**Міністерство освіти і науки України**
**Київський Національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## Дипломної роботи

***магістра***
(назва освітньо-кваліфікаційного рівня)

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

**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)

**освітній рівень** ***магістр***
(назва освітнього рівня)

**кваліфікація**
(код і назва кваліфікації)

**на тему**: *Моделі ідентифікації ризиків кібербезпеки в розподілених ІС*

**Виконавець: студент** *2* **курсу, групи** *КБм-21*

*Кучмай Олексій Олегович*
(прізвище ім'я по-батькові)

(підпис)

| | **Прізвище, ініціали** | **Оцінка** | **Підпис** |
|---|---|---|---|
| **Науковий керівник** | *Бабенко Т.В.* | | |
| **Рецензент** | | | |
| **Нормоконтроль** | | | |

**Київ**
**2021**

**Міністерство освіти і науки України**
**Київський Національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
«_____»_____20___року

**ЗАВДАННЯ**
**на виконання дипломної роботи**

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**студенту** *КБм-21* (група) *Кучмай Олексій Олегович* (прізвище ім'я по-батькові)

**Тема дипломної роботи** *Розробка моделі ідентифікації ризиків кібербезпеки в розподілених ІС*

## 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 2 від 08.10.2020

## 2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

**Об'єкт досліджень** *Процес ідентифікації ризиків кібербезпеки в розподілених ІС*

**Предмет досліджень** *Моделі та методи що можуть бути використані для ідентифікації ризиків кібербезпеки в розподілених ІС*

**Мета** *Розробка методу ідентифікації ризиків кібербезпеки в розподілених ІС*

**Вихідні дані для проведення роботи** *Стандарти у сфері інформаційної*

*ки,*
*наукові публікації вітчизняних та іноземних авторів*

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

**Наукова новизна** *Розробка моделі ідентифікації ризиків кібербезпеки в розподілених ІС, за допомогою поєднання існуючих методологій*

**Практична цінність** *Розробка методології для ідентифікації ризиків кібербезпеки у розподілених ІС*

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

*Робота виконана у повному обсязі відповідно до теми.*

## 5. ЕТАПИ ВИКОНАННЯ РОБОТИ

| **Найменування етапів робіт** | **Строки виконання робіт (початок-кінець)** |
|---|---|
| Уточнення постановки задачі | 12.10.2020 – 16.10.2020 |
| Аналіз літератури | 19.10.2020 – 10.12.2020 |
| Аналіз нормативно-правового забезпечення | 25.01.2021 – 12.02.2021 |
| Розробка плану для досягнення мети роботи | 15.02.2021 – 26.02.2021 |
| Розробка моделі ідентифікації ризиків кібербезпеки в розподілених ІС | 05.04.2021 – 16.04.2021 |
| Формування висновків | 17.04.2021 – 07.05.2021 |
| Оформлення пояснювальної записки | 08.05.2021 – 10.05.2021 |
| Підготовка до захисту дипломної роботи | 11.05.2021 – 16.05.2021 |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** *Зниження збитків через викрадення даних*

**Соціальний ефект** *Покращення технологій забезпечення захисту інформації в розподілених ІС підприємств*

## 7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Т. В. Бабенко
(підпис) (прізвище, ініціали)

Завдання прийняв

до виконання _____ О. О. Кучмай
(підпис) (прізвище, ініціали)

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

**УДК 681.3.**

## РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Розробка моделі ідентифікації ризиків кібербезпеки в розподілених ІС» складається зі списку скорочень, вступу, основної частини, що містить 3 розділів, висновків, списку літератури та джерел. Загальний обсяг роботи – 98 сторінка. Робота містить 8 рисунків. Список використаних джерел включає 58 джерел.

Об’єкт дослідження – процес ідентифікації ризиків кібербезпеки в розподілених ІС.

Мета роботи – розробка методу ідентифікації ризиків кібербезпеки в розподілених ІС.

Предмет дослідження – моделі та методи що можуть бути використані для .

Метод дослідження – аналіз та опрацювання літератури за даною темою, аналіз документації міжнародних стандартів та їх порівняння.

Практична цінність отриманих результатів полягає у розробці методу щодо ідентифікації ризиків кібербезпеки у розподілених ІС.

Ключові слова: інформаційна безпека, ідентифікація ризиків, кібербезпека, інформаційні системи, загроза, ризик.

# ЗМІСТ

ВСТУП..... 8
РОЗДІЛ 1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ УПРАВЛІННЯ РИЗИКАМИ..... 9
1.1. Функціональні методи оцінки ризиків ..... 9
1.2. Стандарти аналізу ризиків.....20
1.2.1 Стандарт NIST SP 800-30.....20
1.2.2 Методологія FRAP.....26
1.2.3 Методологія ISO 2700x.....30
1.3 Порівняння методів оцінки ризиків .....34
1.4 Постановка задачі.....38
Висновки до розділу 1 .....39
РОЗДІЛ 2 РОЗРОБКА МОДЕЛІ ІДЕНТИФІКАЦІЇ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІС .....40
2.1 Визначення активів .....41
2.2 Визначення загроз .....42
2.3 Визначення існуючих заходів і засобів контролю та управління.....43
2.4 Виявлення вразливостей .....45
2.5 Визначення наслідків .....46
2.6 Встановлення значення ризику .....47
2.7 Оцінка наслідків .....48
2.8 Оцінка ймовірності інциденту.....50
2.9 Встановлення значень рівня ризиків .....51
2.10 Результатом ідентифікації ризиків .....52
Висновки до розділу 1 .....53
РОЗДІЛ 3 ПЕРЕВІРКА АДЕКВАТНОСТІ ВИКОРИСТАННЯ МОДЕЛІ Ідентифікації ризиків .....54
3.1 Характеристика об’єкта інформаційної діяльності ТОВ «ССК „Укрконсалтинг“».....54

3.1.1 Загальна характеристика та призначення підприємства.....54
3.1.2 Характеристика фізичного середовища ІТС.....55
3.1.3 Інформація що обробляється в ІС.....56
3.2 Виконання перевірки адекватності моделі ідентифікації ризиків на прикладі ТОВ «ССК „Укрконсалтинг“» .....58
3.2.1 Опис бізнес-цілей і бізнес-функцій, основних бізнес-процесів ТОВ «ССК" Укрконсалтинг "».....58
3.2.2 Ідентифікація активів .....61
3.2.3 Оцінка важливості інформаційних активів.....62
Висновки до розділу 3 .....90
ВИСНОВКИ.....91
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....92
ДОДАТКИ .....99

# ВСТУП

У сучасному світі все більше уваги приділяється захисту інформації. Як і в будь-якому іншому виді діяльності, грамотне планування забезпечення безпеки інформації є найважливішим етапом на шляху до забезпечення безпеки даних.

Організація ефективної системи захисту інформації стає критично важливим стратегічним чинником розвитку будь-якого підприємства, так як, інформація є одним з ключових елементів бізнесу. При цьому під інформацією розуміються не тільки статичні інформаційні ресурси (бази даних, поточні налаштування обладнання та інші), а й динамічні інформаційні процеси обробки даних.

В дипломній роботі розглядається питання ідентифікації ризиків кібербезпеки у розподілених ІС.

# РОЗДІЛ 1
# АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ УПРАВЛІННЯ РИЗИКАМИ

## 1.1. Функціональні методи оцінки ризиків

Для того щоб відповідальним сторонам краще зрозуміти ризики, які впливають на результативність запроваджених засобів контролю та досягнення поставлених цілей, необхідне загальне оцінювання ризику. Саме це дає основу для прийняття рішень для найбільш відповідного підходу оброблення ризиків. Вихідні дані загального оцінювання ризику - це вхідні дані для процесів прийняття рішень в організації.

Процес який дає змогу ідентифікувати, аналізувати та оцінювати ризик називається - загальним оцінюванням ризику що показано на рисунку 1.1.

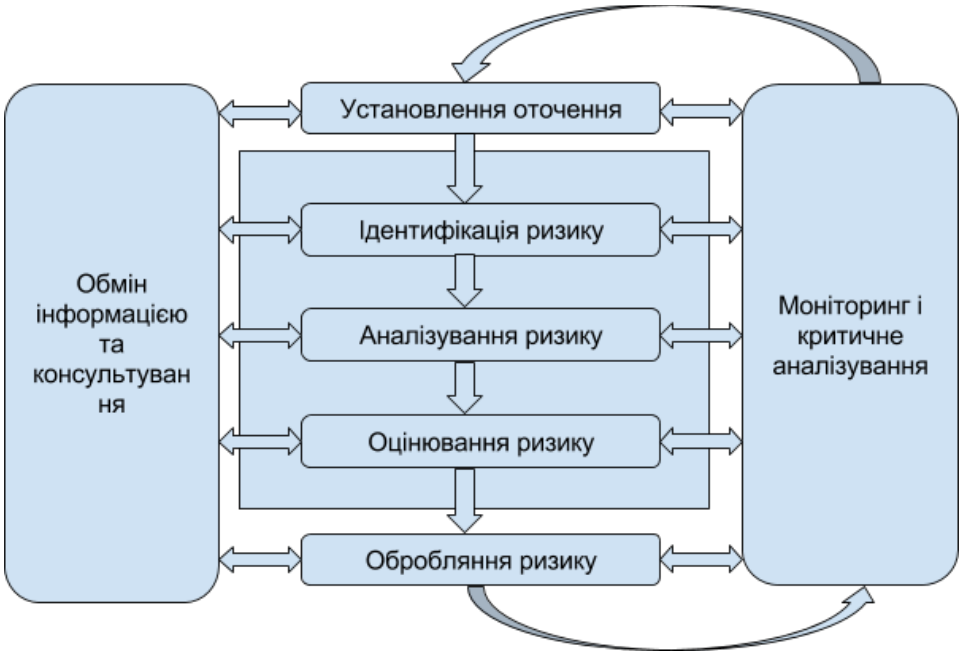


Рисунок 1.1 - Процес загального оцінювання ризику

Процес виявлення, усвідомлення та реєстрування ризику називається - ідентифікуванням ризику, його призначення - визначити, які саме ситуації можуть виникнути, що можуть впливати на досягнення поставлених цілей організації. Після того, як ризик ідентифіковано, організація має визначити будь-які наявні засоби контролю, стосовно конструктивних особливостей, персоналу, процесів і систем.

Метою ідентифікації ризику є визначення того, що могло б статися, щобспричинити потенційні втрати, і щоб отримати уявлення про те, як, де і чомуці втрати можуть виникати. Етапи, які входять в ідентифікацію ризику,повинні збирати вхідні дані для дії щодо аналізу ризику:

1. ідентифікація активів СУІБ (активом є щось, що має цінність дляорганізації і, отже, потребує захисту);

2. ідентифікація загроз;

3. ідентифікація існуючих засобів контролю;

4. ідентифікація вразливостей;

5. ідентифікація наслідків.

Методологія аналізу ризиків може бути якісною чи кількісною, або їх комбінацією залежно від обставин. Рівні ризиків повинні порівнюватися з критеріями оцінювання ризику і критеріями прийняття ризику.

Існують такі методи ідентифікування ризику:

- доказові методи, наприклад, застосування переліків контрольних запитань і критичне аналізування даних;
- системні методи групової роботи, коли група експертів систематично ідентифікує ризики за допомогою структурованого набору навідних фраз або запитань;
- та інші.

Можна використовувати допоміжні методи, для того щоб поліпшити точність і повноту ідентифікування ризику. Наприклад “Мозкову атаку” чи “Метод Дельфі”. Особливу увагу під час ідентифікування ризику необхідно приділяти організаційним та людським чинникам, враховувати відхили від очікуваних станів, а також події, які

пов’язані з технічними та програмними засобами. Поглиблене розуміння ризику дає змогу прийняти рішення щодо найбільш відповідних стратегій і методик обробляння ризику.

До основних проблем забезпечення кібербезпеки на сучасному підприємстві можна віднести: відсутність кваліфікованого персоналу (зазвичай функції фахівця з кібербезпеки виконує досвідчений користувач з числа штатних співробітників або, в кращому випадку, системний адміністратор), такі організації не проводять оцінку ризиків та реагують на інцидент після заподіяння збитків.

Основні етапи процесу оцінки ризиків інформаційної безпеки можуть бути представлені у вигляді вкладених алгоритмів (процедур), як показано на рис. 1.3.

Даний процес та його етапи аналогічні для усіх організацій та об’єктів інформаційної інфраструктури незалежно від їх сфери діяльності та масштабів. Проте дані етапи вирішують конкретні задачі та мають свої особливості, тому для оцінки ризиків кібербезпеки на різних етапах необхідно застосовувати різні механізми їх реалізації.

На етапі аналізу потоку даних в інформаційній системі будується модель інформаційної системи, визначається призначення її елементів та підсистем, взаємозв’язки між ними, а також маршрути потоків інформації.

Мета даного етапу – визначити недоліки в інформаційній системі, суттєві для інформаційної безпеки. Відповідно модель системи повинна бути наглядною та зручною для аналізу. Такими є функціональні моделі, побудовані за допомогою методів структурного аналізу в графічній формі зі змістовним описом, що дозволяє аналізувати діаграми.

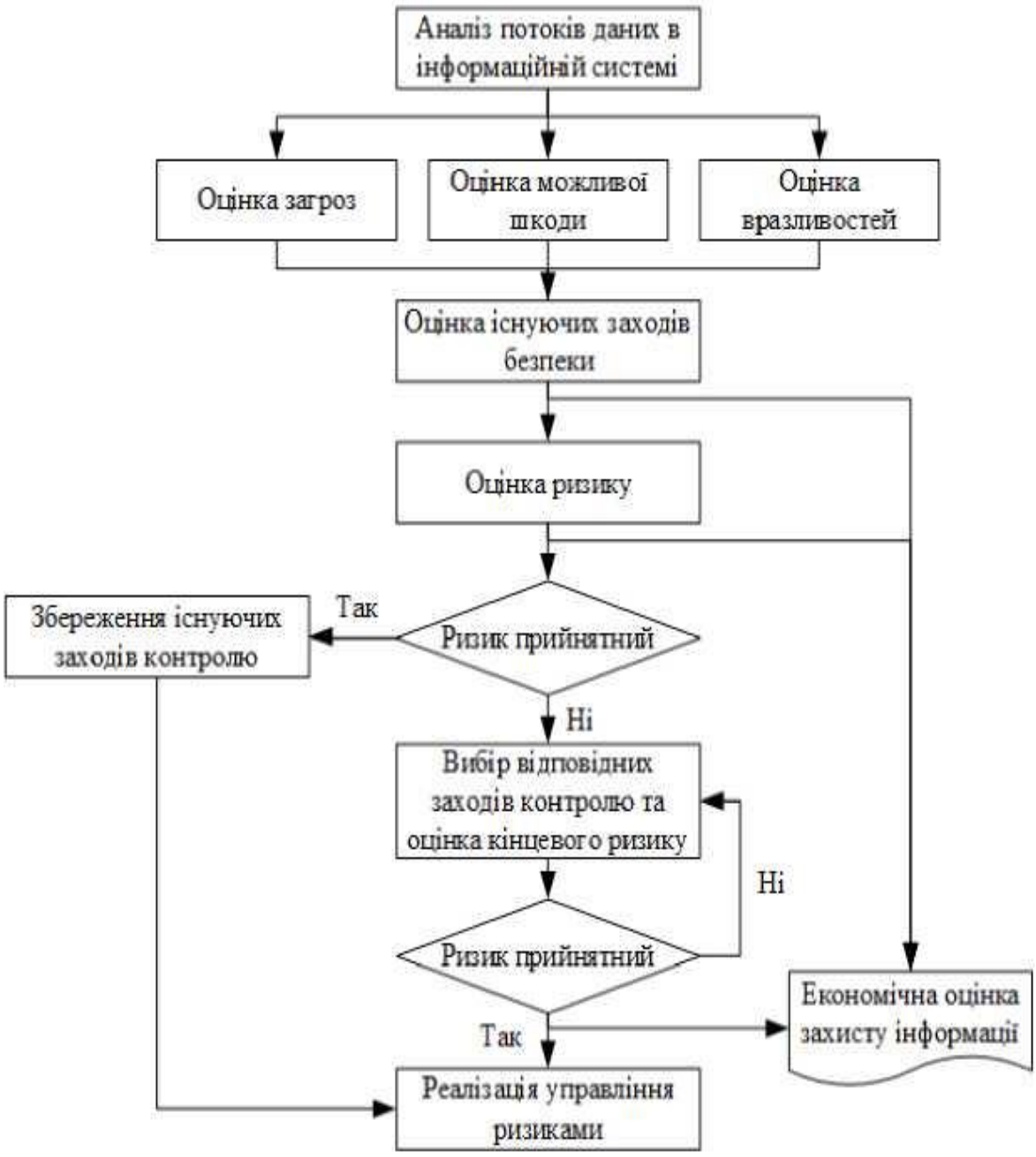


Рисунок 1.2 - Процес оцінки ризиків інформаційної безпеки

На наступному етапі вирішується задача оцінки факторів ризику – Xi, X2 та X3. Методи для вирішення задачі оцінки можна розділити на кількісні та якісні, які відрізняються за вибором шкали вимірювання – числової та лінгвістичної.

