефіцієнт вагомості параметра
	Краще +5…+4	Середнє +3	Гірше +1..+2	
Кількість факторів впливу	4			0,7
Складність розрахунків		3		0,2
Кількість виконання необхідних етапів			2	0,1

Із врахуванням коефіцієнтів вагомості відповідних параметрів можна визначити абсолютний рівень якості інноваційного рішення за формулою:

$$К_{я.а.} = \sum_{i=1}^{n} Рн_i \cdot a_i, \quad (4.1)$$

де $Рн_i$ – числове значення i-го параметра інноваційного рішення,

n – кількість параметрів інноваційного рішення, що прийняті для оцінювання,

a_i – коефіцієнт вагомості відповідного параметра (сума коефіцієнтів вагомості всіх параметрів повинна дорівнювати 1).

Отже, абсолютний рівень якості методу оцінювання ризиків інформаційної безпеки для медичної установи складає 3,6 бали.

Одночасно визначаємо відносний рівень якості розробленого методу оцінювання ризиків інформаційної безпеки для медичної установи, шляхом порівнюючи показники з абсолютними показниками якості найліпших аналогів, що представлено у таблиці 4.4.

Таблиця 4.4 – Порівняння основних параметрів методу оцінювання ризиків інформаційної безпеки для медичної установи та товару-конкурента

Параметри	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (конкурент)	Новий		
Кількість факторів впливу	3	4	3	0,7
Складність розрахунків	2	3	0,7	0,2
Кількість виконання необхідних етапів	6	8	1	0,1

Відносний рівень якості методу оцінювання ризиків інформаційної безпеки для медичної установи визначаємо за формулою:

$$К_{я.в.} = \sum_{i=1}^{n} q_i \cdot a_i, \quad (4.2)$$

де q_i – відносний показник якості.

За розрахунками відносний рівень якості методу оцінювання ризиків інформаційної безпеки для медичної установи складає 2,34. Це означає, що нова розробка якісніша на 71% відносно товару-аналога.

У найширшому розумінні конкурентоспроможність товару – це можливість його успішного продажу на певному ринку і в певний проміжок часу. Водночас конкурентоспроможною можна вважати лише однорідну продукцію з технічними параметрами і техніко-економічними показниками, що ідентичні аналогічним показникам уже проданого товару. Для того, щоб високоякісний товар був одночасно і конкурентоспроможним, він має відповідати критеріям оцінювання споживачів конкретного ринку в конкретний період часу.

Дані для розрахунку загального показника конкурентоспроможності розробки необхідно занести до таблиці 4.5.

Таблиця 4.5 – Нормативні, технічні та економічні параметри методу оцінювання ризиків інформаційної безпеки для медичної установи та товару-конкурента

Параметри	Варіанти		Відносний показник якості	Коефіцієнт вагомості параметра
	Базовий (конкурент)	Новий		
Кількість факторів впливу	3	4	3	0,7
Складність розрахунків	2	3	0,7	0,2
Кількість виконання необхідних етапів	6	8	1	0,1
Ціна за продукт, грн	2000	1500	0,75	-

Загальний показник конкурентоспроможності розробки ($К$) з урахуванням вищезазначених груп показників визначаємо за формулою:

$$К = \frac{I_{Т.П.}}{I_{Е.П.}} = \frac{2,34}{0,75} = 3,12, \quad (4.3)$$

де $I_{Т.П.}$ – індекс технічних параметрів (відносний рівень якості інноваційного рішення);

$I_{Е.П.}$ – індекс економічних параметрів розрахований нижче за формулою:

$$I_{Е.П.} = \frac{РН_{EI}}{РБ_{EI}} = \frac{1500}{2000} = 0,75, \quad (4.4)$$

де $РН_{EI}$, $РБ_{EI}$ – економічні параметри (ціна придбання та споживання товару) відповідно нового та базового товарів.

Згідно розрахунків загальний показник конкурентоспроможності 3,12, що свідчить про більшу конкурентну спроможність методу оцінювання

ризиків інформаційної безпеки для медичної установи у порівнянні з товаром-аналогом.

4.2 Прогнозування витрат на виконання науково-дослідної та конструкторсько-технологічної роботи

4.2.1 Розрахунок витрат, що стосуються виконавців розробки методу оцінювання ризиків інформаційної безпеки для медичної установи

Команда розробки методу оцінювання ризиків інформаційної безпеки для медичної установи складається з керівника, розробника та експерта.

Основна заробітна плата для розробників (дослідників) *Зо*, якщо вони працюють в наукових установах бюджетної сфери визначається за формулою:

$$З_О = \frac{M}{T_p} t \qquad (4.5)$$

де M – місячний посадовий оклад розробника;

T_p – кількість робочих днів у місяці, T_p = 22 дні;

t – число днів роботи.

Розрахунки заробітної плати для розробників наведені в таблиці 4.6.

Таблиця 4.6 – Розрахунки основної заробітної плати розробників

Працівник	Оклад М, грн.	Оплата за робочий день, грн.	Число днів роботи, t	Витрати на оплату праці, грн.
Керівник	24000	1090,9	7	7636,3
Розробник	22000	1000	15	15000
Всього:				22636,3

Основна заробітна плата робітників *Зр*, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_Р = \sum_{i=1}^{n} t_i \cdot C_i \ , \qquad (4.6)$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин;

n – число робіт по видах та розрядах;

C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$\mathrm{C}_i = \frac{M_M \cdot K_i}{T_\mathrm{р} \cdot T_\mathrm{ЗМ}}, \qquad (4.7)$$

де M_M – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн.,

K_i – тарифний коефіцієнт робітника відповідного розряду,

$T_р$ = 22 дні;

$T_{зм}$ – тривалість зміни, $T_{зм}$ =8 годин.

Таблиця 4.7 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	53,92	1,46	431,36
Тестування	3	4	49,48	1,34	148,44
Впровадження	2	2	38,03	1,03	76,06
Всього					655,86

Додаткова заробітна плата $З_Д$ всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як 10-12% від суми основної заробітної плати всіх розробників та робітників. Додаткова заробітна плата розраховується за формулою:

$$\mathrm{З_Д} = 0.1 \cdot (\mathrm{З_О} + \mathrm{З_Р}) = 0{,}1 \cdot (22636{,}3 + 655{,}86) = 2329{,}216 \text{ (грн.)} \qquad (4.8)$$

Нарахування на заробітну плату $Н_{ЗП}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$Н_{ЗП} = (З_О + З_Р + З_Д) \cdot \frac{\beta}{100}, \quad (4.9)$$

де $З_О$ – основна заробітна плата розробників, грн.;

$З_р$ – основна заробітна плата робітників, грн.;

$З_Д$ – додаткова заробітна плата розробників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

$Н_{ЗП} = (22636{,}3 + 655{,}86 + 2329{,}216) \cdot 0{,}22 = 5636{,}7$ (грн.)