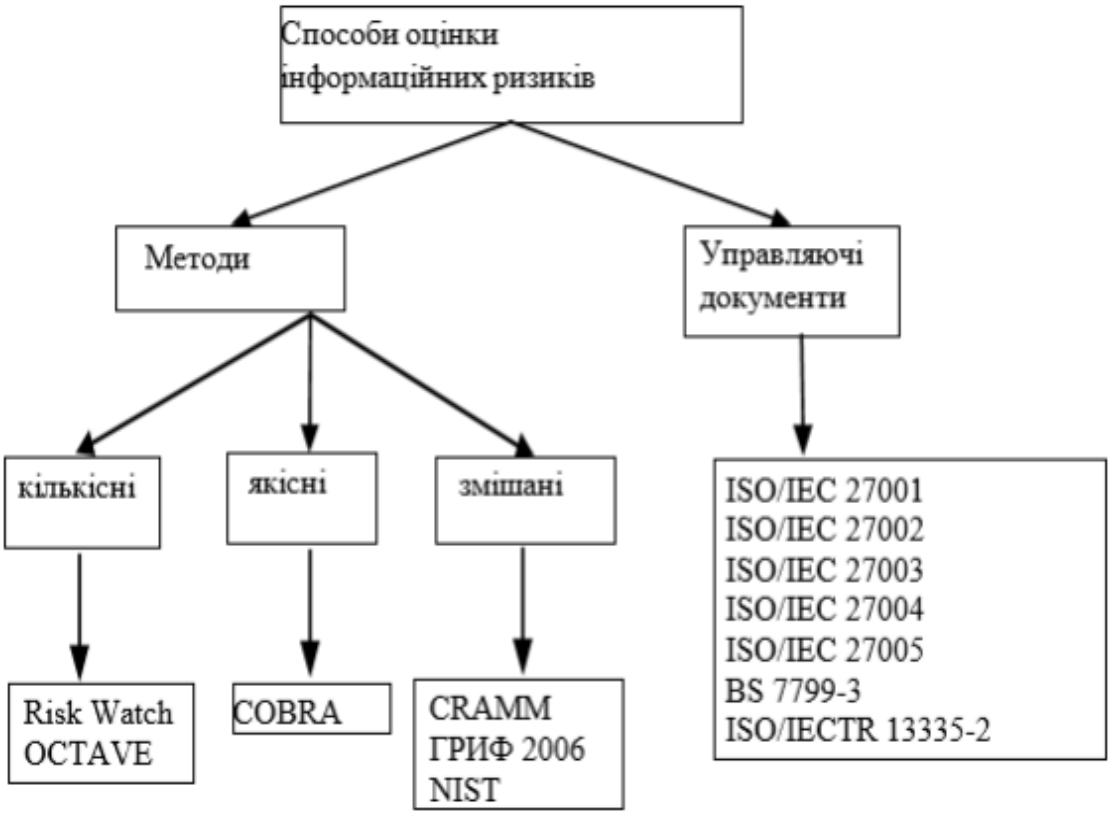


Рисунок 1.3 - Схематичний розподіл методів визначення ризиків в розподілених інформаційних системах

Кожна група методів має свої переваги та недоліки, які наведено у таблиці 1.1.

Мінімізувати перераховані недоліки дозволяє поєднання кількісних та якісних методів – використання шкали числових коефіцієнтів разом з лінгвістичним описом її окремих інтервалів (рівнів). Поєднані методи слід використовувати як на даному, так і на наступному етапі – оцінці існуючих заходів безпеки.

Особливістю даних етапів є те, що оцінити фактори ризику можна тільки експертно. Особливо це стосується оцінки можливої шкоди, яка включає визначення вартості інформаційних активів та ресурсів. Для оцінки решти факторів експерти можуть використовувати результати аналізу потоків даних в інформаційній системі, отриманих на першому етапі, а також статистичні дані (якщо такі є) про загрози, вразливості та ефективність існуючих заходів безпеки.

Таблиця 1.1

Переваги та недоліки кількісних та якісних методів

| Методи оцінки | Переваги | Недоліки |
|---|---|---|
| Кількісні методи | Дозволяють чисельно оцінити необхідні параметри.<br>Реалізовують аналіз витрат та прибутку при виборі захисту.<br>Надають більш точне відображення шуканих значень. | Кількісні міри залежать від об'єму та точності шкали виміру.<br>Результати оцінки можуть бути неточними.<br>Повинні доповнюватись якісними характеристиками.<br>Оцінка з застосуванням цих методів зазвичай потребує більше досвіду та сучасного інструментарію. |
| Якісні методи | Дозволяють визначити області критичних рівнів в короткий проміжок часу без значних витрат.<br>Дозволяють оцінювати відносно легко та дешево. | Не дозволяють визначити імовірності та результати з використанням числових коефіцієнтів.<br>Аналіз витрат та користі при виборі захисту важчий.<br>Отримані результати мають загальний, наближений характер. |

Етап оцінки ризику повторюється до тих пір, поки рівень остаточного ризику, знижений в результаті впровадження контрзаходів, не буде прийнятним. Окремим етапом йде економічна оцінка захисту інформації, метою якої є розрахунок співвідношень ризику інформаційної безпеки, витрат на контрзаходи та переваги, отримувані від їх впровадження.

В залежності від рівня ризику та оцінки економічних витрат на його зниження реалізується завершаючий етап – управління ризиками. Існує 4 типових методи його реалізації:

– мінімізація ризику – виконання дій для зменшення імовірності та / або негативних наслідків, пов'язаних з ризиком;

– прийняття ризику – готовність організації зазнати збитки від конкретного ризику у випадку, якщо його рівень вважається прийнятним;

– ухилення від ризику – відмова від втягнення в ризиковану ситуацію чи дію, що попереджує її виникнення;

– передача ризику – покладання відповідальності за ризик на треті особи .

Методи експертних оцінок – це комплекс логічних та математично-статистичних методів та процедур по обробці результатів опитування групи експертів, при цьому результати опитування є єдиним джерелом інформації. Метод використовується тоді, коли недостатність чи повна відсутність інформації не дозволяє використовувати інші можливості.

Метод Дельфі. Даний метод є одним з найбільш формальних методів експертного прогнозування. Згідно методу Дельфі аналіз проблеми відбувається в декілька етапів. На першому етапі аналітики розробляють систему змінних для конкретного випадку, потім залучивши ряд експертів визначають вагу кожної змінної по поточному ризику, та на етапі аналізу проводяться оцінка висновків експертів, аналіз отриманих висновків та підготовка кінцевих практичних рекомендацій по поставленій проблемі.

Імітаційне моделювання та імовірність виконання. Метод імітаційного моделювання є одним із потужніших методів аналізу системи. Загалом даний метод в основі має процес проведення на ЕОМ експериментів з математичними моделями складних реальних систем. В свою чергу, оцінка імовірності виконання дозволяє дати спрощену статистичну оцінку імовірності виконання досліджуваного рішення шляхом розрахунку частки виконаних та невиконаних рішень в загальній сумі прийнятих рішень.

Імітаційне моделювання застосовується в тих випадках, коли проведення реальних експериментів нецілеспрямовано, потребує значних витрат або неможливе на практиці. Окрім того, зазвичай практично неможливий або потребує значних витрат збір необхідної інформації для прийняття рішень. В подібних випадках відсутність фактичних даних замінюється величинами, отриманими в процесі імітаційного експерименту .

Метод CORAS. Даний метод дозволяє здійснити аналіз ризиків шляхом їх моделювання. В його основі лежить адаптація, уточнення та поєднання таких методів проведення аналізу ризиків, як Event-Tree-Analysis, ланцюги Маркова,

HazOp та FMECA. CORAS використовує технологію UML та базується на австралійському / новозеландському стандарті AS / NZS 4360:1999 Risk.

Management та ISO / IEC 17799–1:2000 Code of Practice for Information Security Management. У цьому стандарті враховані рекомендації, наведені в документах ISO / IEC TE 13335–1: 2001 Guidelines for the Management of IT Security та IEC 61508: 2000 Functional of Electrical / Electronic / Programmable Safety Related. Відповідно до підходу CORAS інформаційні системи розглядаються не тільки з точки зору використовуваних технологій, а як складний комплекс, в якому враховується і людський фактор [3].

Процес аналізу ризиків за допомогою методології CORAS загалом складається з наступних етапів:

– підготовка до проведення аналізу – збір відомостей про об'єкти аналізу, оцінка меж аналізу та його глибини;

– проведення співбесіди з організацією – визначення точки зору організації на об'єкти аналізу;

– опис задачі аналітиками після проведення співбесіди та вивчення документації – виявлення основних активів, які потребують захисту, високорівневий опис актуальних загроз, сценаріїв проведення загроз;

– вивчення представленої документації на об'єкти аналізу – визначення критерію оцінювання ризику для кожного активу;

– проведення заходів щодо ідентифікації ризиків. В цих цілях CORAS використовує структурований «мозковий штурм» – це методика, по якій аналітики покроково вивчають об'єкт аналізу за допомогою співробітників організації. Сутність даного методу полягає в неоднорідності експертів, що мають різну компетенцію, уподобання, схильності та судження, що дозволяє охопити велику частину особливостей об'єкта вивчення при проведенні аналізу та виявити існуючі ризики;

– ідентифікація ризику – включає в себе виявлення актуальних загроз, інцидентів інформаційної безпеки, сценаріїв загроз, вразливостей відносно конкретного об'єкта аналізу;

– визначення рівня ризику, який виникає при конкретному інциденті інформаційної безпеки;

– на даному етапі визначається політика обробки ризиків;

– останній етап присвячений ідентифікації та аналізу методів обробки. Неприйнятні ризики аналізуються з метою пошуку методів їх мінімізації. Одним із суттєвих факторів при виборі методу обробки ризиків є вартість його реалізації.

Метод ситуаційного аналізу. Однією з технологій для побудови системи активного захисту інформаційної системи є ситуаційний аналіз кібербезпеки (cybersecurity situation evaluation, далі – CSSE). На основі аналізу великої кількості подій та моніторингу результатів технологія CSSE дозволяє спрогнозувати та оцінити загальний стан кібербезпеки мережі. Оцінка методів захисту від кібератак зосереджена в основному на інформуванні (cybersecurity situation awareness, далі – CSSAw), оцінці (cybersecurity situation assessment, далі – CSSAs) та прогнозуванні (cybersecurity situation forecast, далі – CSSF) [4]:

– CSSAw використовується для відображення локального стану кібербезпеки в цільовій мережі;

– CSSAs може інтегрувати результати CSSAw по всій мережі, щоб отримати загальну оцінку кібербезпеки (cybersecurity situation value, далі – CSSV);

– CSSV відображає оцінку кібербезпеки в режимі реального часу в цільовій області на макрорівні;

– CSSF використовується для отримання оцінки кібербезпеки в цільовій мережі в наступний момент.

В роботі [5] представлена інтегрована модель CSSE. Практично вона була розгорнута в інформаційній мережі Державної електромережної корпорації Китаю (SGCC). Етапи були наступні: було проведено поглиблений аналіз робочих процедур CSSAw та CSSF та отримано математичні характеристики для знаходження зв’язків з їх математичними моделями.

На основі алгоритму AdaBoost була розроблена модель CSSE, яка послідовно виконує функції CSSAw, CSSAs та CSSE. Тут алгоритм AdaBoost застосовується кілька разів, щоб спростити структуру моделі CSSE, також використання характеру

самонавчаючого алгоритму AdaBoost ефективно покращує точність CSSE. На основі проєкту «системи забезпечення безпеки інформаційної мережі (ISS)» модель CSSE була розгорнута в великомасштабній системі моніторингу кібербезпеки.

CSSAw є ефективним засобом для отримання в режимі реального часу інформації про мікро-ситуації з кібербезпекою для мережі, по якій можна судити про існування кібератак на основі загального збору даних з конкретних вузлів в цільовій мережі. Дані містять інформацію про мережеві повідомлення, розподілення мережевих потоків, стан системних процесів та функціонування сервісів. Зазвичай в якості CSSAw для малих та середніх мереж може використовуватись технологія виявлення вторгнень.

CSSAs може відповідати за використання системи індексів оцінки кібербезпеки для розрахунку поточної CSSV за допомогою мікро-результатів CSSAw та за відображення в реальному часі макро-ситуації кібербезпеки цільової мережі. CSSV – числовий опис ситуації кібербезпеки. Це значення безпосередньо відображає макро-ситуацію кібербезпеки в цілому. CSSF передбачує тенденції розвитку ситуації макро-кібербезпеки шляхом прогнозування майбутнього CSSV цільової мережі.

Таким чином, існує явний зв’язок між трьома робочими процесами: CSSAw – перший процес, який має бути запущений при оцінці CSSE; CSSAs використовує CSSV для опису ситуації макро-кібербезпеки засобом всеохоплюючого розрахунку результатів CSSAw; CSSF використовує CSSV у якості джерела даних. Повний цикл роботи CSSE показаний на рисунку 1.4.

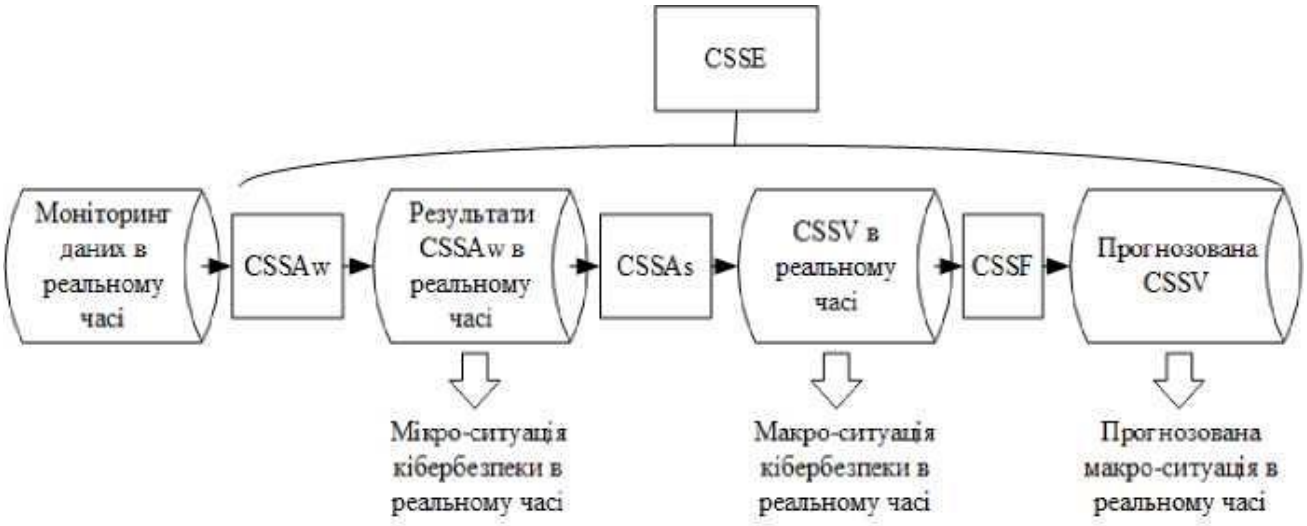


Рисунок 1.4 - Схематичне зображення циклу роботи CSSE

Відмінною рисою аналізу кібербезпеки такого класу інформаційних систем, як автоматизовані системи управління технологічними процесами (АСУТП) є пересічення задач безпеки функціонування об'єкта управління (ОУ), функціональної безпеки апаратно-програмних засобів захисту та інформаційної безпеки. При цьому кінцевою метою та критерієм виконання задач кібербезпеки є забезпечення правильного та надійного функціонування ОУ.