Розрахунок амортизаційних відрахувань виконується за такою формулою:

$$А = \frac{Ц}{t_В} \cdot \frac{Т}{12} \quad (4.10)$$

де $Ц$ – балансова вартість обладнання, грн;

$Т$ – термін використання ($Т$ = 2 місяці);

$t_в$ – корисний час використання ($t_в$ для комп'ютера становить 4 роки).

Під час виконання розробки використовувався ноутбук вартістю 27000 грн. Амортизаційні відрахування для ноутбуку представлені у таблиці 4.8.

Таблиця 4.8 - Амортизаційні відрахування

Найменування	Ціна, грн.	Корисний час використання, роки	Термін використання, міс.	Сума амортизації, грн.
Ноутбук	27000	4	2	1125
Всього	1125			

Витрати на силову електроенергію розраховуються за формулою:

$$В_Е = В \cdot П \cdot Ф \cdot К_П \quad (4.11)$$

де $В$ – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

$П$ – установлена потужність комп'ютеру ($П$=0,74 кВт);

$Ф$ – фактична кількість годин роботи комп'ютеру ($Ф$=176=(7+15)*8 год);

$К_П$ – коефіцієнт використання потужності ($К_П$ <1, $К_П$ = 0,8).

Відповідно до формули (4.11) витрати на силову електроенергію:

$$В_Е = 4{,}62 \cdot 0{,}74 \cdot 176 \cdot 0{,}8 = 481{,}36 \text{ (грн.)}$$

Інші витрати $В_{ін}$ можна прийняти як 100-300% від суми основної заробітної плати розробників, які виконували роботу, тобто:

$$Він = 1 \cdot (22636{,}3 + 655{,}86) = 23292{,}16 \text{ (грн.)} \qquad (4.12)$$

Сума усіх попередніх витрат дає загальні витрати на виконання роботи. Усі витрати складають:

$$В = 22636{,}3+655{,}86+2329{,}216+ 5636{,}7 + 481{,}36 + 23292{,}16 + 1125 = \\ = 56156{,}59 \text{ (грн.)}$$

Розрахунок загальної вартості наукової розробки $В_{заг}$ за формулою:

$$В_{заг} = \frac{В}{\alpha}, \qquad (4.13)$$

де α = 1 – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних одиницях.

$$В_{заг} = \frac{56156{,}59}{1} = 56156{,}59 \text{ (грн.)}$$

Прогнозування загальних витрат $ЗВ$ на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою:

$$З_В = \frac{В_{заг}}{\beta} \qquad (4.14)$$

Розрахунок прогнозованих загальних витрат:

$$З_В = \frac{56156{,}59}{0{,}7} = 80223{,}7 \text{ (грн.)}$$

4.2.2 Розрахунок собівартості розробки методу оцінювання ризиків інформаційної безпеки для медичної установи

Витрати на силову електроенергію розраховуються за формулою:

$$В_Е = В \cdot П \cdot Ф \cdot К_П \quad (4.15)$$

де *В* – вартість 1кВт-години електроенергії (В=4,62 грн/кВт);

П – установлена потужність комп'ютеру (*П*=0,74 кВт);

Ф – фактична кількість годин роботи комп'ютеру (*Ф*=22*8=176 год);

$К_П$ – коефіцієнт використання потужності ($К_П$ <1, $К_П$ = 0,8).

Відповідно до формули (4.14) витрати на силову електроенергію:

$$В_Е = 4{,}62 \cdot 0{,}74 \cdot 176 \cdot 0{,}8 = 481{,}36 \text{ (грн.)}$$

Основна заробітна плата робітників *Зр*, якщо вони беруть участь у виконанні даного етапу роботи і виконують роботи за робочими професіями у випадку, коли вони працюють в наукових установах бюджетної сфери, розраховується за формулою:

$$З_Р = \sum_{i=1}^{n} t_i \cdot C_i, \quad (4.16)$$

де t_i – норма часу (трудомісткість) на виконання конкретної роботи, годин;

n – число робіт по видах та розрядах;

C_i – погодинна тарифна ставка робітника відповідного розряду, який виконує дану роботу. C_i визначається за формулою:

$$С_i = \frac{M_M \cdot K_i}{T_р \cdot T_{ЗМ}}, \quad (4.17)$$

де M_M – розмір мінімальної заробітної плати за місяць, грн.; в 2021 році мінімальна заробітна плата становить – 6500 грн.,

K_i – тарифний коефіцієнт робітника відповідного розряду,

$T_р$ = 22 дні;

$T_{зм}$ – тривалість зміни, $T_{зм}$ =8 годин.

Таблиця 4.9 – Заробітна плата робітників

Найменування робіт	Трудомісткість, н-год.	Розряд роботи	Погодинна тарифна ставка	Тариф. коеф.	Величина, грн.
Розробка	8	5	53,92	1,46	431,36
Тестування	3	4	49,48	1,34	148,44
Впровадження	2	2	38,03	1,03	76,06
Всього					655,86

Додаткова заробітна плата $З_Д$ всіх робітників, які брали участь у виконанні даного етапу роботи, розраховується як 10-12% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$З_Д = 0.1 \cdot (З_Р) = 0{,}1 \cdot (655{,}86) = 65{,}58 \text{ (грн.)} \quad (4.18)$$

Нарахування на заробітну плату $Н_{ЗП}$ розраховується як 22% від суми основної та додаткової заробітної плати:

$$Н_{ЗП} = (З_Р + З_Д) \cdot \frac{\beta}{100} = (655{,}86 + 65{,}58) \cdot 0{,}22 = 158{,}71 \text{ (грн.)} \quad (4.19)$$

де $З_р$ – основна заробітна плата робітників, грн.;

$З_Д$ – додаткова заробітна плата робітників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне страхування.

Загальновиробничі витрати з рахунку на одиницю продукції можна розрахувати за нормативами відносно до основної заробітної плати основних робітників, які виготовляють продукцію :

$$ЗВВ = Н_В \cdot З_О, \quad (4.20)$$

Норматив загальновиробничих витрат для програмних продуктів становить 230-270%.

$$ЗВВ = 2{,}7 * 655{,}86 = 1770{,}82 \text{ (грн.)}$$

Сума попередніх витрат утворює виробничу собівартість розробки.

$$S_В = 481{,}36 + 655{,}86 + 65{,}58 + 158{,}71 + 1770{,}82 = 3132{,}33 \text{ (грн.)} \quad (4.21)$$

Виробнича собівартість розробки становить 3132,33 грн.

4.3 Розрахунок мінімальної ціни та чистого прибутку від реалізації розробки методу оцінювання ризиків інформаційної безпеки для медичної установи

Ціна – це грошовий вираз вартості товару (продукції, послуги). Вона завжди коливається навколо ціни виробництва (перетвореної форми вартості одиниці товару, що дорівнює сумі витрат виробництва й середнього прибутку) та відображає рівень суспільне необхідних витрат праці.