Логіко-імовірнісний підхід. Даний підхід включає в себе аналіз наслідків кібератак з урахуванням їх впливу на промислову безпеку з точки зору надійності та безпеки функціонування ОУ та на кількісні економічні показники. Такий підхід до аналізу кібербезпеки АСУТП є функціональним та ризико-орієнтованим та пропонує вирішення задач оцінки не тільки успішності чи провальності самої кібератаки, але і збереження стійкого функціонування АСУТП та ОУ шляхом їх адаптації до результатів несанкціонованого вторгнення [6].

Аналогічно з визначенням логіко-імовірнісної теорії безпеки (ЛІТ) професора Рябініна І. А., суть логіко-імовірнісного підходу до аналізу кібербезпеки проявляється у формуванні основних закономірностей розвитку знань про можливі зміни станів технічної системи не лише в умовах нормальної експлуатації, але й при наявності:

– зовнішніх впливів;
– порушень правил експлуатації;
– умисних шкідливих дій порушника (загроз, атак).

Першочерговою задачею ЛІТ кібербезпеки технічних систем є розробка методів розрахунку показників безпеки. Враховуючи необхідність розробки особливих, властивих лише задачам інформаційної безпеки, методів аналізу кібератак, та враховуючи те, що кінцевою метою аналізу є забезпечення саме надійного функціонування ОУ, варто при аналізі ризиків, пов'язаних з відмовами АСУТП, оцінювати технічний ризик, показники якого визначаються відповідними методами теорії надійності. При цьому методи аналізу надійності технічних систем рекомендується поєднувати з методами моделювання аварій та кількісною оцінкою ризику аварій.

## 1.2. Стандарти аналізу ризиків

Практично всі сучасні стандарти в області безпеки відображають спільний підхід до організації управління ризиками, що склався у міжнародній практиці.

Вважається, що міжнародні стандарти, створені на основі аналізу та узагальнення найкращих методів, апробованих, як великими групами професіоналів так і провідними організаціями на практиці, в більшості випадків визначають найкращі варіанти дій при виникненні інцидентів в інформаційній безпеці. Використання стандартів збільшує цінність створюваної інформаційної системи або технології, але немає таких стандартів, які б охопили всі аспекти управління, безпеки та якості.

### 1.2.1 Стандарт NIST SP 800-30

Метод NIST (National Institute of Standards and Technology).

Метод Національного інституту стандартів і технологій (NIST) - це метод оцінки ризику інформаційної безпеки національного органу з питань стандартів США. NIST відповідає за просування стандартів та керівних принципів, а також мінімальних вимог до інформаційної безпеки, особливо до інформаційних систем. Ці стандарти та керівні принципи управління ризиками інформаційної безпеки дають вказівки щодо інтегрованої, керованої інформацією організації організацій інформаційної безпеки. Принципи систем кібербезпеки, розроблені NIST у тісній співпраці з приватним та державним секторами у 2013-2014 роках, реалізують процес управління ризиками .

Ця система добровільно використовується приватними агентствами США, але вона вимагається державними установами та установами США. Оскільки ці норми призначені для вирішення питань кібербезпеки критичної інфраструктури, вони широко поширені в інших країнах та регіонах світу. Система відповідає чинним стандартам NIST та керівним принципам управління ризиками інформаційної безпеки та доповнена передовими практиками.

Даний метод вимагає попередньої оцінки двох параметрів: імовірність інциденту; потенційний збиток. Процес управління ризиками інформаційної безпеки, запропонований даним методом представлено на рисунку 1.5.

До переваг даного методу можна віднести:

– простота реалізації та здатність зосередити зусилля на результативності та ефективності процесів;

– забезпечення довіри клієнтів та інших зацікавлених сторін щодо стабільної роботи організації;

– детальний опис всіх можливих ризиків проаналізованих інформаційних активів;

– пропонує використання усіх можливих типів зниження ризиків таких, як перенесення, прийняття, уникнення або зниження ризику;

– зменшення витрат і тривалості циклу загального керування організацією, за рахунок ефективного використання ресурсів; – послідовне й

передбачуване збільшення результатів; – забезпечення можливостей для фокусування і пріоритетності ініціатив щодо поліпшення діяльності організації;

– відносно легке та зручне у використанні та застосуванні програмне забезпечення;

– порівняно мала вартість ліцензії з-поміж інших подібних експертних систем – $ 149 – $ 254.

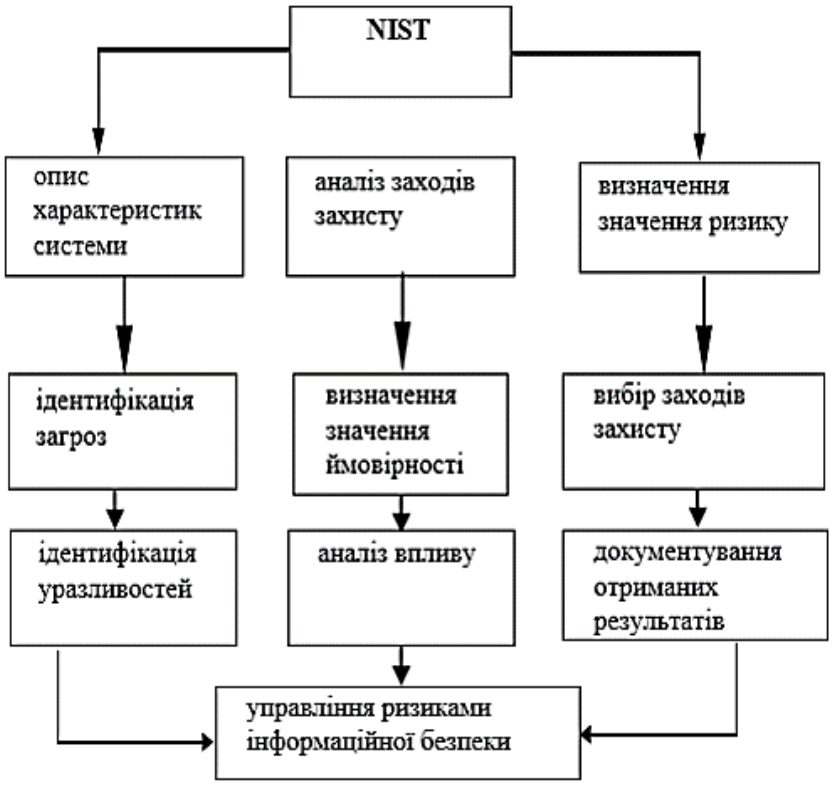


Рисунок 1.5 - Порядок роботи методу NIST по етапах

Недоліки методу NIST: – аналіз забирає багато часу; – вимогливий до компетентності користувача в області інформаційної безпеки.

Процесний підхід охоплює взаємодію, а також систематичне визначення та управління процесами. Для досягнення бажаних результатів - зменшення ризиків інформаційної безпеки - розробити політику інформаційної безпеки, яка повністю доповнює всі аспекти організації, беручи до уваги положення чинних відповідних

документів щодо управління ризиками, які довели свою ефективність та ефективність.

Можна використовувати цикл PDCA (Plan-Do-See-Law, Plan-Do-See-Law, також відомий як цикл Шухарта-Демінга) для здійснення загального управління процесами та системою.

Вибрані входи та виходи можуть бути типу (наприклад, пристрій, пристрій чи пристрій) або невидимі (наприклад, енергія чи інформація). Вихід також може бути ненавмисним, наприклад, відходи або забруднення. Кожен процес має клієнтів та інших зацікавлених сторін, які можуть перебувати всередині або поза організацією. Процесний підхід також фокусується на потребах, очікуваннях та вимогах, які є вхідними в процес процесами, що визначають результати, результати та основні результати процесу.

Ядро процесу, ядро шляху процесу, система повинна використовувати отримані дані для зворотного зв'язку продуктивності процесу. Ці дані слід проаналізувати, щоб визначити, чи потрібні поліпшення та запобіжні заходи, або для покращення роботи системи. Усі процеси слід порівнювати з цілями організації, рівнями та складністю, і повинні бути розроблені для додавання вартості організації.

Ефективність та результативність організації (як процесу) можна оцінити за допомогою внутрішніх або зовнішніх оглядів, які є частиною загального процесу управління організацією. Розуміння процесуального підходу випливає з того факту, що він є потужним організаційним інструментом і спрямований на управління діяльністю, яка створює або додає вартість для споживачів та інших зацікавлених сторін. Організації часто утворюються відповідно до керівництва блоком роботи, елементом якого є структура організації. Організаціями, як правило, керують вертикально, виконуючи роль прогнозування результативності, яка поділяється на обмеження ефективності (підрозділи організаційної структури: підрозділи з волонтерами та постійною роботою) .

Кінцеві користувачі або інші зацікавлені сторони не завжди можуть бути видимими для всіх учасників. Отже, проблеми, що виникають під час процесу сегментації, часто менш важливі, ніж короткострокові цілі. Поліпшення для

зацікавленої сторони майже не відбувається, оскільки дії, як правило, зосереджуються на виконаній роботі, а не на запланованому результаті. Процесний підхід створює горизонтальний контроль (на відміну від вертикальних зв'язків), перетинаючи бар'єри між різними блоками роботи та зосереджуючись на ключових організаційних цілях. Це також покращує інтегроване управління процесами. Організаційна ефективність зростає завдяки використанню технологічних методів. Обробляє системи управління, конкретні технологічні мережі та взаємодії, щоб створити глибше розуміння доданої вартості організації.

NIST рекомендує надавати пріоритет управлінню безпекою відповідно до ключових засобів контролю. Крім того, надання громадськості інформації про пріоритети основних вимог безпеки та контролю може призвести до шкоди, не розповсюджуючи конфіденційну інформацію порушникам, агентам та опонентам. Однак ця прозорість створює враження прозорості у стратегіях державного захисту.

Підхід NIST до управління ризиками надає торговцям добре спланований, добре спланований та простий у виборі процес вибору відповідної системи управління безпекою. Підхід NIST визначає ефективність контролю та видимість прозорості та визначення залишкового ризику для діяльності організацій, фондів та приватних осіб. Розгортання контролю безпеки захищає всі об'єкти інформаційної системи від кіберзагроз, використовуючи комплексний, інтегрований підхід до безпеки, який поєднує в собі управління, продуктивність, технологію та заходи безпеки.

Збалансований підхід до вибору та впровадження засобів управління показує, що ця технологія не може захистити інформаційні системи. Сучасний бізнес потребує комплексного підходу до захисту критично важливих активів та ділових функцій, які охоплюють людей, процеси та технології та які підтримують та зміцнюють їх таким чином. Сьогодні в галузі безпеки відомі три категорії документів NIST: - Спеціальна публікація NIST SP 800 Комп'ютерна безпека, - Спеціальна публікація NIST SP 500 Комп'ютерні системи, - Спеціальна публікація NIST SP 1800 Практичні рекомендації Інтернет-безпека. Ця серія охоплює

комп’ютерну / мережеву / безпекову безпеку та надає керівництво, керівництво та інформацію експертам з безпеки в сучасних інформаційних системах.

Кількість документів: Спеціальна публікація NIST SP 500 Computer System Technologies-2, Спеціальна публікація NIST SP 1800 - Відповідні вказівки щодо мережевої безпеки-8, Спеціальна публікація NIST SP 800 Комп’ютерна безпека та зміни, вдосконалення та нові розробки. Сприяння політиці та процедурам безпечної безпеки є одним із найважливіших факторів у створенні ефективного плану захисту інформації. Політика безпеки відображає чіткі та однозначні правила, незважаючи на публічність, а організована команда демонструє прагнення та прагнення всіх працівників забезпечити інформаційну безпеку. Політика безпеки стосується захисту діяльності організації (через встановлену місію, професію, посаду та репутацію) та активів приватних осіб, інших організацій, загалом інтересів держави, інтересів держави (держави) . рахунок. Процедури безпеки використовуються бізнес-професіоналами для ефективної реалізації політики безпеки. Відповідна політика та процедури та основні навички управління безпекою забезпечують всебічний і всебічний захист систем корпоративної інформаційної безпеки та управління ризиками.

NIST SP 800-30 та NIST SP 800-60 - загальноприйняті технології. NIST SP 800-30 в основному фокусується на комп'ютерних системах. Команда експертів збирає інформацію з Інтернету та від людей, що працюють в організації. Ці цифри використовуються як початкові значення та обробляються відповідно до зазначеного вище.

NIST SP 800-39 описує практичний алгоритм. Попередніми даними для цієї методики є аналіз впливу збитків, ідентифікація ресурсів та оцінка важливості інформації. Використовуйте цю інформацію для встановлення рівня ресурсу. Тоді ступінь компромісу та доцільність запланованих або існуючих заходів безпеки на основі виявленої експлуатаційної загрози є безпосередньою оцінкою ризику. Після початку оцінки ризику визначаються запропоновані заходи безпеки та готуються звітні документи. Це створює захисний малюнок. Метод NIST SP 800-39 найкраще підходить для управління ризиками інформаційної безпеки, оскільки він розглядає

майже всі методи розкриття інформації. Також перевага цієї технології полягає в тому, що вона може використовуватися підприємствами та іншими організаціями. Недоліками цього підходу може бути те, що процес аналізу є дуже тривалим, а інші функції автоматично відсутні.

Метою NIST SP 800-53A є встановлення загальної процедури оцінки ефективності засобів контролю в інформаційних системах. Зокрема, ці заходи контролю перелічені в іншому спеціальному дописі в цій колонці, NIST SP 800-53. Методи та процедури оцінки використовуються для забезпечення належного впровадження засобів контролю безпеки, функціонування, як очікувалося, та дотримання процедур та вимог безпеки організації для досягнення бажаних результатів.

Організація використовує рекомендовану процедуру оцінки та NIST SP 800-53A як вихідну точку для полегшення більш конкретних процедур оцінки. Процедури оцінки NIST SP 800-53A можуть бути доповнені на основі оцінки ризику організації, якщо це необхідно. Організації повинні встановити додаткові процедури для оцінки заходів безпеки, відсутніх у NIST SP 800-53. Використання стандартизованих процедур оцінки дозволяє забезпечити більш послідовну роботу, яку можна порівняти з результативною оцінкою безпеки інформаційних систем. Метою спеціальної публікації NIST SP 800-53A є надання вказівок щодо використання систем управління ризиками управління інформацією, включаючи заходи класифікації безпеки, вибір та впровадження заходів контролю безпеки, оцінку безпеки заходів контролю та затвердження інформаційної системи. І аутентифікація заходів контролю безпеки.

### 1.2.2 Методологія FRAP

Методологія FRAP (Facilitated Risk Analysis Process) є відносно спрощеним способом оцінки ризиків, з фокусом тільки на найкритичніших активах. Якісний аналіз проводиться за допомогою експертної оцінки.

Методика "Facilitated Risk Analysis Process (FRAP)" пропонована компанією Peltier and Associates (розроблена Томасом Пелтієр (Thomas R. Peltier) У методиці, забезпечення ІБ ІВ пропонується розглядати в рамках процесу управління ризиками. Управління ризиками в сфері ІБ - процес, що дозволяє компаніям знайти баланс між витратами коштів і сил на засоби захисту і одержуваних ефектом.

Управління ризиками має починатися з оцінки ризиків: належним чином оформлені результати оцінки стануть основою для прийняття рішень в області підвищення безпеки системи.

Після завершення оцінки, проводиться аналіз співвідношення витрат і одержуваного ефекту (англ. Cost / benefit analysis), який дозволяє визначити ті засоби захисту, які потрібні, для зниження ризику до прийнятного рівня.

Нижче наведені основні етапи оцінки ризиків. Даний список багато в чому повторює аналогічний перелік з інших методик, але у FRAP більш докладно розкриваються шляхи отримання даних про систему і її слабкі місця.

Визначення активів що захищаються проводиться з використанням опитувальних листів, вивчення документації на систему, використання інструментів автоматизованого аналізу (сканування) мереж.

Ідентифікація загроз. При складанні списку загроз можуть використовуватися різні підходи:

– заздалегідь підготовлені експертами переліки загроз (checklists), з яких вибираються актуальні для даної системи;

– аналіз статистики пригод в даній ІС і в подібних їй - оцінюється частота їх виникнення; по ряду загроз, наприклад, загрозу виникнення пожежі, подібну статистику можна отримати у відповідних державних організацій;

– "Мозковий штурм", що проводиться співробітниками компанії.