Виходячи з того, що розробки, як правило, приймаються та впроваджуються за завданням замовника, або коли результатом розробки є продукція, що підлягає державному регулюванню, то нижню межу ціни реалізації розробки можна розрахувати за формулою:

$$Ц = S_В \cdot (1 + \frac{P}{100}) \cdot (1 + \frac{\omega}{100}), \quad (4.22)$$

де S_B – виробнича собівартість інноваційного рішення, грн.;

P – норматив рентабельності узгоджений із замовником або встановлений державою, (Р=30…60%);

ω – ставка податку на додану вартість, % (з осені 2021 року $\omega = 20\%$).

$$Ц = 3132{,}33 \cdot (1 + \frac{60}{100}) \cdot (1 + \frac{20}{100}) = 6014{,}07 \text{ (грн.)}$$

Із врахуванням коефіцієнта якості ціна розробки становить 21650,65 грн.

Чистий прибуток від реалізації розробки можна розрахувати за формулою:

$$П = (Ц - \frac{(Ц - МР) \cdot f}{100} - S_B - \frac{q \cdot S_B}{100}) \cdot (1 - \frac{h}{100}) \cdot РП, \quad (4.23)$$

де *Ц* – ціна розробки, грн.;

МР – вартість матеріальних та інших ресурсів, що були придбані виробником для виготовлення розробки (*МР*=(0,1…0,2) *Ц*), грн.;

f – зустрічна ставка податку на додану вартість, %; S_B – виробнича собівартість розробки, грн.;

q – норматив, який визначає величину адміністративних витрат, витрат на збут та інші операційні витрати, % (рекомендовано *q*=5…10%);

h – ставка податку на прибуток, %,

РП – прогнозований попит продажів.

$$П = (21650{,}65 - \frac{(21650{,}65 - 21650{,}65 \cdot 0{,}2) \cdot 14}{100} - 3132{,}33 - \frac{5 \cdot 3132{,}33}{100}) \cdot (1 - \frac{18}{100}) \cdot 2 = 28136{,}41 \text{ (грн.)},$$

Прогнозований чистий прибуток від реалізації розробки складає 26136,41 грн.

4.4 Розрахунок терміну окупності коштів вкладених у наукову розробку методу оцінювання ризиків інформаційної безпеки для медичної установи

Термін окупності вкладених у реалізацію наукового проекту інвестицій розраховано за формулою:

$$T_{ОК} = \frac{ЗВ}{П} = \frac{80223{,}7}{28136{,}41} = 2{,}85 \text{ (роки)} \quad (4.24)$$

Оскільки $T_{ОК} < 3$ років, то фінансування наукової розробки методу оцінювання ризиків інформаційної безпеки для медичної установи є доцільним.

4.5 Висновки до розділу

Отже, у цьому розділі виконано обґрунтування економічної доцільності проведення наукового дослідження та розробки методу оцінювання ризиків інформаційної безпеки для медичної установи.

Рівень комерційного потенціалу розробки методу оцінювання ризиків інформаційної безпеки для медичної установи становить вище середнього.

На основі параметрів методу оцінювання ризиків інформаційної безпеки для медичної установи визначено абсолютний рівень якості методу, який складає 3,6 бали.

Відносний рівень якості розробки, що складає 2,34. Це означає, що нова розробка якісніша на 71% відносно товару-аналога. Загальний показник конкурентоспроможності становить 3,12, що свідчить про більшу конкурентну спроможність методу оцінювання ризиків інформаційної безпеки для медичної установи у порівнянні з товаром-аналогом.

Загальні витрати, що стосуються виконавців розробки склали 80223,7 грн, а собівартість розробки – 3132,33 грн.

Розраховано мінімальну ціну та прогнозований чистий річний прибуток від реалізації розробки, які склали 21650,65 грн. та 28136,41 грн. відповідно. Термін окупності продукції вкладених інвестицій складає 2,85 роки, що свідчить про доцільність фінансування розробки.

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи було розроблено метод оцінювання ризиків інформаційної безпеки для медичної установи.

Проаналізувавши існуючі методи, підходи та засоби для оцінки ризиків інформаційної безпеки було виявлено, що їх є велика кількість, проте вони є не досконалими, так, як можуть оцінювати тільки окремі загрози, але важливо знати загальний рівень інформаційної безпеки установи.

У ході виявленої проблематики даної сфери було запропоновано метод оцінювання ризиків інформаційної безпеки для медичної установи, який передбачає дві стадії:

1) Оцінка загального рівня ризику всіх наявних активів.

2) Оцінка впливу загроз на напрями ІБ та на загальний рівень ІБ установи.

Перша стадія виконується за допомогою методу оцінювання ризиків, представленого в стандарті ISO 27005. На даній стадії обчислюється загальні рівні ризиків за допомогою врахування та оцінки наступних факторів:

- цінність активу;
- рівень вразливості для співвідношення загроз та активів;
- ймовірність реалізації загрози для кожного активу;
- показник порушника.

Такі дані допомагають у виконанні другої стадії, а саме: оцінені раніше рівні ризиків перетворюються до вигляду логіко-ймовірнісного моделювання, яке власне є ключовим при оцінці впливу загроз на напрями ІБ та на загальний рівень ІБ установи. Після перетворення за відповідними шкалами, розраховуються впливи ризиків на напрями ІБ та на загальний рівень ІБ.

Метод було застосовано на практиці для медичної установи типу «міська клінічна лікарня». Було оцінено ризики для даної установи та виявлено її загальний рівень ІБ. Оцінювання ризиків допомогло виявити вразливі місця, на які слід звернути увагу та прийняти певні заходи та засоби захисту.

Розроблено базу даних загальних активів та загроз інформаційної безпеки для медичних установ типу «міська клінічна лікарня». Така база даних містить типові активи та загрози та передбачена для подальшого включення її до програмних засобів для оцінки ризиків інформаційної безпеки медичних установ.

У економічні частина магістерської кваліфікаційної роботи було оцінено комерційний потенціал розробки, загальні витрати на впровадження та виконання результатів наукової роботи, розраховано чистий прибуток та ціну реалізації щодо результатів розробки, а також розраховано період окупності результатів розробки та наукової роботи. В ході результатів розрахунків було виявлено доцільність даної розробки, так як показник якості розробки показав, що даний метод є більш ефективним за альтернативи.

Отже, було розроблено метод оцінювання ризиків інформаційної безпеки для медичної установи, який має переваги в порівнянні з іншими існуючими методами та допомагає визначити на що слід спрямувати захист, а також загальний рівень ІБ установи, що є дуже важливим.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ясінська Я.О., Куперштейн Л.М., «Розробка політики інформаційної безпеки медичного закладу» в Матеріали конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2021)», Вінниця, 2021. URL: http://ir.lib.vntu.edu.ua//handle/123456789/31280 (дата звернення: 14.09.2021).