Коли список загроз закінчений, кожної з них зіставляють ймовірність виникнення. Після чого оцінюють збиток, який може бути нанесений даної загрозою. Виходячи з отриманих значень, оцінюється рівень загрози.

При проведенні аналізу, як правило, приймають, що на початковому етапі в системі відсутні кошти і механізми захисту. Таким чином оцінюється рівень ризику для незахищеної ІС, що надалі дозволяє показати ефект від впровадження засобів захисту інформації (СЗІ).

Оцінка проводиться для ймовірності виникнення загрози і шкоди від неї за наступними шкалами.

Імовірність (Probability):

– Висока (High Probability) - дуже ймовірно, що загроза реалізується протягом наступного року;

– Середня (Medium Probability) - можливо загроза реалізується протягом наступного року;

– Низька (Low Probability) - малоймовірно, що загроза реалізується протягом наступного року.

Збиток (Impact) - міра величини втрат або шкоди, що завдається активу:

– Високий (High Impact): зупинка критично важливих бізнес-підрозділів, яка призводить до істотного збитку для бізнесу, втрати іміджу або неотримання істотного прибутку;

– Середній (Medium Impact): короткочасне переривання роботи критичних процесів або систем, що призводить до обмежених фінансових втрат в одному бізнес-підрозділі;

– Низький (Low Impact): перерва в роботі, що не викликає відчутних фінансових втрат.

Оцінка визначається відповідно до правила, що задається матрицею ризиків, зображеної на рис. 2. Отримана оцінка рівня ризику може інтерпретуватися наступним чином:

– рівень А - пов'язані з ризиком дії (наприклад, впровадження СЗІ) повинні бути виконані негайно і в обов'язковому порядку;

– рівень В - пов'язані з ризиком дії повинні бути зроблені;

– рівень C - потрібно моніторинг ситуації (але безпосередніх заходів з протидії загрозі приймати, можливо, не треба);

– рівень D-ніяких дій в даний момент робити не потрібно.

Після того, як буде опублікована оцінка загрози та ризику ідентифікації, вам слід попросити визначити заходи пом'якшення. Для цього важливо дотримуватись законодавчих обмежень або положень обов'язкового портового законодавства, можна оцінити той самий ризик, щоб визначити очікуваний ефект, але запропонована ГІС враховується. Інші ГІС, можливо, доведеться припинити, якщо не існує ризику скорочень. Поряд із визначенням методу лікування важливо визначити, які витрати будуть понесені на його доступність та реалізацію (вартість може бути як доріжка. Важливо також оцінити, чи безпечний цей препарат, а не створювати нову вразливу систему. .

З точки зору практичного застосування можна виділити такі переваги методу FRAP:

– Простота і прозорість процесу аналізу та оцінки ризиків дозволяє приступити до реалізації процесу в стислі терміни без необхідності тривалого вивчення методики та документації по ній;

– Мінімальні трудовитрати на виконання аналізу і оцінки ризиків дозволяють реалізувати процеси без істотних витрат;

– Залучення невеликої кількості учасників дозволяє мінімізувати витрати на організацію спільної роботи, комунікації всередині проектної команди і узгодження результатів з усіма зацікавленими особами.

При цьому методології FRAP притаманні такі недоліки:

– Відсутність жорстко регламентованого процесу управління ризиками інформаційної безпеки та докладних допоміжних матеріалів, таких як каталоги загроз, вразливостей, наслідків, заходів забезпечення інформаційної безпеки знижують повторюваність результатів аналізу ризиків інформаційної безпеки і підвищують значимість наявності спеціальних знань і компетентності безпосередніх виконавців заходів з аналізу та управління ризиками;

– Відсутність можливості глибокої декомпозиції, докладної і точної оцінки ризиків ускладнює можливість точкового застосування мінімального необхідного набору заходів та засобів захисту, що може негативно вплинути на загальну економічну ефективність системи інформаційної безпеки;

Відсутність можливості оцінки ризиків в грошах ускладнює використання результатів оцінки ризиків інформаційної безпеки при розрахунку техніко-економічного обґрунтування інвестицій, необхідних на впровадження засобів і методів захисту інформації

### 1.2.3 Методологія ISO 2700x

Більша частина програмних експертних систем відповідають стандарту ISO / IEC 27001:2005. Дані стандарти формулюють вимоги до систем управління інформаційною безпекою, процесу управління ризиками, основні метрики і способи вимірювання, а також керування їх впровадженням.

Ключова модель, що використовується для керування ризиками інформаційної безпеки це модель, яка була відображена у всіх стандартних підходах до управління ризиками інформаційної безпеки і є основою ISO / IEC 27005 і BS 7799–3. В цій моделі вказано перелік та черговість використання ключових для управління ризиками інформаційної безпеки процесів, серед яких планування, реалізація, перевірка, дія .

Згідно з цим стандартом вся документація, яка окреслює межі керування інформаційними ризиками установи, повинна включати: – задокументовану заяву, або її копію, про політику та мету системи управління інформаційною безпекою; – функціональної особливості програми системи управління інформаційною безпекою; – процедури і інструменти управління для підтримки системи управління інформаційною безпекою; – опис методики оцінки інформаційних ризиків; – звітність по аналітичних оцінках ризиків; – схеми використання контрзаходів. Даний стандарт створений як модель для функціонування системи забезпечення інформаційної безпеки. Крім вищезгаданого міжнародного стандарту можна

перерахувати ще багато схожих стандартів, які співіснують та взаємодоповнюють один одного у галузі забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах.

Таблиця 1.2

Міжнародні стандарти з управління інформаційними ризиками

| Стандарт | Назва стандарту | Коротка характеристика |
|---|---|---|
| ISO / IEC 27002–2012 | Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій | Цей стандарт надає додаткові рекомендації з реалізації та менеджменту інформаційної безпеки в підприємствах. Визначає вимоги оцінки ризику до системи інформаційної безпеки та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, підтримку й покращення менеджменту. |
| ISO / IEC 27003–2012 | Інструкція з реалізації системи менеджменту інформаційної безпеки | У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІВ відповідно зі стандартом ISO / 1EC 27001:2005, який розглядає процес визначення та розробку СМІВ від початку до стану впровадження. |
| ISO / IEC 27004–2011 | Менеджмент інформаційної безпеки вимірювання | Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІВ. Процес вимірювання реалізується у вигляді програми, пов’язаний з інформаційною безпекою. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІВ |
| 1SO / IEC 27005–2010 | Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику | Цей стандарт поданий у вигляді додатку для виявлення типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків асоціюється з стандартом BS 7799, а саме з його двома частинами: першою BS 7799–1 «Звіт правил з менеджменту безпеки інформації» та другою – BS 7799–2 «Системи менеджменгу безпекою інформації», у яких |

| | | |
|---|---|---|
| | | вперше питання аналізу стану безпеки інформації та формування її захисту були пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799–3 «Настанови з менеджменту ризиками безпеки інформації». |
| ISO / IEC TR 13335–2:1997 | Настанови з керування безпекою інформаційних технологій (IT) | Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій. |

Стандарт ISO / IEC 27001:2013 описує загальну методологію підходу до забезпечення інформаційної безпеки в організації і акцентує увагу на найбільш критичних складових інформаційної системи. Він охоплює елементи управління системою інформаційної безпеки, актуальні для всіх без винятку сфер бізнесу, такі як: – політика інформаційної безпеки; – розподіл відповідальності за інформаційною безпекою; – проведення навчання в цій області; – звітність по інцидентах; – захист від вірусів; – забезпечення безперервності роботи; – контроль копіювання ліцензійного програмного забезпечення, – захист архівної документації та захист персональних даних. Цей стандарт дає компанії інструмент, що дозволяє управляти конфіденційністю, цілісністю і збереженням такого важливого активу компанії як інформація.

Елементи управління системою інформаційної безпеки розділені в стандарті по декількох групах, і включають в себе розділи:

– політика безпеки – підтримка політики у сфері інформаційної безпеки з боку керівництва підприємства;

– інфраструктура системи безпеки – створення організаційної структури, яка буде забезпечувати працездатність системи інформаційної безпеки в організації;

– класифікація ресурсів і управління – пріоритизація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;

– співробітники – зниження ризику людських помилок, крадіжки і неправильного використання устаткування;

– фізична і зовнішня безпека – запобігання несанкціонованого доступу та порушення роботи інформаційної системи організації.

Стандарт складається з двох частин: в першій частині описані механізми контролю, необхідні для побудови системи управління інформаційною безпекою. Ця частина використовується в якості основи для проведення аудиту системи інформаційної безпеки в організації. У другій частині стандарту описуються ті критерії, по яких проводиться сертифікація системи інформаційної безпеки. Виходячи з ідеології стандарту ключовим елементом системи інформаційної безпеки є система управління ризиками, найважливішою частина яких є аналіз цих ризиків з метою визначення, які ресурси від яких загроз необхідно захищати, а також якою мірою ресурси потребують захисту.

Проведення аналізу ризиків дозволяє організації оцінити можливі збитки в кількісних і якісних показниках. Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення системи управління інформаційною безпекою. Передбачається, що прийняття системи інформаційної безпеки є стратегічним для організації. Стандарт приймає процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані і поліпшення системи інформаційної безпеки організації.

Стандарт рекомендує проводити постійний контроль результативності системи управління інформаційною безпекою, аналіз цілей управління, беручи до уваги результати аудиту та статистику виникнення порушень. У відповідності з стандартом ISO / IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе: – документовану заяву про політику та цілі системи управління інформаційною безпекою; – область програми системи управління інформаційною безпекою; – процедури і засоби управління на підтримку

системи управління інформаційною безпекою; – опис методології оцінки ризиків; – звіт про оцінки ризиків; – план обробки ризиків.

В стандарті наголошується відповідальність керівництва в організації управління інформаційними ризиками. У розділі розглядаються види зобов'язань керівництва, деякі принципи менеджменту ресурсів і забезпечення необхідного рівня компетентності персоналу. Стандарт розглядає основні цілі та принципи проведення аудиту захищеності організації від загроз в інформаційній сфері, а також аналіз системи управління інформаційною безпекою з точки зору керівництва. У стандарті зазначено основні вхідні і вихідні дані для внутрішнього аудиту. В якості важливих результатів аудиту можна виділити оновлення оцінки ризиків для організації та відповідно зміну методів управління ними. Заключна частина стандарту присвячена принципу постійного поліпшення в системі управління інформаційною безпекою.

## 1.3 Порівняння методів оцінки ризиків

У таблиці 1.3 наведено матрицю критеріїв вибору вищеописаних методів, які слід враховувати при їх використанні для оцінки ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури у сфері ядерної енергетики.

Проаналізувавши методом порівняння вищенаведені інструментальні засоби оцінювання ризиків, можна визначити найпоширеніші недоліки, серед яких можна виділити: – складний процес отримання даних – потрібно довший час, ретельно оцінювати зміни в системі для отримання коректних результатів; – при постійному оновленні програмного забезпечення, інформаційне середовище, в якому проходить процес аналізу, зазнає відчутних змін, в порівнянні з первинним виглядом – витрати часу для проведення аналітики, здебільшого не відповідає вимогам шо до швидкості реагування на виявлені.

Таблиця 1.3

Критерії вибору методів аналізу ризиків

| Критерії | Методи | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Метод Дельфі | FRAP | NIST | Імітаційне моделювання та імовірність виконання | Метод CORAS | Метод ситуаційного аналізу кібербезпеки | Логіко-імовірнісний підхід | Імовірнісний аналіз безпеки |
| Аналіз потоків даних в інформаційній системі | - | + | - | - | + | + | - | - |
| Побудова функціональної моделі системи | - | - | + | + | + | + | + | + |
| Кількісна оцінка ризиків | - | + | - | + | + | + | + | + |
| Якісна оцінка ризиків | + | + | + | - | + | - | + | + |
| Оцінка існуючих заходів безпеки | + | - | + | + | + | + | + | + |
| Збір / використання статистичних даних | + | + | _ | + | + | + | - | + |
| Проведення експериментів / тестування | - | + | - | + | - | - | - | - |
| Врахування зовнішніх впливів (людський фактор) | + | _ | - | - | + | - | + | + |
| Оцінка надійності технічних систем | - | - | - | + | - | - | + | + |
| Прогнозування | - | + | + | + | - | + | - | + |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| стану кібербезпеки | | | | | | | | |
| Реалізація управління ризиками | - | + | + | - | + | + | + | + |
| Економічна оцінка захисту інформації | + | - | - | + | + | - | + | - |
| Застосовність для оцінки ризиків кібербезпеки | + | - | - | + | + | + | + | - |

Якщо ж говорити про кількісні методи оцінювання інформаційних ризиків, можна зробити висновки, що дані методи досить таки не точні, та зовсім не надійні. І ось основні причини: – для кількісної оцінки дуже складно зібрати актуальні дані, що пов’язано з потребою їх точної реєстрації на великому проміжку часу; – сучасне інформаційне середовище швидко змінюється в зв’язку з невпинним вдосконаленням програмного забезпечення – час, витрачений для аналізу зазвичай досить великий.

Серед переваг методу Дельфі можна виділити те, що якісний підхід дозволяє оцінити специфіку кожної конкретної ситуації. В деяких випадках поглиблене дослідження різних елементів, що визначають ситуацію, може бути більш важливим, ніж проведення систематичної кількісної оцінки. Даний метод стимулює незалежне мислення членів експертної групи та дозволяє отримати зважену оцінку розглянутого питання .

До недоліків можна віднести надлишкову суб’єктивність оцінок – під час прийняття рішень будь-які риси чи вподобання експертів можуть мати суттєвий вплив на результати оцінок. Також основним обмеженням використання методу є складність підбору великої групи експертів, які володіють необхідною компетенцією в досліджуваному питанні.

Можна зробити висновок, що метод Дельфі можна застосовувати в сфері забезпечення інформаційної безпеки, але лише для поверхневого аналізу ризиків. В

той же час комбінуючи даний метод з іншими можна отримати результат з широким покриттям можливих варіацій досліджуваної проблеми.

Основною перевагою імітаційного моделювання та імовірності виконання є те, що він надає можливість виконати експеримент в той час, як проведення реальних експериментів практично неможливе. Це дозволяє отримати спрощену оцінку імовірності виконання. Якщо даних для проведення експериментів недостатньо, вони генеруються машинним методом. В свою чергу, використання імітаційного підходу створює імовірність того, що оцінка ризику буде виконана не повністю або не будуть охоплені усі необхідні ризики.

Даний метод має місце для застосування у сфері інформаційної безпеки. Його використання може дати попередню оцінку вразливості інформаційних систем, оскільки є можливість проведення моделювання реалізації загрози інформаційної безпеки без взаємодії з реальною системою.

Метод CORAS відноситься до категорії інформаційних методів, та застосовується для здійснення аналізу ризиків з використанням усіх основних етапів аналізу кібербезпеки. Як перевагу можна виділити використання методики «мозкового штурму», яка включає залучення експертів різної компетенції, уподобань, схильності та суджень, що дозволяє виділити більшу частину специфіки досліджуваного об’єкту при проведенні аналізу ризиків.

Як недолік можна виділити специфіку застосування методу. Для використання у сфері ядерної енергетики потребується перегляд та доопрацювання стандартів, покладених у його основу.

Метод ситуаційного аналізу кібербезпеки може відображати в режимі реального часу загрози кібербезпеки всіх типів мережевих атак на мікро- рівні, інформувати про атаки на макро-рівні та прогнозувати майбутні загрози на глобальному рівні. Даний метод доцільно використовувати в активній системі захисту від кіберзагроз, його реалізація надає вирішення проблем кібербезпеки, які виникають при побудові інтелектуальних мереж.

З точки зору застосування на об’єктах критичної інформаційної інфраструктури, даний метод обмежений забезпеченням кібербезпеки лише на

мережевому рівні. У ньому не враховуються ризики, пов’язані із відмовами по загальним причинам, діями персоналу, іншими зовнішніми впливами.

Даний метод має місце застосування, як частина комплексу забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури, в тому числі у сфері ядерної енергетики.