2. Л.М. Купершейн, А.В. Дудатьєв, О.П. Войтович, Я.О. Ясінська «Модель політики інформаційної безпеки для об'єктів критичної інфраструктури» // Вимірювальна та обчислювальна техніка в технологічних процесах №2 , 2021.

3. Метод расчета риска информационной безопасности. URL: https://core.ac.uk/download/pdf/145189961.pdf / (дата звернення: 15.09.2021).

4. Козлова, Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. URL: https://moluch.ru/archive/52/6967/ (дата звернення: 17.09.2021).

5. Оцінка інформаційних ризиків. Левадний С.М. URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm (дата звернення: 19.09.2021).

6. Исследование средств оценивания рисков безопасности ресурсов информационных систем. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Zi_2017_19_1_9.pdf (дата звернення: 21.09.2021).

7. Ebios risk manager – the method. URL: https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/ (дата звернення: 23.09.2021).

8. Методики управления рисками информационной безопасности и их оценки (часть 2). URL: https://safe-surf.ru/specialists/article/5194/587935/ (дата звернення: 24.09.2021).

9. IT-Grundschutz (IT Baseline Protection Manual). URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html (дата звернення: 25.09.2021).

10. Cramm. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 25.09.2021).

11. ДСТУ ISO/IEC 27001:2015. Методи захисту системи управління інформаційною безпекою / Нац. стандарт України. – Вид. офіц. – [Чинний від 2017-01-01]. – Київ : ДП «УкрНДНЦ», 2017. – 31 с.

12. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки / Нац. стандарт України. – Вид. офіц. – [Чинний від 2019-11-01]. – Київ : ДП «УкрНДНЦ», 2019. – 76 с.

13. ДСТУ ISO/IEC 17799:2005. Практичні правила управління інформаційної безпекою. URL: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (дата звернення 26.09.2021).

14. Анализ международных документов по управлению рисками информационной безопасности. URL: https://habr.com/ru/post/495236/ (дата звернення: 26.09.2021).

15. Cobra. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_cobra.html (дата звернення 27.09.2021).

16. Riskwatch. URL: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html (дата звернення 28.09.2021).

17. Анализ модели угроз иб и уязвимостей. URL: https://studfile.net/preview/3245995/ (дата звернення 28.09.2021)

18. Обеспечение информационной безопасности в современном медицинском учреждении. URL: http://rus.safensoft.com/security.phtml?c=852 (дата звернення 29.09.2021).

19. Уязвимость (информационной системы). URL: https://safe-surf.ru/glossary/ru/1225/ (дата звернення 31.09.2021).

20. Оценка угроз и уязвимостей. URL: http://xn----7sbab7afcqes2bn.xn--p1ai/content/ocenka-ugroz-i-uyazvimostey (дата звернення 02.10.2021).

21. Модель порушника. Мета та принципи розробки. URL: http://www.rusnauka.com/11_EISN_2010/Informatica/63866.doc.htm (дата звернення 05.10.2021).

22. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.ua/ua/nd_tz_1.1-002-99.html (дата звернення 06.10.2020).

23. Методика побудови логіковероятностной моделі надійності логістичної системи. URL: https://stud.com.ua/53516/logistika/metodika_pobudovi_logikoveroyatnostnoy_modeli_nadiynosti_logistichnoyi_sistemi (дата звернення 08.10.2020).

24. Етапи нечіткого виведення. URL: https://stud.com.ua/133134/informatika/etapi_nechitkogo_vivedennya (дата звернення 08.10.2020).

25. Дудатьев. А. В., Лужецкий В. А., Коротаев В. А.. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны // Восточно-Европейский журнал передовых технологий, 2016. 4-11 с. URL: http://nbuv.gov.ua/UJRN/Vejpte_2016_2%282%29__2 (дата звернення: 14.10.2020).

26. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця: ВНТУ, 2013. 221 с.

ДОДАТКИ

Додаток А.Технічне завдання

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра захисту інформації

ЗАТВЕРДЖУЮ

Зав. кафедри ЗІ, д. т. н., проф.

_____В. А. Лужецький

_____ _____2021 року

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

на тему: «Метод оцінювання ризиків інформаційної безпеки для медичної установи»

08-20.МКР.013.00.000 ТЗ

Керівник: к. т. н., доц. каф. ЗІ

_____Куперштейн Л. М.

Вінниця 2021

1 Підстави для проведення робіт

Робота проводиться на підставі наказу ректора ВНТУ від 1 вересня 2021 року №207.

Дата початку роботи 01.09.2021 р.

Дата закінчення роботи 21.12.2021 р.

2 Мета та призначення МКР

Об'єктом дослідження є процеси оцінювання ризиків інформаційної безпеки.

Предметом дослідження є методи та засоби оцінювання ризиків інформаційної безпеки.

Метою магістерської кваліфікаційної роботи є підвищення рівня інформаційної безпеки медичної установи шляхом оцінки її ризиків ІБ задля подальшого їх усунення або зниження.

Актуальність теми полягає у тому, що медичні установи стають все більш вразливими через перенесення великої частини роботи у цифровий простір, тому виникає необхідність забезпечення інформаційної безпеки. У цьому може допомогти оцінка ризиків інформаційної безпеки задля їх подальшого усунення або щонайменше зниження.

3 Вихідні дані для проведення МКР

МКР проводиться вперше і вихідними даними для проведення МКР є:

3.1 Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця: ВНТУ, 2013. 221 с.

3.2 Метод расчета риска информационной безопасности. URL: https://core.ac.uk/download/pdf/145189961.pdf / (дата звернення: 15.09.2021).

3.3 Козлова, Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. URL: https://moluch.ru/archive/52/6967/ (дата звернення: 17.09.2021).

3.4 Оцінка інформаційних ризиків. Левадний С.М. URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm (дата звернення: 19.09.2021).

4 Виконавці МКР

Студентка групи 1БС-20м Ясінська Яна Олександрівна.

5 Вимоги до виконання МКР

Метод оцінювання ризиків інформаційної безпеки для медичної установи має відповідати наступним вимогам:

- Мати щонайменше 3 фактора для оцінки ризиків;
- Бути основаним на існуючих методах;
- Мати можливість оцінити кожну загрозу;
- Мати можливість оцінити загальний рівень ІБ установи.

6 Вимоги до супровідної документації

Графічна і текстова документація повинна відповідати діючим стандартам України – ДСТУ 3008:2015.

7 Стадії та етапи розробки

Робота по темі виконується в чотири етапи

Етап	Зміст	Початок	Закінчення	Результат
1	Аналіз завдання. Вступ	09.09.2021	16.09.2021	Вступ
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	17.09.2021	21.09.2021	Розділ 1
3	Розробка рішень	21.09.2021	27.09.2021	Розділ 2
4	Практична реалізація, моделювання, експериментування, результати	28.09.2021	18.10.2021	Розділ 3
5	Розробка розділу економічного обґрунтування доцільності розробки	19.10.2021	27.10.2021	Розділ 4

8 Очікувані результати та порядок реалізації МКР

Розробка нового методу оцінки ризиків інформаційної безпеки для медичної установи. Створення ази даних типових загроз для установ типу «міська клінічна лікарня».