Логіко-імовірнісний підхід застосовується для аналізу кібербезпеки автоматизованих систем управління технологічними процесами, що дає підстави для його використання при проведенні аналізу кібербезпеки об’єктів критичної інформаційної інфраструктури у сфері ядерної енергетики. Важливо, що даний підхід враховує оцінку надійності та ризику технічних систем, враховуються відмови по загальній причині при аналізі надійності резервуючих систем в задачах аналізу функціональної безпеки.

Імовірнісний аналіз безпеки дозволяє виявити, охарактеризувати та оцінити імовірні ризики експлуатаційної безпеки АЕС. ІАБ сприяє більш чіткому розумінню взаємодії обладнання та персоналу при нормальному режимі експлуатації та при аварійних режимах. Також дозволяє виявити «вразливі» місця в обладнанні систем, що в свою чергу є основою для розробки заходів, які направлені на підвищення безпеки.

Даний метод розглядається з точки зору забезпечення функціональної та фізичної безпеки об’єктів. Проведення аналізу кібербезпеки потребує використання інших методів, або їх комбінацію з ІАБ.

## 1.4 Постановка задачі

Мета даного дослідження полягає в розробці моделі ідентифікації ризиків кібербезпеки у інформаційних системах. При цьому проведений в першому розділі аналіз дозволяє зробити висновок, що розроблювана модель має бути придатною для проведення ідентифікації ризиків кібербезпеки, простою та доступною у використанні. При цьому результат використання моделі має давати як кількісну так і якісну характеристику ризиків кібербезпеки.

Задля досягнення поставленої мети в ході виконання кваліфікаційної магістерської роботи необхідно розробити модель, яка б дала змогу ідентифікувати ризики кібербезпеки у інформаційних системах.

Відповідно до мети роботи, вирішувались наступні завдання:

- аналіз існуючих світових стандартів у сфері кібербезпеки щодо ідентифікації ризиків та оцінки загроз;
- приведення даних до узагальненого;
- розробка алгоритму ідентифікації ризиків у ІС;
- синтез моделі ідентифікації ризиків на основі проаналізованих стандартів.
- аналіз адекватності синтезованої моделі

**Висновки до розділу 1**

В даному розділі було описано та коротко охарактеризовано основні методи ідентифікації ризиків. Детально описано особливості таких методів, як NIST, FRAP та ISO 2700x. Наведено їх характеристики, вказано переваги та недоліки.

# РОЗДІЛ 2
# РОЗРОБКА МОДЕЛІ ІДЕНТИФІКАЦІЇ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІС

Ідентифікація ризику - це процес виявлення, дослідження та опису ризиків.

Етап ідентифікації ризиків полягає в систематичному виявленні та вивченні ризиків, які характерні для певного виду діяльності, схильною до ризикового впливу.

Ключовими, в представленому визначенні, є словосполучення - «систематичне виявлення» і «вивчення ризиків». Вони наголошують на необхідності в постійній і комплексну роботу в даному напрямку. Тільки наявність саме «таких» процесів дозволить гарантувати досягнення поставлених результатів діяльності з управління ризиками

Мета ідентифікації ризику - визначити, що могло б статися при нанесенні можливого збитку, і отримати уявлення про те, як, де і чому міг мати місце цей збиток. Етапи, описані нижче, повинні об'єднувати вхідні дані для діяльності по кількісній оцінці ризику.

У процесі ідентифікації повинні брати участь члени команди проекту та експерти з питань управління ризиками. У ній можуть брати участь замовники, учасники проекту та експерти в певних областях. Залучення додаткових сторін до процесу ідентифікації допоможе виробити почуття власності і відповідальності за ризики, і за дії з реагування на них у всіх зацікавлених сторін.

Алгоритм яким можна буде керуватися при здійсненні процесу ідентифікації ризиків, можна подати наступним чином:

- Визначення активів
- Визначення загроз
- Визначення існуючих заходів і засобів контролю та управління
- Виявлення вразливостей

- Визначення наслідків
- Визначення значень ризиків
- Оцінка наслідків
- Оцінка ймовірності інциденту
- Встановлення значень рівня ризиків

## 2.1 Визначення активів

Активом є що-небудь, що має цінність для організації і, отже, потребує захисту. При визначенні активів слід мати на увазі, що інформаційна система складається не тільки з апаратних і програмних засобів.

Активи повинні бути ідентифіковані з точним рівнем інформації, щоб забезпечити достатньо інформації для оцінки ризику. Кількість інформації, яка використовується для визначення активу, впливає на загальну інформацію, зібрану під час оцінки ризику. Ця інформація може бути детально розроблена під час наступних заходів з оцінки ризику.

Для встановлення облікової та відповідальності щодо кожного активу повинен бути визначений власник. Власник активу може не мати права власності на актив, але він несе відповідальність за його отримання, розробку, підтримку, використання і безпеку. Найчастіше власник активу є найбільш підходящим особою, яка спроможна визначити реальну цінність активу для організації

Кордоном аналізу є периметр активів організації, керований в рамках процесу менеджменту ризику ІБ.

Вхідні дані. Сфера дії та межі проведення оцінки ризику, перелік, що включає власників, місце розташування, функцію і т.д.

Дія. Повинні бути визначені активи, що входять до встановлену сферу дії.

Керівництво по реалізації. Вихідні дані. Перелік активів, що підлягають менеджменту ризику, і перелік бізнес-процесів, пов'язаних з активами, а також їх значимість.

## 2.2 Визначення загроз

Вхідні дані. Інформація про погрози, отримана в результаті аналізу інциденту від власників активів, користувачів, а також з інших джерел, включаючи списки зовнішніх загроз.

Дія. Загрози і їх джерела повинні бути визначені

Загрози можуть завдати шкоди організаційним активам, таким як інформація, процеси та системи. Загрози можуть виникнути внаслідок природної події чи дії людини, а також можуть бути випадковими або навмисними. Вам потрібно виявити джерело всіх нещасних та навмисних загроз. Загрози можуть надходити як від самої організації, так і від джерел за межами периметра. Загрози слід ідентифікувати за типом (наприклад, несанкціонована експлуатація, фізичний збиток, технічний збій) та, якщо потрібно, особисті загрози в межах загального класу. Це означає, що, незважаючи на несподівані загрози, жодні загрози не усуваються, але рівень необхідної роботи все ж зменшився.Деякі загрози можуть впливати більш ніж на один актив. У таких випадках вони можуть бути причиною різних впливів в залежності від того, на які активи вони впливають.

Вхідні дані для визначення і кількісної оцінки ймовірності виникнення загроз (див. 8.2.2.3) можуть бути отримані від власників активів або користувачів, персоналу відділу кадрів, керівництва організації та фахівців у галузі ІБ, експертів в галузі фізичної безпеки, фахівців юридичного відділу та інших структур , а також від юридичних організацій, метеорологічних служб, страхових компаній, національних урядових установ. При аналізі загроз повинні враховуватися аспекти середовища і культури.

Досвід, отриманий з інцидентів, і попередні оцінки загроз повинні бути враховані в поточній оцінці. При необхідності для заповнення переліку загальних загроз може бути доцільним впоратися в інших реєстрах загроз (можливо, специфічних для конкретної організації або бізнесу). Списки загроз і їх статистику можна отримати від промислових підприємств, федерального уряду, юридичних організацій, страхових компаній і т.д.

Використовуючи списки загроз або результати попередніх оцінок загроз, не слід забувати про те, що відбувається постійна зміна значущих загроз, особливо, якщо змінюються бізнес-середовище або інформаційні системи.

Більш детальну інформацію про типи загроз можна знайти в додатку С.

Вихідні дані. Перелік загроз з визначенням їх виду і джерела.

## 2.3 Визначення існуючих заходів і засобів контролю та управління

Вхідні дані. Документація по заходам і засобам контролю і управління, плани по реалізації обробки ризику.

Дія. Повинні бути визначені існуючі та заплановані заходи і засоби контролю і управління.

Керівництво по реалізації. Щоб уникнути зайвої роботи або витрат, наприклад, при дублюванні заходів і засобів контролю та управління, необхідно визначити існуючі заходи і засоби контролю і управління. Крім того, при визначенні існуючих заходів і засобів контролю та управління слід провести перевірку, щоб переконатися в правильності функціонування заходів і засобів контролю та управління - звернення до існуючих звітів по аудиту СМІБ повинні скорочувати час, що витрачається на вирішення цього завдання. Неналежне функціонування заходів і засобів контролю та управління може стати причиною вразливості. Слід приділити увагу ситуації, коли обрані заходи і засоби контролю і управління (або стратегія) не виконують своїх функцій, і для ефективного і своєчасного реагування на ідентифіковані ризики потрібні додаткові заходи і засоби контролю і управління. У СМІБ, відповідно до ISO / IEC 27001, це підтримується виміром ефективності заходів і засобів контролю та управління. Один із способів кількісної оцінки дії заходів і засобів контролю та управління - виявити, як воно знижує ймовірність виникнення загрози, ускладнює використання уразливості і можливості впливу інциденту. Перевірки, проведені керівництвом, і звіти по аудиту також забезпечують інформацію про ефективність існуючих заходів і засобів контролю та управління.

Заходи і засоби контролю і управління, які планується реалізувати відповідно до планів реалізації обробки ризику, повинні бути визначені тим же самим способом, який вже був реалізований.

Існуючі або плановані заходи і засоби контролю і управління можуть бути віднесені до розряду неефективних, недостатніх або необгрунтованих. Якщо їх порахували необгрунтованими або недостатніми, міру і засіб контролю та управління необхідно піддати перевірці, щоб визначити, чи підлягають вони видаленню, заміні більш придатними, або варто залишити їх, наприклад з міркувань вартості.

Для визначення існуючих або планованих заходів і засобів контролю та управління можуть бути корисні наступні заходи:

- перегляд документів, що містять інформацію про засоби контролю (наприклад, плани обробки ризиків), якщо процеси менеджменту ІБ документовані належним чином, то інформація про всіх існуючих або плановані заходи і засоби контролю і управління, а також про стан їх реалізації повинна бути доступна;

- перевірка, яка проводиться спільно з співробітниками, що відповідають за ІБ (наприклад, співробітником, які займаються забезпеченням ІБ, співробітником, відповідальним за безпеку інформаційної системи, комендантом будівлі або керівником робіт) і користувачами, що стосується того, які заходи і засоби контролю і управління дійсно реалізовані для розглянутого інформаційного процесу або інформаційної системи;

- обхід будівлі з метою огляду фізичних засобів контролю, порівняння існуючих засобів контролю з переліком тих, які повинні бути реалізовані, і перевірка існуючих засобів контролю на предмет правильної і ефективної роботи;

- розгляд результатів внутрішніх аудитів.

Вихідні дані. Перелік всіх існуючих і планованих заходів і засобів контролю та управління, їх знаходження і стан використання.

## 2.4 Виявлення вразливостей

Вхідні дані. Переліки відомих загроз, переліки активів і існуючих заходів і засобів контролю та управління.

Дія. Необхідно виявити уразливості, які можуть бути використані загрозами для нанесення шкоди активів або організації [пов'язане з ISO / IEC 27001, пункт 4.2.1, перерахування d) 3)].

Уразливості можуть бути виявлені в наступних областях:

- організація робіт;
- процеси і процедури;
- сталий порядок управління;
- персонал;
- фізичне середовище;
- конфігурація інформаційної системи;
- апаратні засоби, програмне забезпечення та апаратура зв'язку;
- залежність від зовнішніх сторін.

Наявність уразливості саме по собі не завдає шкоди, оскільки необхідна наявність загрози, яка зможе скористатися нею. Для уразливості, якої не відповідає певна загроза, може не знадобитися впровадження засобів контролю та управління, але вона повинна усвідомлювати і піддаватися моніторингу на предмет змін. Слід зазначити, що невірно реалізоване, неправильно функціонує або неправильно використовуваний засіб контролю і управління саме може стати вразливістю. Заходи і засоби контролю і управління можуть бути ефективними або неефективними в залежності від середовища, в якій вони функціонують. З іншого боку, загроза, якої не відповідає певна вразливість, може не призводити до ризику.

Уразливості можуть бути пов'язані з властивостями активу. Спосіб і цілі використання активу можуть відрізнятися від планованих при придбанні або створенні активу. Необхідно враховувати уразливості, що виникають з різних джерел, наприклад ті, які є зовнішніми або внутрішніми по відношенню до активу.

Приклади вразливостей і методи їх оцінки можна знайти в додатку D.

Вихідні дані. Перелік вразливостей, пов'язаних з активами, погрозами і заходами і засобами контролю і управління; перелік вразливостей, які пов'язані з виявленою загрозою, що підлягає розгляду.

## 2.5 Визначення наслідків

Вхідні дані. Перелік активів, бізнес-процесів, загроз і вразливостей, де це доречно, пов'язаних з активами, і їхню соціальну значимість.

Дія. Повинні бути визначені наслідки для активів, викликані втратою конфіденційності, цілісності та доступності

Керівництво по реалізації. Наслідком може бути зниження ефективності, несприятливі операційні умови, втрата бізнесу, збиток, нанесений репутації і т.д.

Ця діяльність визначає збитки або наслідки для організації, які можуть бути обумовлені сценарієм інциденту. Сценарій інциденту - це опис загрози, використовує певну вразливість або сукупність вразливостей в інциденті ІБ . Вплив сценаріїв інцидентів обумовлюється критеріями впливу, обумовленими протягом діяльності по встановленню контексту. Вплив може зачіпати один або кілька активів, а також частина активу. Тому активів може призначатися цінність, обумовлена як їх фінансової вартістю, так і наслідками для бізнесу в разі їх псування або компрометації. Наслідки можуть бути тимчасовими або постійними, як це буває в разі руйнування активів.

Примітка - У ISO / IEC 27001 описується походження сценаріїв інцидентів як "недоліків безпеки".

Організації повинні визначати операційні наслідки сценаріїв інцидентів на основі (але не обмежуючись):

- часу на розслідування і відновлення;
- втрат (робочого) часу;
- втрачену можливість;
- охорони праці та безпеки;

- фінансових витрат на придбання специфічних навичок, необхідних для усунення несправності;

- репутації і іншого "невловимого капіталу".

Подробиці, що стосуються оцінки технічних вразливостей, можна знайти в B.3 (додаток B).

Вихідні дані. Перелік сценаріїв інцидентів з їх наслідками, пов'язаними з активами і бізнес-процесами.

## 2.6 Встановлення значення ризику

Аналіз ризиків може проводитися на різних рівнях інформації залежно від вартості активу, поширеності відомих слабких місць та минулих подій, пов'язаних з організацією. Метод визначення цінних паперів з ризиком може бути стандартним, кількісним або комбінованим, залежно від ситуації. На практиці встановлення значення якості часто використовується спочатку для отримання загальної інформації про рівень ризику та для визначення основних значень ризику. Загалом, результати аналізу якості порівняно з вимірюванням є складними та недорогими, тому пізніше при розрахунку ключових значень ризику може знадобитися більш конкретний аналіз.

Метод аналізу повинен відповідати критеріям оцінки ризику, розробленим як частина навколишнього середовища.

Для встановлення якісного значення використовується шкала кваліфікації атрибутів, за допомогою якої описуються величини можливих наслідків (наприклад низький, середній і високий) і ймовірності виникнення цих наслідків. Перевага встановлення якісного значення полягає в доступності для розуміння всім відповідним персоналом, а недоліком - залежність від суб'єктивного вибору шкали.

Такі шкали можуть бути адаптовані або скориговані відповідно до обставин, для різних ризиків можуть використовуватися різні описи. Встановлення якісного значення може використовуватися:

- як початкова діяльність по ретельній перевірці для ідентифікації ризиків, які потребують більш детального аналізу;

- там, де цей вид аналізу сприяє прийняттю рішення;

- там, де числові дані або ресурси є неадекватними для встановлення кількісного значення.

Якісний аналіз повинен використовувати фактичну інформацію і доступні дані.

Для встановлення кількісної оцінки використовується шкала з числовими значеннями (а не описові шкали, які використовуються при встановленні якісного значення) як наслідків, так і ймовірності, із застосуванням даних з різних джерел. Якість аналізу залежить від точності і повноти числових значень і від обгрунтованості використовуваних моделей. У більшості випадків для встановлення кількісного значення використовуються фактичні дані за минулий період. Перевага полягає в тому, що встановлення кількісного значення може бути прямо пов'язане з цілями інформаційної безпеки і проблемами організації. Недоліки кількісного підходу можуть мати місце, коли фактичні перевіряються дані недоступні, тому створюється ілюзія цінності і точності встановлення кількісного значення ризику.