9 Матеріали які подаються після закінчення МКР

По завершенню роботи подається пояснювальна записка та ілюстративна частина.

10 Порядок приймання МКР та її етапів

Апробація на науково-технічних конференціях та семінарах. Результати роботи будуть розглядатися на засіданні ДЕК із захисту магістерських кваліфікаційних робіт.

Попередній захист та доопрацювання МКР – 3-4 грудня 2021 р.

Представлення МКР до захисту – 18 грудня 2021 р.

Захист МКР – 21.12.21.

11 Вимоги до розроблення документації

Документація буде виконуватись за допомогою комп’ютерного набору у відповідності вимог ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання».

12 Вимоги щодо технічного захисту інформації з обмеженим доступом

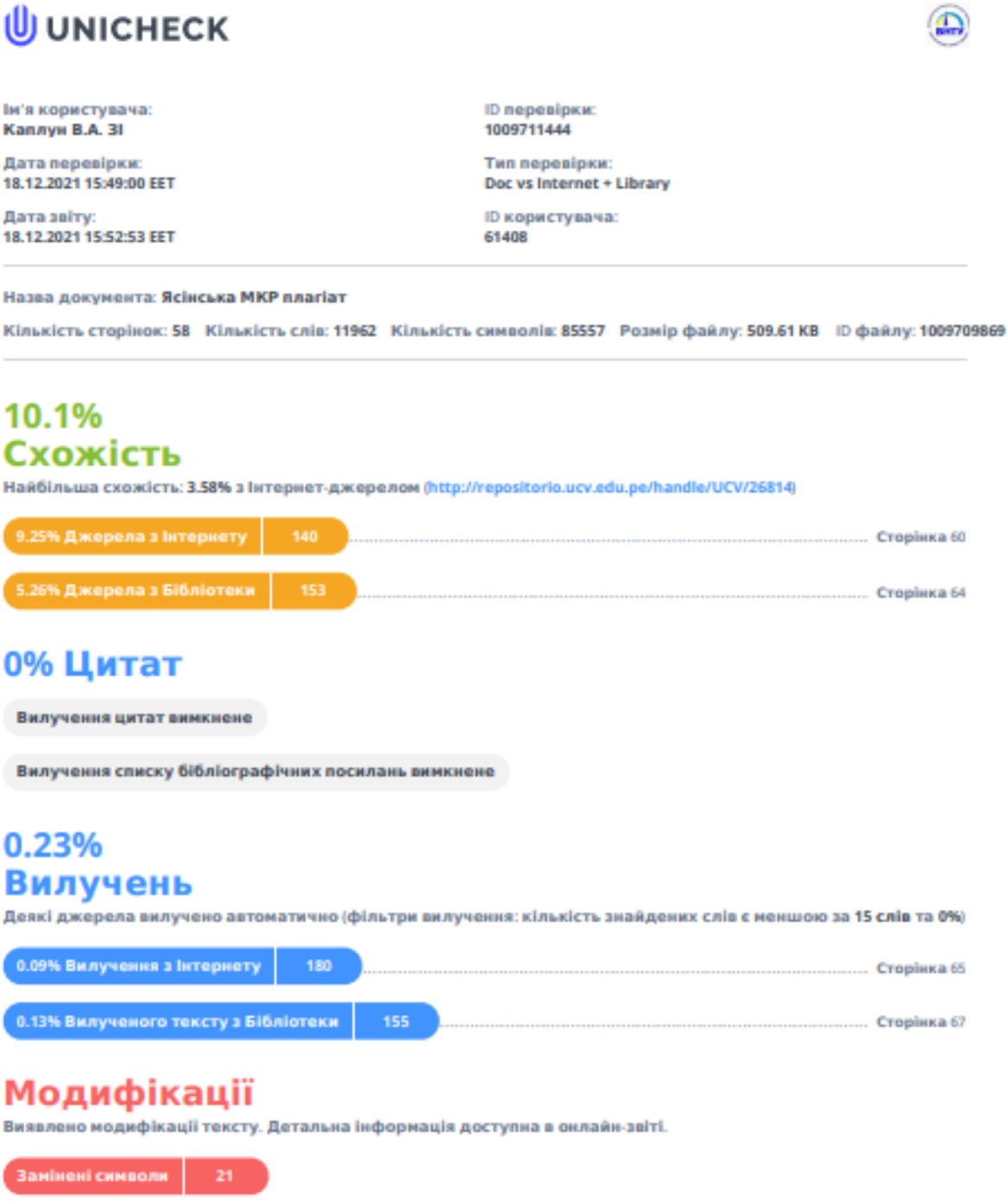
У зв’язку з тим, що дана робота не містить інформації, що потребує захисту у відповідності до законів України, заходи з її технічного захисту не передбачаються.

Додаток Б. Критерії оцінювання комерційного потенціалу розробки

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Критерій	1	2	3	4	5
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
8	Відсутні фахівці як з технічної,	Необхідно наймати фахівців або	Необхідне незначне навчання	Необхідне незначне	Є фахівці з питань як з технічної, так і

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Критерій	1	2	3	4	5
	так і з комерційної реалізації ідеї	витрачати значні кошти та час на навчання наявних фахівців	фахівців та збільшення їх штату	навчання фахівців	з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Додаток В. Результат перевірки роботи на плагіат



UNICHECK

Ім'я користувача:
Каплун В.А. ЗІ

ID перевірки:
1009711444

Дата перевірки:
18.12.2021 15:49:00 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
18.12.2021 15:52:53 EET

ID користувача:
61408

Назва документа: Ясінська МКР плагіат

Кількість сторінок: 58 Кількість слів: 11962 Кількість символів: 85557 Розмір файлу: 509.61 KB ID файлу: 1009709869

10.1%
Схожість

Найбільша схожість: 3.58% з Інтернет-джерелом (http://repositorio.ucv.edu.pe/handle/UCV/26814)

9.25% Джерела з Інтернету 140 Сторінка 60

5.26% Джерела з Бібліотеки 153 Сторінка 64

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0.23%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 15 слів та 0%)