Спосіб вираження наслідків ризику і ймовірності його виникнення, а також способи їх комбінування для отримання інформації про рівень ризику змінюються в залежності від виду ризику і мети, для досягнення якої повинні використовуватися вихідні дані оцінки ризику. При аналізі ризику слід враховувати невизначеність і змінність наслідків ризику, а також ймовірність його виникнення і повідомляти про них ефективним чином.

## 2.7 Оцінка наслідків

Вхідні дані. Перелік певних значущих сценаріїв інцидентів, включаючи виявлення загроз, вразливостей і порушених активів, а також наслідків для активів і бізнес-процесів.

Дія. Повинно бути оцінено вплив на бізнес організації, яке може бути результатом передбачуваних або фактичних інцидентів ІБ з урахуванням наслідків порушення ІБ, таких, як втрата конфіденційності, цілісності або доступності активів [пов'язане з ISO / IEC 27001, 4.2.1, перерахування e) 1) ].

Керівництво по реалізації. Після визначення всіх перевірених активів, привласнена їм цінність повинна враховуватися при оцінці наслідків.

Значення впливу на бізнес може бути виражено в якісній або кількісній формах. Проте більш наочним є метод присвоєння грошового вираження, який, як правило, дає більше інформації для прийняття рішень і, отже, робить процес прийняття рішень більш ефективним.

Визначення цінності активів починається з класифікації активів відповідно до їх критичністю точки зору важливості активів для здійснення бізнес-цілей організації. Потім цінність активів визначається з використанням двох заходів:

- відновної вартості активу - вартості його очищення з метою відновлення і заміни інформації (якщо це можливо);

- наслідків для бізнесу від втрати або компрометації активу, наприклад можливі несприятливі наслідки для бізнесу та / або законодавчі або регулюють наслідки розкриття, модифікації, недоступності і / або руйнування інформації, а також інших інформаційних активів.

Це визначення цінності може бути встановлено на основі аналізу впливу на бізнес. Цінність, яка визначається наслідками для бізнесу, зазвичай значно вище просто відновної вартості і залежить від значущості активу для організації при виконанні її бізнес-цілей.

Визначення цінності активів є ключовим фактором оцінки впливу сценарію інциденту, оскільки інцидент може торкатися більш одного активу (наприклад, залежні активи), або тільки частина активу. Різні загрози і вразливості можуть мати різний вплив на активи, наприклад втрата конфіденційності, цілісності та доступності. Тому оцінка наслідків пов'язана з визначенням цінності активів або стає пов'язаної, виходячи з аналізу впливу на бізнес.

Наслідки або вплив на бізнес можуть визначатися шляхом моделювання результатів події або сукупності подій, екстраполяції експериментальних досліджень або даних за минулий час.

Наслідки можуть бути виражені за допомогою грошових, технічних персональних критеріїв впливу або інших критеріїв, які є значущими для організації. В окремих випадках для визначення наслідків, що розрізняються за часом, місцем, групам або ситуацій, потрібно більше одного цифрового значення.

Наслідки, що розрізняються за часом або фінансів, повинні вимірюватися з використанням того ж підходу, який застосовується щодо ймовірності загрози і вразливості. Повинна підтримуватися послідовність кількісного або якісного підходу.

У додатку В наводиться більш детальна інформація, що стосується визначення цінності активів і оцінки впливу.

Вихідні дані. Перелік оцінених наслідків сценарію інцидентів, виражених з урахуванням активів і критеріїв впливу.

## 2.8 Оцінка ймовірності інциденту

Вхідні дані. Перелік певних значущих сценаріїв інцидентів, включаючи визначення загроз, які поставлені активи, які використовуються уразливості і наслідки для активів і бізнес-процесів. Крім того, переліки всіх існуючих і планованих заходів і засобів контролю та управління, рівень їх ефективності, реалізації та використання.

Дія. Повинна бути оцінена ймовірність дії сценаріїв інцидентів [пов'язане з ISO / IEC 27001, пункт 4.2.1, перерахування e) 2)].

Керівництво по реалізації. Після визначення сценаріїв інцидентів необхідно оцінити ймовірність дії кожного сценарію і його вплив з використанням якісного або кількісного методу встановлення значення. Необхідно брати до уваги частоту виникнення загроз і простоту використання уразливості, з урахуванням:

- досвіду і відповідної статистики ймовірності виникнення загроз;

- для джерел умисних загроз - мотивації і можливості, які будуть змінюватися з плином часу, ресурсів, доступних для потенційних порушників, а також сприйняття потенційним порушником привабливості і уразливості активів;

- для джерел випадкових загроз - територіальних чинників, наприклад близькість до хімічного або нафтопереробному заводу, можливість екстремальних погодних умов і факторів, які можуть викликати помилки персоналу і збої обладнання;

- вразливостей як окремих, так і в сукупності;

- існуючих заходів і засобів контролю та управління і того, наскільки ефективно вони знижують уразливості.

Наприклад, інформаційна система може мати вразливість по відношенню до погроз імітації особистості користувача та зловживанню ресурсами. Уразливість, пов'язана з імітацією особистості користувача, може бути високою через відсутність аутентифікації користувачів. З іншого боку, ймовірність зловживання ресурсами може бути низькою, незважаючи на відсутність аутентифікації користувачів, оскільки способи зловживання ресурсами обмежені.

Залежно від необхідної точності активи можуть бути згруповані або розбиті на елементи, і може виникати необхідність співвіднесення сценаріїв з елементами. Наприклад в залежності від місця розташування характер загроз щодо одних і тих же видів активів може змінюватися або може відрізнятися ефективність існуючих заходів і засобів контролю та управління.

Вихідні дані. Імовірність дії сценаріїв інцидентів (в кількісному або якісному вираженні).

## 2.9 Встановлення значень рівня ризиків

Вхідні дані. Перелік сценаріїв інцидентів з їх наслідками, що стосуються активів і бізнес-процесів, і їх вірогідність (в кількісному або якісному вираженні).

Дія. Повинні бути встановлені значення рівня ризиків для всіх значущих сценаріїв інцидентів.

Керівництво по реалізації. При встановленні значень ризиків присвоюються значення ймовірності виникнення ризику і його наслідків. Ці значення можуть бути виражені якісно або кількісно.

Встановлення значень ризиків грунтується на оцінених наслідки і їх ймовірності. Крім того, воно може також враховувати вартість і ефективність, проблеми причетних сторін та інші змінні, використовувані при оцінці ризику. Задана ризику є комбінацією значень ймовірності сценарію інциденту і його наслідків.

## 2.10 Результатом ідентифікації ризиків

Результатом етапу ідентифікації ризиків повинен бути перелік можливих ризиків, який прийнято називати «реєстр ризиків».

Приклад наведено у таблиці 2.1.

Таблиця 2.1

Реєстр ідентифікації ризиків

| № | Дата виникнення ризику | Дата реєстрації ризику | Найменування і опис ризику | Ініціатор | Причини | Наслідки | Власник ризику | Дата закінчення дії ризику |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |

Задокументовані ризики і їх характеристики, відображені в реєстрі ризиків, дозволяють досліджувати причини і можливі суміжні ризики, які можуть взаємно впливати і взаємо заміняти один одного, в залежності від параметрів оточення діяльності.

Розмір реєстру ризиків, буде залежати від масштабу діяльності, але, якщо організація має на меті підвищення якості своєї діяльності та створення якомога більш якісного продукту або послуги, то реєстр ризиків повинен бути максимально повним, незалежно від ймовірності і значення подій ризику.

Управляти всіма можливими ризиками представляється малоймовірним, так як це вимагає великих фінансових і кадрових витрат. Тому обов'язковою умовою для реєстру ризиків є наявність в ньому пріоритетів.

Пріоритет ризику - це параметр, якими ідентифікується найбільш важливі і значущі з них, в даний момент часу.

Саме важливість, коректного визначення пріоритетів ризиків, серед їх загального числа, може забезпечити надійні «тили» значущих процесів і проектів, що проводяться в організації.

**Висновки до розділу 2**

В ході даного розділу було проаналізовано результати досліджень компонентів КЗЗ КСЗІ.

# РОЗДІЛ 3
# ПЕРЕВІРКА АДЕКВАТНОСТІ ВИКОРИСТАННЯ МОДЕЛІ ІДЕНТИФІКАЦІЇ РИЗИКІВ

## 3.1 Характеристика об'єкта інформаційної діяльності ТОВ «ССК „Укрконсалтинг“»

Для та перевірки адекватності моделі було товариство з обмеженою відповідальністю «ССК «Укрконсалтинг»», Будівельно-транспортне підприємство ТОВ «ССК „Укрконсалтинг“» має в наявності більше 25 видів будівельної техніки та механізмів. Надає послуги оренди будівельної техніки та виконує такі роботи :

- технічне обслуговування та ремонт автотранспортних засобів;
- діяльність у сфері бухгалтерського обліку й аудиту; консультування з питань оподаткування;
- діяльність у сфері інжинірингу, геології та геодезії, надання послуг технічного консультування в цих сферах;
- будівництво житлових і нежитлових будівель;
- будівництво доріг і автострад;
- будівництво трубопроводів.

### 3.1.1 Загальна характеристика та призначення підприємства

Інформаційно система підприємства призначена для інформаційного забезпечення працівників цього підприємства в ході виконання ними своїх посадових обов'язків та автоматизації виробничих завдань, які стоять перед ним. ІС забезпечує доступ до баз персональних даних авторизованим користувачам, доступ до користування сервісами і ресурсами інформаційної системи підприємства та користування глобальною системою Інтернет (доступ до довідково-інформаційних

даних). ІС підприємства являє собою сукупність окремих інформаційно-телекомунікаційних систем бухгалтерського обліку, об'єднаних в єдину інформаційно систему рисунок 3.1.

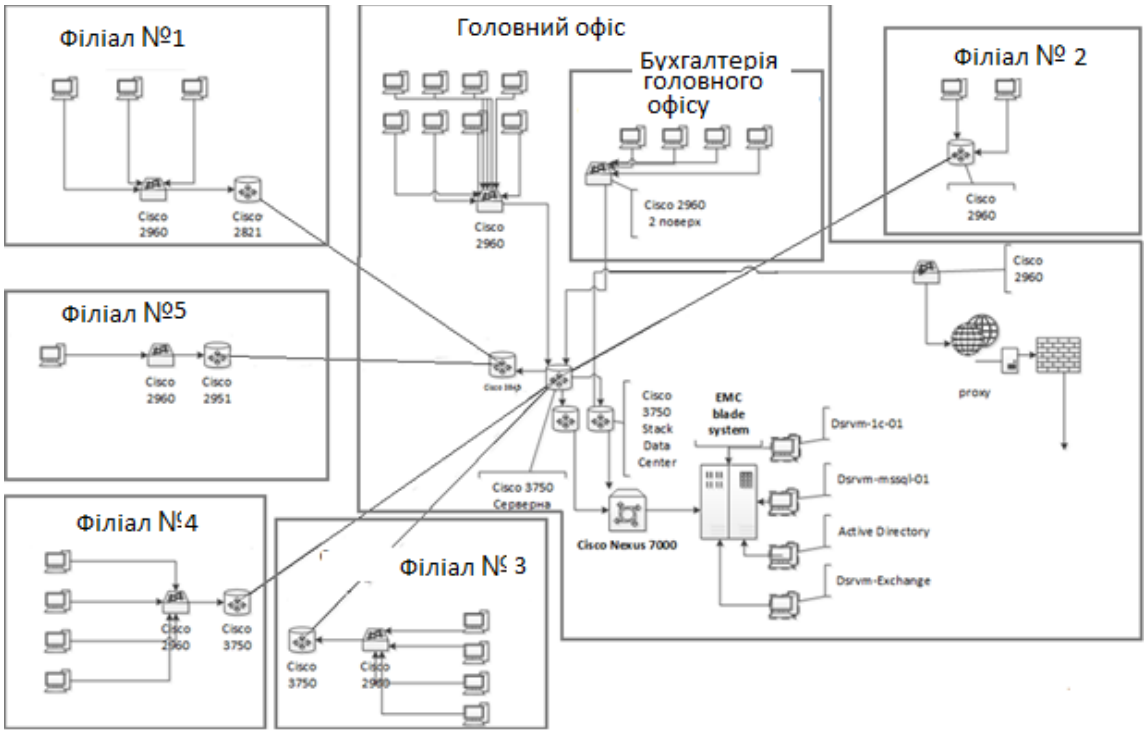


Рисунок 3.1 Узагальнена структурна схема ІС підприємства ТОВ «ССК „Укрконсалтинг“»

### 3.1.2 Характеристика фізичного середовища ІТС

Для здійснення інформаційного обміну між складовими інформаційно-телекомунікаційної системи побудовано структуровану кабельну систему (далі – СКС) з елементною базою категорії 5е. Архітектура СКС приміщень підприємства – «розподілена зірка» з мінімальною кількістю проміжних сполучень між робочими станціями та активними мережевими пристроями. Елементна база системи (кросове обладнання, інсталяційний (магістральний) кабель, інформаційні розетки, кросувальні шнури) розраховані на передачу інформаційного сигналу зі смугою частот до 125МГц і придатні для побудови локальної мережі за технологією Fast

Ethernet IEEE 802.3u (з пропускною здатністю каналів 100 Мбіт/с). Елементи СКС розташовані в межах контрольованої зони.

Для здійснення інформаційного обміну між головним офісом та розподіленими філіалами здійснюється за технологією Gigabit Ethernet IEEE 802.3ah (з пропускною здатністю каналів 1024 Мбіт/с)

Обмін конфіденційної інформації між філіями та головним офісом через незахищене середовище відкритими каналами зв'язку здійснюється у зашифрованому вигляді згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

У кожній віддаленій філії існує виділений сегмент ІС підприємства в межах якого ведеться обробка персональних даних користувачами (бухгалтерами) віддаленої філії. Користувачі цих сегментів ІС зареєстровані в домені головного офісу.

### 3.1.3 Інформація що обробляється в ІС

Відповідно до функціонального призначення в ІТС підприємства здійснюється передача, обробка та зберігання:

- конфіденційної інформації, до якої відносяться інформаційні об'єкти, що містять персональні дані працівників підприємства;
- відкритої інформації, до якої відносяться інформаційні об'єкти службової діяльності підприємства;
- технологічної інформації.

Технологія обробки інформації в ІТС побудована на технології «клієнт – сервер застосувань – сервер баз даних». Користувачі (за виключенням адміністратора БД) не мають безпосереднього доступу до бази даних. Всі запити користувачів обробляються сервером застосувань, який, в свою чергу, звертається до серверу баз даних.

Інформацію, що становить цінність для підприємства, вказано в таблиці

нижче у таблиці 3.1.

Таблиця 3.1

Інформаційні активи підприємства

| | **Інформація** | **В якій формі** | **Де зберігається** | **Умовні** |
|---|---|---|---|---|
| Відкрита інформація | Інформація про підприємство, | Електроний та паперовий носії | На сервері, у кабінеті секретаря | 1.1 |
| | Організаційно -статутна документація | Електроний та паперовий носії | На сервері, у кабінеті секретаря та | 1.2 |
| | Ліцензії | Електроний та паперовий носії | На сервері, у кабінеті | 1.3 |
| | Рекламні проспекти, інформація | Електроний та паперовий носії | На сервері | 1.4 |
| Інформація з обмеженим доступом | Договори з партнерами | Електроний та паперовий носії | На сервері, у кабінеті директора | 1.5 |
| | Персональні дані працівників | Електроний та паперовий носії | На сервері, на ПК бухгалтерів, у | 1.6 |
| | База даних клієнтів | Електроний носій | На сервері | 1.7 |
| | Організаційно -розпорядна документація | Електроний та паперовий носії | На сервері, у сейфах директора та | 1.8 |

| | | | | |
|---|---|---|---|---|
| | Бухгалтерська звітність | Електроний та паперовий носії | На сервері, на ПК бухгалтерів, у | 1.9 |
| | Технічні завдання | Електроний та паперовий носії | На сервері, у сейфі керівників | 1.10 |
| | Розроблені проекти, їх документація | Електроний носій | На ПК програмістів, курівників відділів, на сервері | 1.11 |

## 3.2 Виконання перевірки адекватності моделі ідентифікації ризиків на прикладі ТОВ «ССК „Укрконсалтинг“»

### 3.2.1 Опис бізнес-цілей і бізнес-функцій, основних бізнес-процесів ТОВ «ССК" Укрконсалтинг "»

Як організації розглядається поліклініка, основною метою (цільовою функцією) поліклініки є надання медичних послуг населенню.

Декомпозиція цільової функції дозволяє визначити основні інформаційні процеси, що реалізуються інформаційною системою організації, необхідні для цього ресурси, а також способи управління і перетворення інформації.

Для реалізації цільової функції в організації повинні бути реалізовані три процесу основної діяльності:

- реєстрація клієнтів;
- обстеження клієнтів;
- управління.

Зазначені процеси реалізуються основною функцією

«Взаємодія співробітників знаходяться на різних робочих місцях», при цьому в складі цієї основної функції можна виділити наступні функції:

- збереження всіх персональних і реєстраційних даних, діагнозів, аналізів на сервері організації;
- прийом персональних даних від громадян, що надійшли в поліклініку;
- друк оформлених звітів і діагнозів.

Блок А0, відповідний основної функції, показаний на малюнку 3.2.

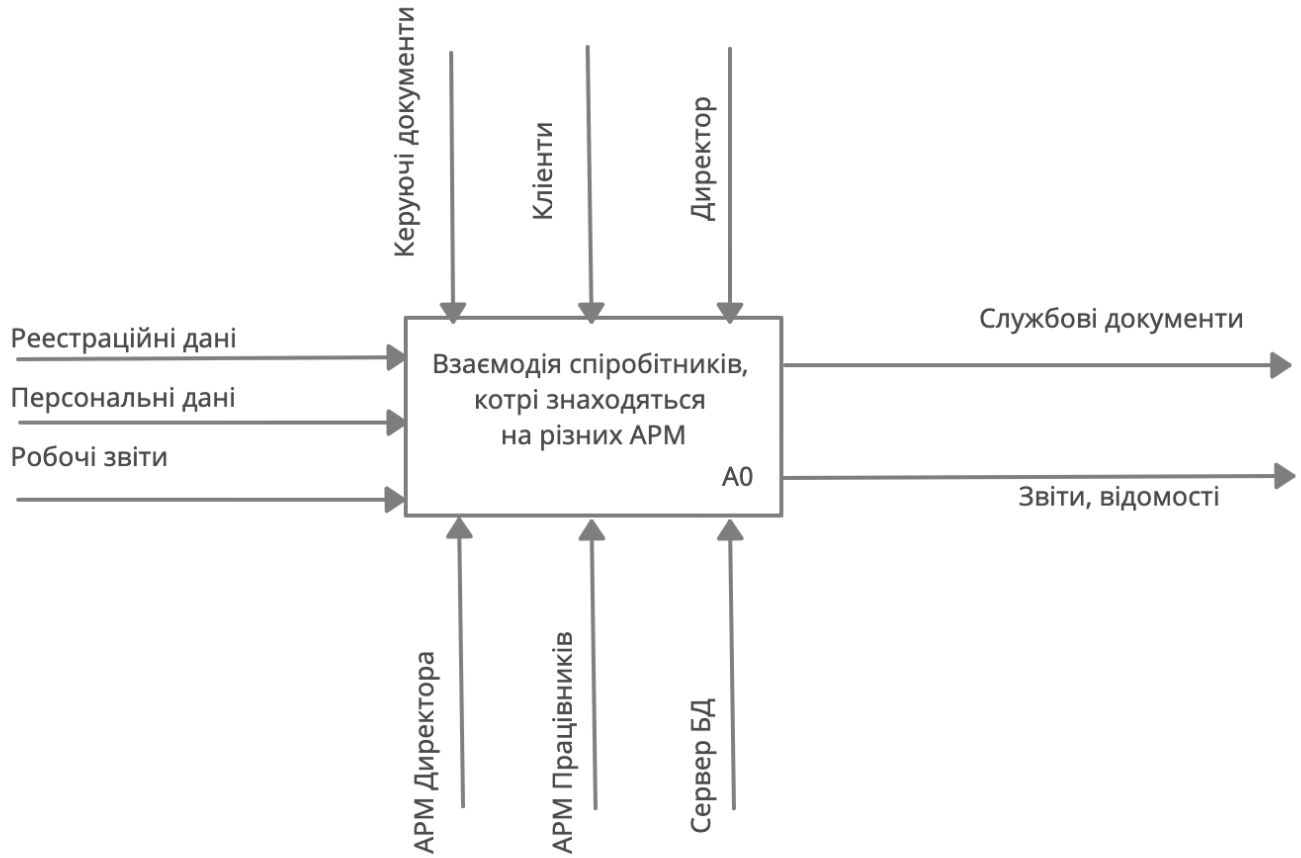


Рисунок 3.2- Диаграмма основной функции

Декомпозиція блоку А0 на складові функції представлена на малюнку 3.3.

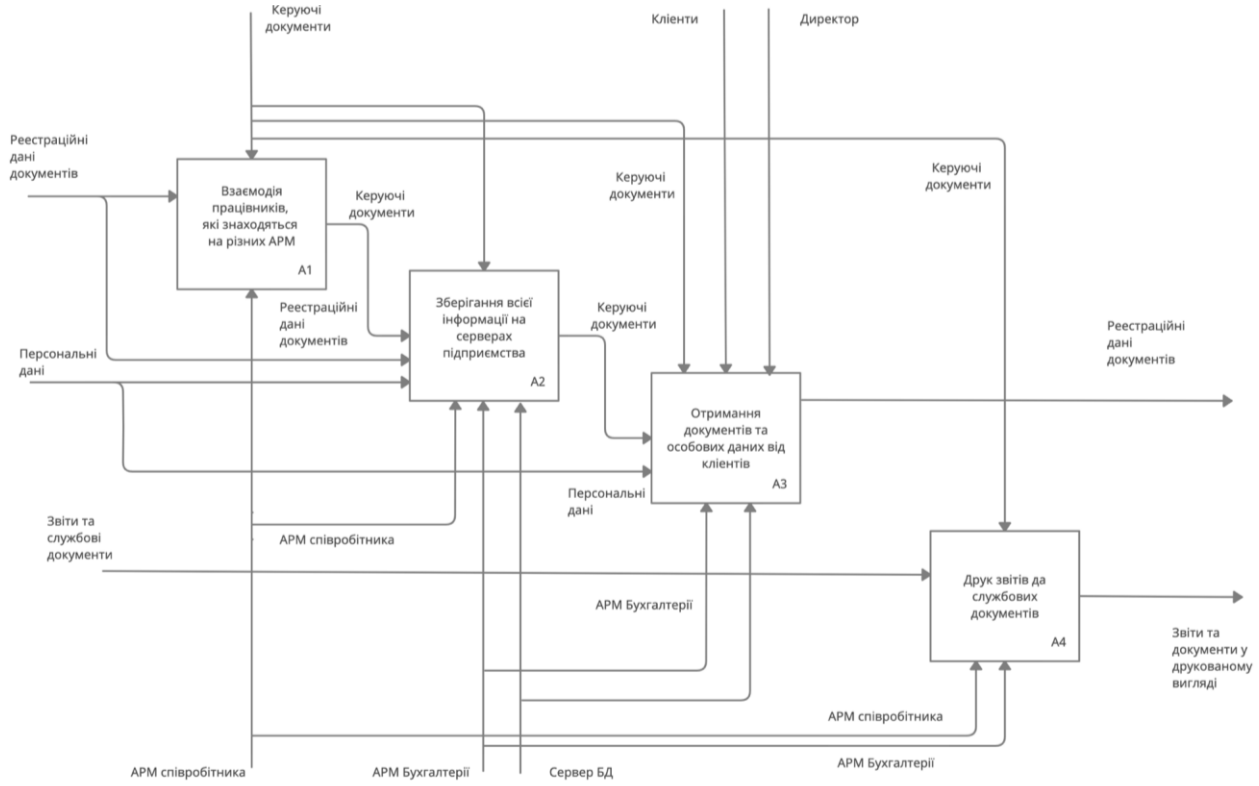


Рисунок 3.3 – Диаграмма составляющих функций

Після визначення основних інформаційних процесів в інформаційній системі організації була побудована загальна інфологіческая модель, що представляє собою спрямований граф.

Вершинами графа є інформаційні компоненти, зазначені в якості ресурсів кожного процесу. Ребрами графа є інформаційні потоки, що зв'язують інформаційні компоненти. Напрямок ребер визначає напрямок інформаційного потоку. Для кожного ребра вказуються:

- назва інформаційного потоку;
- критичність інформаційного потоку;
- передбачуваний обсяг даних.

Критичність потоку може бути позначена як:

- В - висока;
- С - середня;
- Н - низька.

Обсяг потоку може бути позначений як:

- 1 - малий;

- 2 - середній;

- 3 - великий.

Загальна інфологічна модель інформаційної системи наведена на малюнку 3.4.

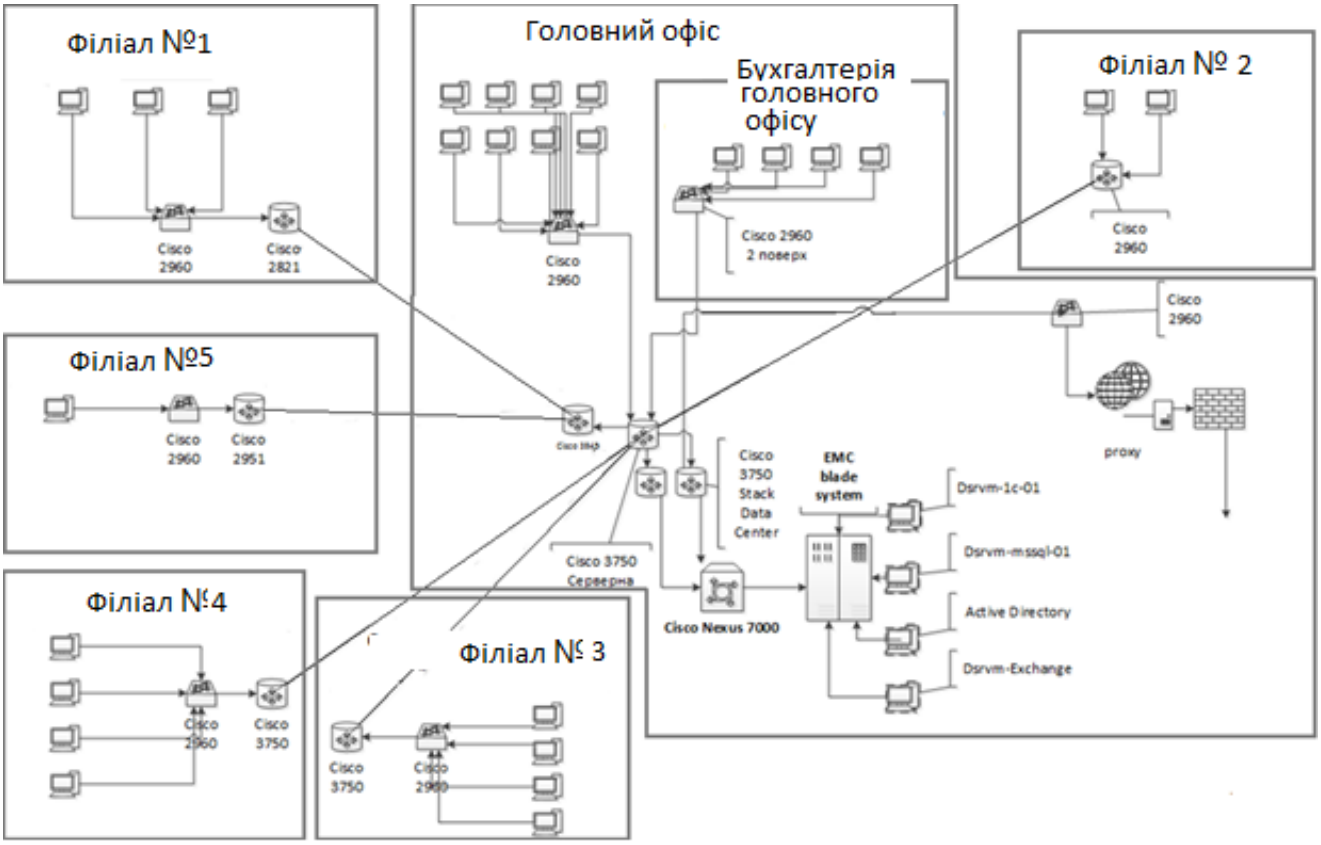


Рисунок 3.4 – Загальна інфологічна модель інформаційної системи

### 3.2.2 Ідентифікація активів

Інформаційні активи організації включають необхідну для здійснення основної діяльності інформацію, організації, інформацію з високою собівартістю, збір, зберігання, обробка і передача якої вимагає багато часу і пов'язана зі значними витратами на придбання.

Перелік інформаційних активів:

- інформація по керівних документах;

- інформація про клієнтів;

- інформація по реєстраційних даних;

- Інформація про директора.

Далі ідентифіковані допоміжні активи і залежності між ними та основними активами організації. Результат представлений у вигляді матриці залежностей в таблиці 3.2.

Таблиця 3.2

Матриця залежностей між активами організації

| Залежний актив | Актив | | | | |
|---|---|---|---|---|---|
| | АРМ співробітни | АРМ співробітник | АРМ співробітни | АРМ співробітник | АРМ співробітника |
| Інформація про керівні документах | + | + | + | - | - |
| Інформація про клієнтів (ІА2) | + | + | + | + | - |
| Інформація про реєстраційні дані (ІА3) | + | + | - | - | + |
| Інформація про директора(ІА4) | + | + | + | + | - |

### 3.2.3 Оцінка важливості інформаційних активів

Потім для кожного з інформаційних активів визначені значимі властивості ІБ.

Документований перелік інформаційних активів представлений в таблиці 3.3.

Таблиця 3.3

Перелік інформаційних активів і їх значущих властивостей

| Інформаційний актив | Значимі властивості інформаційної безпеки | | |
|---|---|---|---|
| | Конфіденційність | Цілісність | Доступність |
| Інформація про керівних документах (ІА1) | - | + | + |
| Інформація про клієнтів (ІА2) | + | + | + |
| Інформація про реєстраційних даних (ІА3) | - | + | + |
| Інформація про директора(ІА4) | + | + | + |

Далі проведено оцінювання величин збитку від порушення властивостей ІБ активів за наступними напрямками:

- ступінь впливу на безперервність діяльності організації;

- обсяг фінансових і матеріальних витрат, необхідних для відновлення властивостей ІБ для інформаційного активу і ліквідації наслідків порушення ІБ;

- обсяг додаткових людських ресурсів, необхідних для відновлення властивостей ІБ для інформаційного активу і ліквідації наслідків порушення ІБ;

- обсяг додаткових тимчасових витрат, необхідних для відновлення властивостей ІБ для інформаційного активу і ліквідації наслідків порушення ІБ;

- ступінь порушення законодавчих вимог і (або) договірних зобов'язань організації.

На підставі результатів оцінювання величини порушень ІБ для кожного інформаційного активу визначена узагальнена якісна оцінка величини порушення ІБ. Результати оцінювання представлені в таблиці 5.3.

Таблиця 3.4

Результати оцінювання велич порушення ІБ

| Інформаційний актив | Властивості безпеки | Величини порушення ІБ за напрямками оцінювання оценивания | | | | | Узагальнена величина порушення ІБ | Цінності активу |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| Інформація про керівних документах (ІА1) | Конфіденційність | М | М | М | М | М | М | С |
| | Цілісність | С | С | М | М | М | С | |
| | Доступність | С | С | М | М | М | С | |
| Інформація про клієнтів (ІА2) | Конфіденційність | В | В | С | В | В | В | В |
| | Цілісність | В | С | М | В | С | В | |
| | Доступність | В | С | М | В | С | В | |
| Інформація про реєстраційних даних (ІА3) | Конфіденційність | М | М | М | М | М | М | С |
| | Цілісність | С | С | М | М | М | С | |
| | Доступність | С | С | М | М | М | С | |
| Інформація про директора(ІА4) | Конфіденційність | В | В | С | В | В | В | В |
| | Цілісність | В | С | М | С | С | В | |
| | Доступність | В | С | М | С | С | В | |

Цінність допоміжних активів була визначена щодо їх вартості, а також цінності залежних від них інформаційних активів. Результат оцінювання представлений в таблиці 3.5.