0.09% Вилучення з Інтернету 180 Сторінка 65

0.13% Вилученого тексту з Бібліотеки 155 Сторінка 67

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

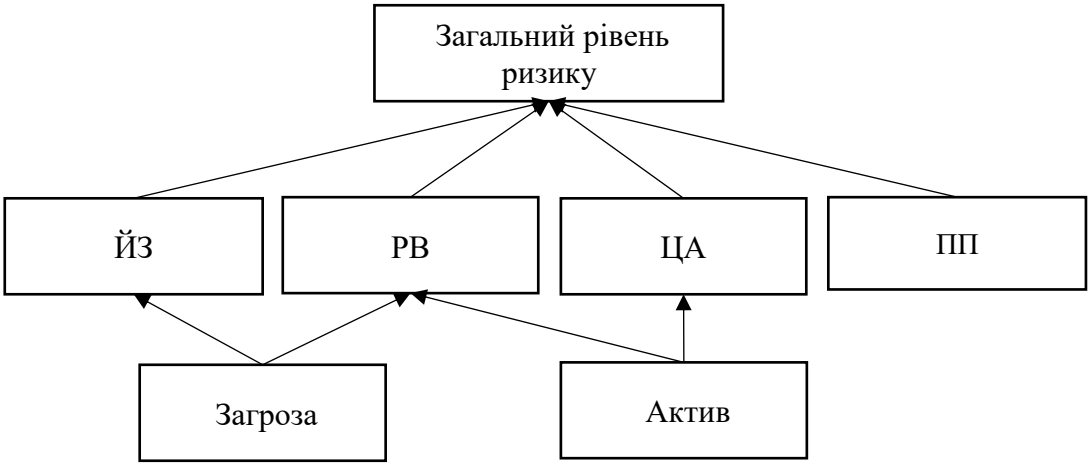
Замінені символи 21

ІЛЮСТРАТИВНА ЧАСТИНА

Загальна модель процесу оцінки ризиків інформаційної безпеки запропонованого методу

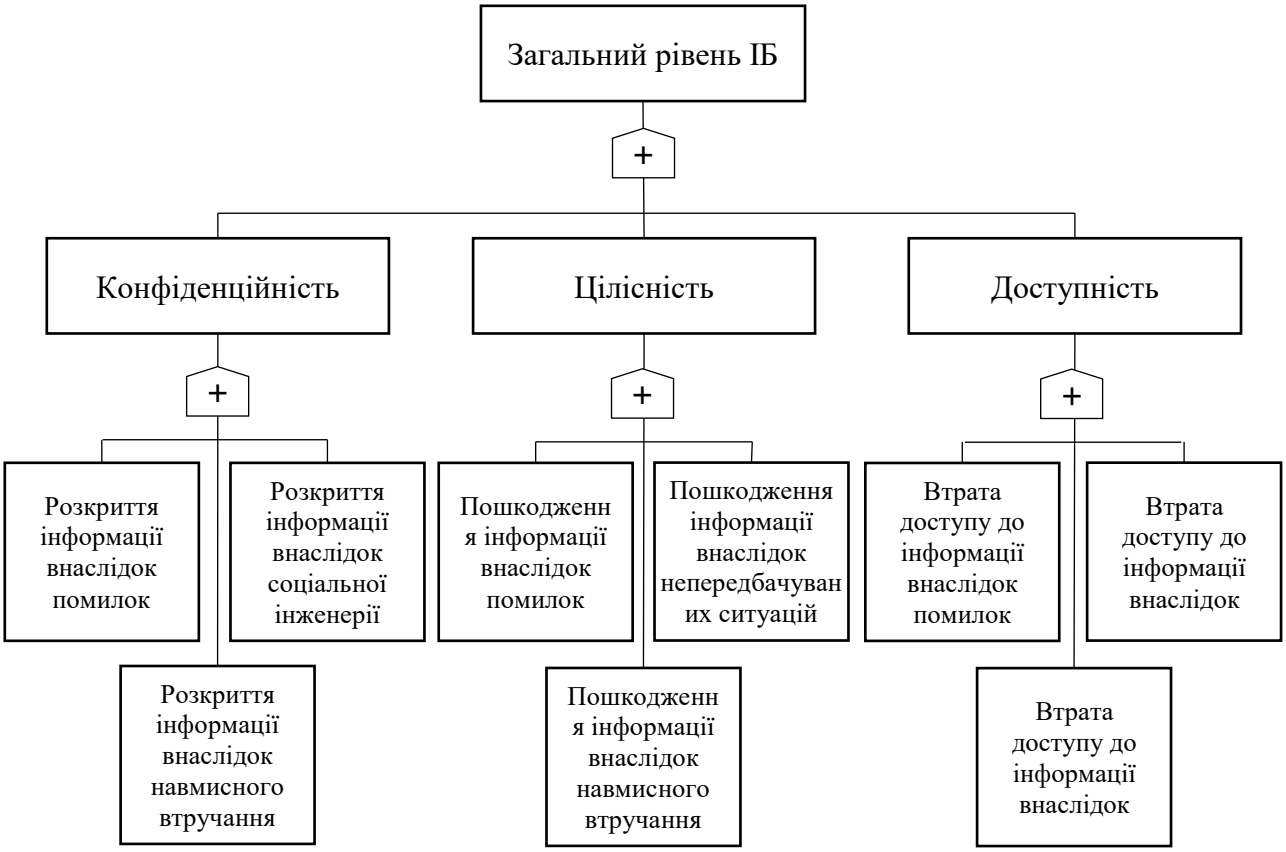
					08-20.МКР.013.00.000 І41		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Загальна модель процесу оцінки ризиків інформаційної безпеки запропонованого методу	Літ.	Арк. 1 / Аркушів 1
Перевір.		Куперштейн Л. М.					
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м	
Н. Контр.		Куперштейн Л. М.					
Затверд.		Лужецький В. А.					

Графічна формалізація першої стадії методу оцінювання ризиків ІБ



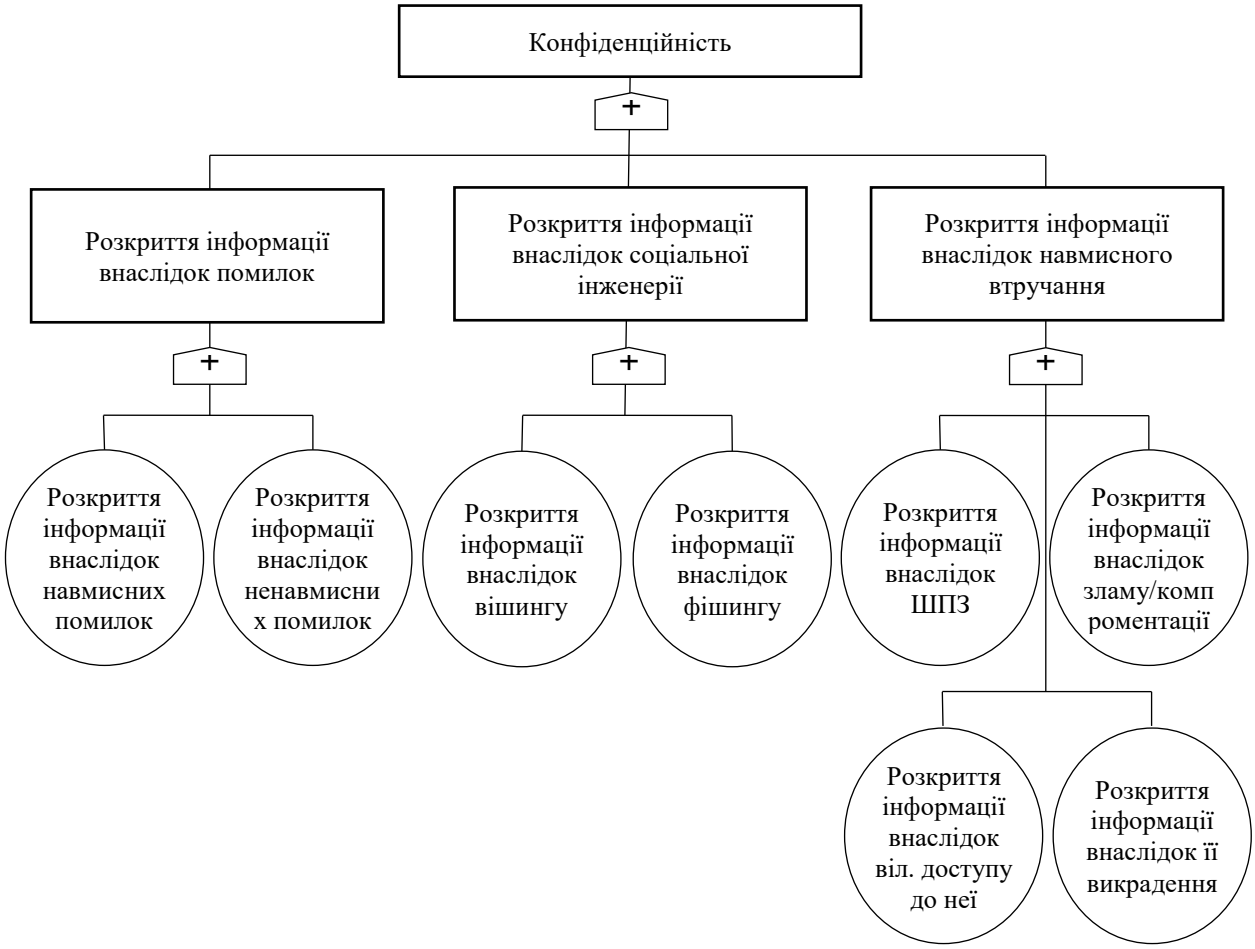
					08-20.МКР.013.00.000 І42			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Графічна формалізація першої стадії методу оцінювання ризиків ІБ	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

Загальний вигляд логіко-ймовірнісної моделі для МКЛ



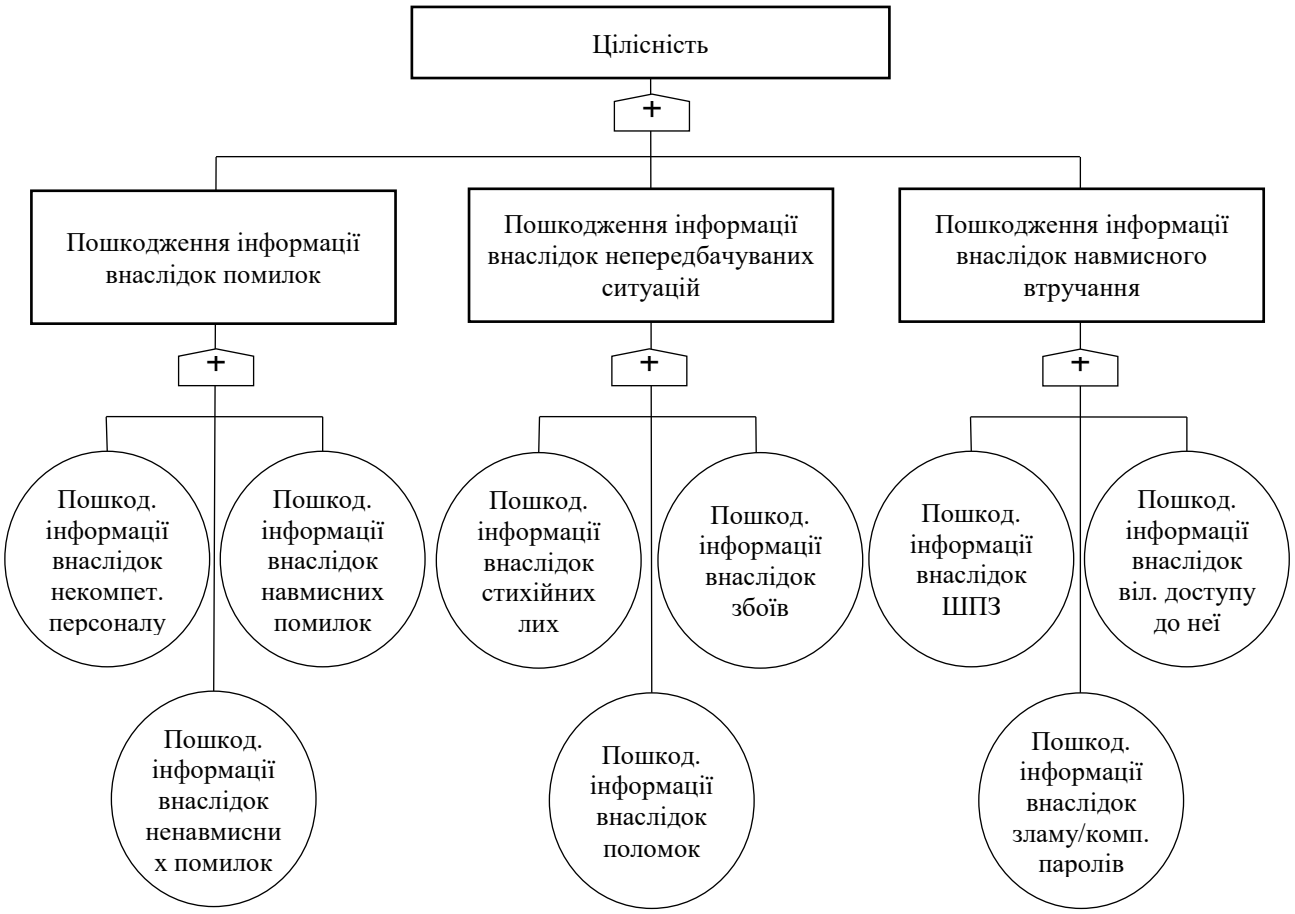
					08-20.МКР.013.00.000 І43			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Загальний вигляд логіко-ймовірнісної моделі для МКЛ	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

Гілка «Конфіденційність»



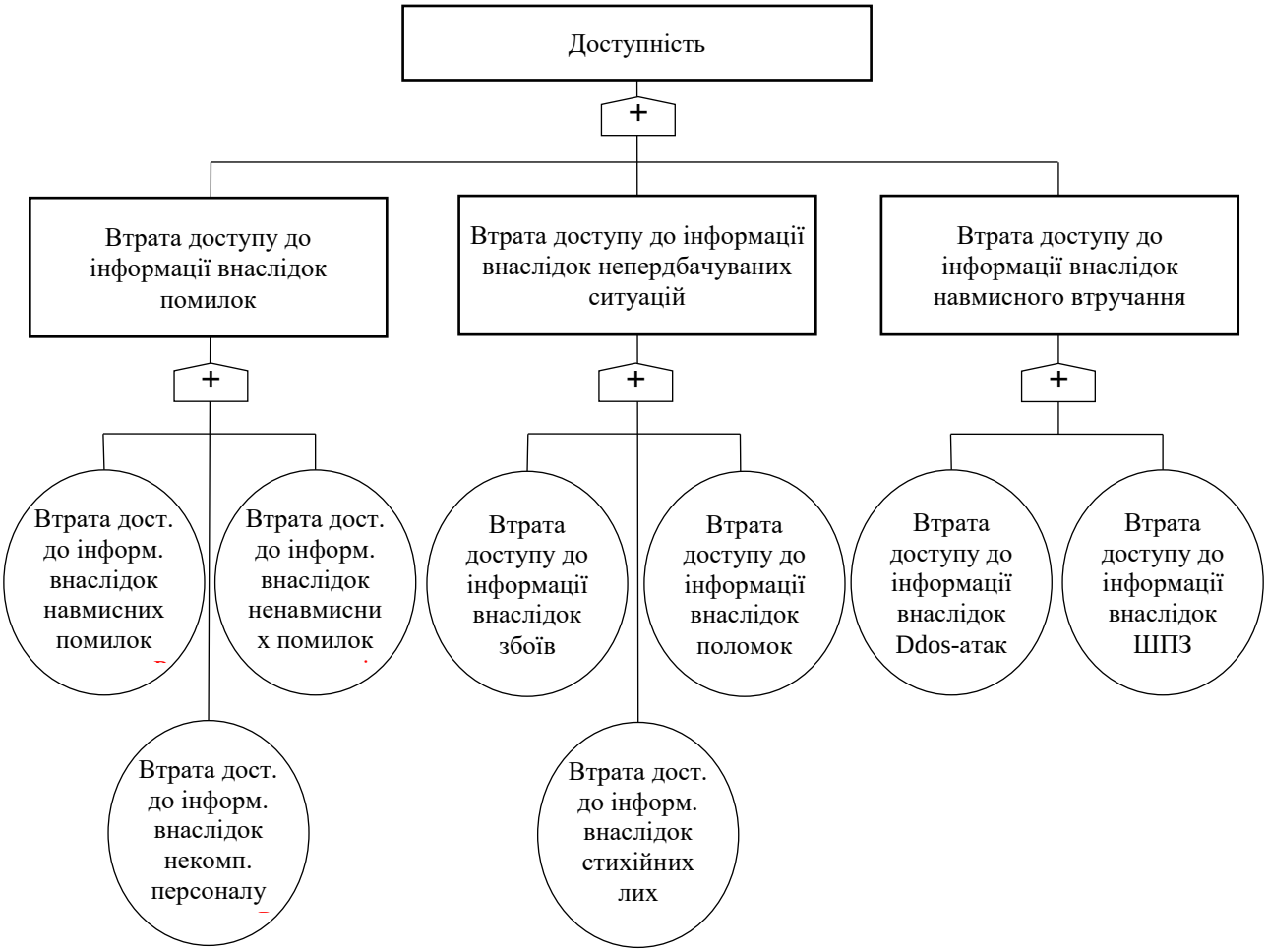
					08-20.МКР.013.00.000 І44			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Гілка «Конфіденційність»	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

Гілка «Цілісність»



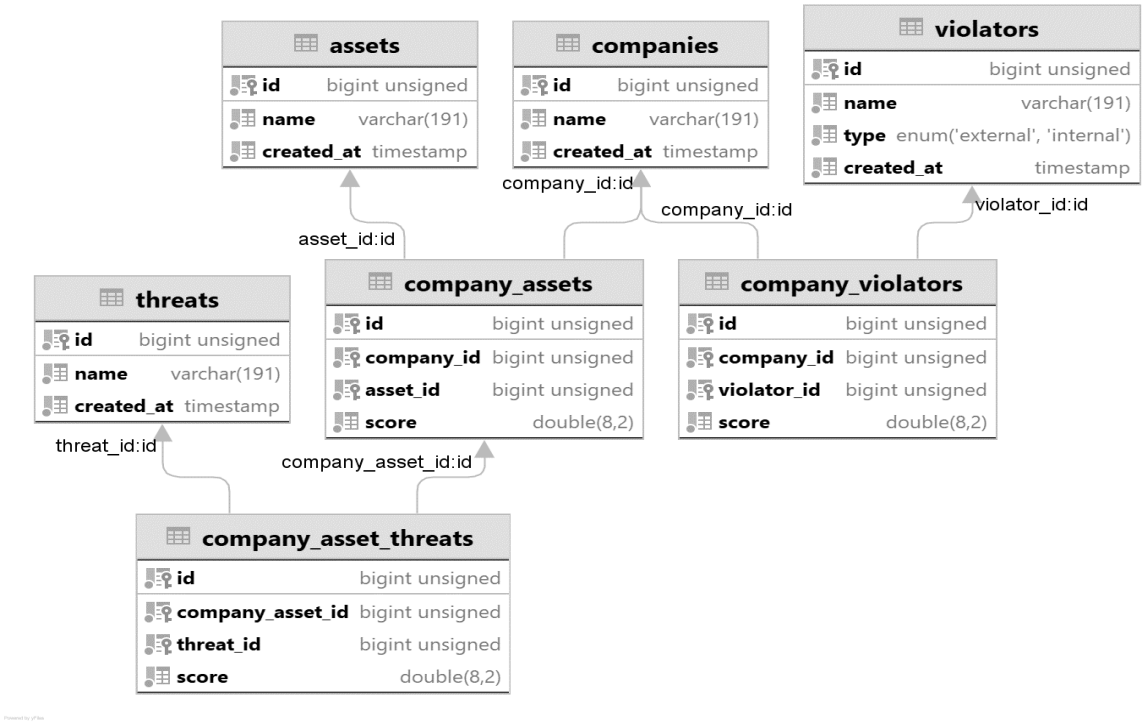
					08-20.МКР.013.00.000 145			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Гілка «Цілісність»	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

Гілка «Доступність»



					08-20.МКР.013.00.000 І46			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Гілка «Доступність»	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

Загальна схема зв’язків бази даних



					08-20.МКР.013.00.000 147			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Ясінська Я. О.			Метод оцінювання ризиків інформаційної безпеки для медичної установи. Загальна схема зв'язків бази даних	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Савицька Л. А.				ВНТУ гр. 1БС-20м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						