Таблиця 3.5

Визначення цінності допоміжних активів

| Актив | Цінність активу без урахування | Залежні активи | | Цінність активу |
|---|---|---|---|---|
| | | Актив | Цінність | |
| АРМ керівника | С | Інформація про керівних документах | С | В |
| | | Інформація про клієнтів | В | |
| | | Інформація про реєстраційних даних | С | |
| | | Інформація про директора | В | |
| АРМ працівників | С | Інформація про керівних документах | С | В |
| | | Інформація про клієнтів | В | |
| | | Інформація про реєстраційних даних | С | |
| | | Інформація про директора | В | |
| Сервер БД | С | Інформація про керівних документах | С | В |
| | | Інформація про клієнтів | В | |
| | | Інформація про реєстраційних даних | В | |
| Персонал | С | Інформація про керівних документах | В | В |
| | | Інформація про клієнтів | В | |
| Термінали | С | Інформація про реєстраційних даних | С | С |

Далі розраховується важливість активів за методикою, розробленою в даній роботі. Спочатку потрібно оцінити важливість активів за таким видом впливу на актив, як «спотворення активу» або А1 з коефіцієнтом

12 у напрямку - «вплив активу на діяльність організації». Вплив активу на діяльність організації для А1 представлено в таблиці 3.6.

Таблиця 3.6

Вплив активу на діяльність організації для А1

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації В1 | Вплив на репутацію організації В2 | Порушення законодавчих вимог або договорів В3 | Порушення вимог регулюючих або наглядових органів В4 | підсумок | важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 3 | 3 | 3 | 3 | 144 | 576 |
| | Інформація про клієнтів | 3 | 3 | 3 | 3 | 144 | |
| АРМ директора | Інформація про реєстраційних даних | 3 | 3 | 3 | 3 | 144 | 576 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 144 | |
| АРМ бухгалтерії | Інформація про керівних документах | 6 | 3 | 3 | 6 | 216 | 720 |
| | Інформація про клієнтів | 3 | 3 | 6 | 6 | 216 | |
| | Інформація про реєстраційн | 3 | 3 | 3 | 3 | 144 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | их даних | | | | | | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 144 | |
| Сервер БД | Інформація про керівних документах | 3 | 3 | 3 | 6 | 180 | 612 |
| | Інформація про клієнтів | 3 | 6 | 6 | 6 | 252 | |
| | Інформація про реєстраційних даних | 3 | 3 | 6 | 3 | 180 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 6 | 3 | 180 | 324 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 144 | |
| Термінали | Інформація про керівних документах | 3 | 6 | 3 | 3 | 180 | 180 |

Таким чином, найвищу оцінку серед активів за таким видом впливу, як «спотворення активу» найбільшу важливість представляє АРМ реєстратури, що пов'язано з спотворенням даних для великого обсягу документів, які друкує реєстратура.

Далі необхідно оцінити важливість активів за таким видом впливу на актив, як «підміна активу» або А2 з коефіцієнтом 14 по напрямку - «вплив активу на діяльність організації». Вплив активу на діяльність організації для А2 представлено в таблиці 3.7.

Таблиця 3.7

Вплив активу на діяльність організації для А2

| Найменування активу | допоміжний актив | Вплив на безперервність діяльності організації В1 | Вплив на репутацію організації В2 | Порушення законодавчих вимог або договорів В3 | Порушення вимог регулюючих або наглядових органів В4 | підсумок | важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 3 | 3 | 6 | 3 | 210 | 714 |
| | Інформація про клієнтів | 3 | 3 | 3 | 3 | 168 | |
| | Інформація про реєстраційних даних Інформація про директора | 3 | 3 | 3 | 3 | 168 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 168 | |
| АРМ бухгалтерії | Інформація про керівних документах | 3 | 3 | 3 | 3 | 168 | 714 |
| | Інформація про клієнтів | 3 | 3 | 6 | 3 | 210 | |
| | Інформація про реєстраційних даних | 3 | 3 | 3 | 3 | 168 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 168 | |
| Сервер БД | Інформація про | 6 | 9 | 6 | 6 | 378 | 1050 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | керівних документах | | | | | | |
| | Інформація про клієнтів | 3 | 9 | 9 | 6 | 378 | |
| | Інформація про реєстраційних даних | 3 | 6 | 6 | 6 | 294 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 3 | 3 | 168 | 336 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 168 | |
| Термінали | Інформація про керівних документах | 3 | 6 | 6 | 3 | 252 | 252 |

Для даного виду впливу на актив найбільшу оцінку важливості активу отримує Сервер БД, так як підміна даних на сервері надає найбільший вплив.

На наступному етапі необхідно оцінити важливість активів за таким видом впливу на актив, як «розкриття активу» або А3 з коефіцієнтом 16 по напрямку - «вплив активу на діяльність організації».

Вплив активу на діяльність організації для А3 представлено в таблиці 3.8. Для даного виду впливу на активи найбільшу важливість має Сервер БД, так як розкриття інформації з бази даних про клієнтів може викликати найбільші коливання громадськість, може привести до великих судових розглядів та інше.

Таблиця 3.8

Вплив активу на діяльність організації для А3

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 3 | 3 | 6 | 6 | 288 | 1008 |
| | Інформація про клієнтів | 3 | 3 | 6 | 6 | 288 | |
| | Інформація про реєстраційних даних Інформація про директора | 3 | 3 | 6 | 3 | 240 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 192 | |
| АРМ бухгалтерії | Інформація про керівних документах | 3 | 6 | 6 | 6 | 336 | 1008 |
| | Інформація про клієнтів | 3 | 6 | 6 | 3 | 288 | |
| | Інформація про реєстраційних даних | 3 | 3 | 3 | 3 | 192 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 192 | |
| Сервер БД | Інформація про керівних документах | 3 | 9 | 9 | 9 | 480 | 1440 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про клієнтів | 6 | 9 | 9 | 9 | 528 | |
| | Інформація про реєстраційних даних | 6 | 6 | 9 | 6 | 432 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 6 | 3 | 240 | 432 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 192 | |
| Термінали | Інформація про керівних документах | 3 | 3 | 6 | 3 | 240 | 240 |

Далі необхідно оцінити важливість активів за таким видом впливу на актив, як Блокування активу або А4 з коефіцієнтом 18 по напрямку - «вплив активу на діяльність організації». Вплив активу на діяльність організації для А4 представлено в таблиці 3.9.

На даному етапі найбільшу оцінку важливості отримали АРМ Реєстратури і Сервер БД, що пов'язано з найбільшим впливом на діяльність і працездатність поліклініки при блокуванні даних.

Таблиця 3.9

Вплив активу на діяльність організації для А4

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| АРМ директора | Інформація про керівних документах | 3 | 3 | 3 | 3 | 216 | 8864 |
| | Інформація про клієнтів | 3 | 3 | 3 | 3 | 216 | |
| | Інформація про реєстраційних | 3 | 3 | 3 | 3 | 216 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 216 | |
| АРМ бухгалтерії | Інформація про керівних документах | 3 | 6 | 3 | 3 | 270 | 1134 |
| | Інформація про клієнтів | 3 | 6 | 3 | 3 | 270 | |
| | Інформація про реєстраційних | 3 | 6 | 6 | 3 | 324 | |
| | Інформація про директора | 3 | 6 | 3 | 3 | 270 | |
| Сервер БД | Інформація про керівних документах | 3 | 6 | 6 | 6 | 378 | 1242 |
| | Інформація про клієнтів | 6 | 6 | 6 | 6 | 432 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про реєстраційних | 6 | 6 | 6 | 6 | 432 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 3 | 3 | 216 | 432 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 216 | |
| Термінали | Інформація про керівних документа | 3 | 3 | 3 | 3 | 216 | 216 |

На останньому етапі необхідно оцінити важливість активів за таким видом впливу на актив, як Знищення активу або А5 з коефіцієнтом 20 по напрямку - «вплив активу на діяльність організації».

Вплив активу на діяльність організації для А5 представлено в таблиці 3.10.

Таблиця 3.10

Вплив активу на діяльність організації для А5

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документа | 6 | 3 | 3 | 3 | 300 | 81140 |
| | Інформація про клієнтів | 6 | 3 | 3 | 3 | 300 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про реєстраційних даних | 6 | 3 | 3 | 3 | 300 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |
| АРМ бухгалтерії | Інформація про керівних документах | 6 | 3 | 3 | 3 | 300 | 1440 |
| | Інформація про клієнтів | 6 | 6 | 6 | 6 | 480 | |
| | Інформація про реєстраційних даних | 6 | 3 | 6 | 6 | 420 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |
| Сервер БД | Інформація про керівних документах | 6 | 6 | 9 | 9 | 600 | 1920 |
| | Інформація про клієнтів | 6 | 9 | 9 | 9 | 660 | |
| | Інформація про реєстраційних даних | 6 | 9 | 9 | 9 | 660 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 6 | 6 | 360 | 600 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Термінали | Інформація про керівних документах | 3 | 3 | 6 | 6 | 360 | 360 |

Таким чином, найбільшу оцінку важливості має сервер даних, так як видалення даних на ньому надасть найбільший вплив на діяльність поліклініки через потребу у відновленні великого обсягу даних, що обов'язково буде освітлено на федеральному рівні.

Після того, як висновок за всіма трьома показниками для кожного з п'яти різних можливих впливів даного напрямку оцінки інформаційного активу були зібрані, розраховується важливість активу для організації за напрямом «вплив активу на діяльність організації». Підсумкове значення важливості і проміжні розрахунки зведені в таблицю 3.11.

Таблиця 3.11

Підсумкове значення важливості

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 144 | 210 | 288 | 216 | 300 | 4302 (Н) |
| | Інформація про клієнтів | 144 | 168 | 288 | 216 | 300 | |
| | Інформація про реєстраційних даних Інформація про директора | 144 | 168 | 240 | 216 | 300 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про директора | 144 | 168 | 192 | 216 | 240 | |
| АРМ бухгалтерії | Інформація про керівних документах | 216 | 168 | 336 | 270 | 300 | 5016 (С) |
| | Інформація про клієнтів | 216 | 210 | 288 | 270 | 480 | |
| | Інформація про реєстрацій них даних | 144 | 168 | 192 | 324 | 420 | |
| | Інформація про директора | 144 | 168 | 192 | 270 | 240 | |
| Сервер БД | Інформація про керівних документах | 18 | 37 | 48 | 37 | 60 | 6264 (В) |
| | Інформація про клієнтів | 0 | 8 | 0 | 8 | 0 | |
| | Інформація про реєстрацій них даних | 6 | 9 | 9 | 9 | 660 | |
| Персонал | Інформація про клієнтів | 180 | 168 | 240 | 216 | 360 | 2124 (Н) |
| | Інформація про директора | 144 | 168 | 192 | 216 | 240 | |
| Термінали | Інформація про керівних документах | 180 | 252 | 240 | 216 | 360 | 1248 (Н) |

Далі необхідно провести оцінку важливості активів поліклініки за напрямом «витрати, необхідні для ліквідації наслідків». Оцінювання на даному етапі здійснюється на підставі висновків за наступними показниками:

- обсяг фінансових і матеріальних витрат, необхідних для ліквідації наслідків (С1);

- обсяг додаткових людських ресурсів, необхідних для ліквідації наслідків (С2);

- обсяг додаткових тимчасових витрат, необхідних для ліквідації наслідків (С3).

Далі необхідно оцінити важливість активів за таким видом впливу на актив, як «спотворення активу» або А1 з коефіцієнтом 12 по напрямку - «витрати для ліквідації наслідків». Вплив активу на діяльність організації представлено в таблиці 3.12.

Таблиця 3.12

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 4 | 4 | 4 | 144 | 4 | 576 |
| | Інформація про клієнтів | 4 | 4 | 4 | 144 | 4 | |
| | Інформація про реєстрацій них даних | 4 | 4 | 4 | 144 | 4 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про директора | | | | | | |
| | Інформація про директора | 4 | 4 | 4 | 144 | 4 | |
| АРМ бухгалтерії | Інформація про керівних документах | 8 | 4 | 4 | 192 | 8 | 672 |
| | Інформація про клієнтів | 4 | 4 | 8 | 192 | 4 | |
| | Інформація про реєстрацій них даних | 4 | 4 | 4 | 144 | 4 | |
| | Інформація про директора | 4 | 4 | 4 | 144 | 4 | |
| Сервер БД | Інформація про керівних документах | 4 | 8 | 8 | 240 | 4 | 1104 |
| | Інформація про клієнтів | 12 | 12 | 12 | 432 | 12 | |
| | Інформація про | 12 | 12 | 12 | 432 | 12 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | реєстрацій них даних | | | | | | |
| Персонал | Інформація про клієнтів | 4 | 4 | 8 | 192 | 4 | 384 |
| | Інформація про директора | 4 | 4 | 8 | 192 | 4 | |
| Термінали | Інформація про керівних документах | 4 | 8 | 8 | 240 | 4 | 240 |

За даними оцінки важливості в таблиці 3.12, можна сказати, що найбільшу оцінку отримав сервер БД, в зв'язку з найбільшими витратами за часом відновлення даних, оскільки буде потрібно пошук і аналіз виниклих помилок в зв'язку зі зміною даних.

Далі необхідно оцінити важливість активів за таким видом впливу на актив, як «підміна активу» або А2 з коефіцієнтом 14 по напрямку - «витрати для ліквідації наслідків» (див. Таблицю 3.13).

Таблиця 3.13

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації С1 | Вплив на репутацію організації С2 | Порушення законодавчих вимог або договорів С3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| АРМ директора | Інформація про керівних документах | 6 | 3 | 3 | 3 | 300 | 81140 |
| | Інформація про клієнтів | 6 | 3 | 3 | 3 | 300 | |
| | Інформація про реєстраційних даних Інформація про | 6 | 3 | 3 | 3 | 300 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |
| АРМ бухгалтерії | Інформація про керівних документах | 6 | 3 | 3 | 3 | 300 | 1440 |
| | Інформація про клієнтів | 6 | 6 | 6 | 6 | 480 | |
| | Інформація про реєстраційних даних | 6 | 3 | 6 | 6 | 420 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |
| Сервер БД | Інформація про керівних документах | 6 | 6 | 9 | 9 | 600 | 1920 |
| | Інформація про клієнтів | 6 | 9 | 9 | 9 | 660 | |
| | Інформація про реєстраційних даних | 6 | 9 | 9 | 9 | 660 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 6 | 6 | 360 | 600 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 240 | |
| Термінали | Інформація про керівних документах | 3 | 3 | 6 | 6 | 360 | 360 |

Наступний етап - оцінка важливості активів за таким видом впливу на актив, як «розкриття активу» або А3 з коефіцієнтом 16 по напрямку - «витрати для ліквідації наслідків» (див. Таблицю 3.14).

Таблиця 3.14

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації С1 | Вплив на репутацію організації С2 | Порушення законодавчих вимог або договорів С3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| АРМ директора | Інформація по керівних документах | 4 | 4 | 4 | 192 | 768 |
| | Інформація про клієнтів | 4 | 4 | 4 | 192 | |
| | Інформація по реєстраційних даних | 4 | 4 | 4 | 192 | |
| | Інформація про головного лікаря | 4 | 4 | 4 | 192 | |
| АРМ бухгалтерії | Інформація по керівних документах | 4 | 4 | 4 | 192 | 832 |
| | Інформація про клієнтів | 4 | 4 | 8 | 256 | |
| | Інформація по реєстраційних даних | 4 | 4 | 4 | 192 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Інформація про головного лікаря | 4 | 4 | 4 | 192 | |
| Сервер БД | Інформація по керівних документах | 4 | 8 | 8 | 320 | 960 |
| | Інформація про клієнтів | 4 | 8 | 8 | 320 | |
| | Інформація по реєстраційних даних | 4 | 8 | 8 | 320 | |
| Персонал | Інформація про клієнтів | 4 | 4 | 8 | 256 | 448 |
| | Інформація про головного лікаря | 4 | 4 | 4 | 192 | |
| Термінали | Інформація по реєстраційних даних | 4 | 4 | 4 | 192 | 192 |

При розкритті даних найбільшу важливість має сервер БД, так як найбільша частина даних є конфіденційною інформацією, розкриття якої приведе до судових розглядів у великому обсязі.

Наступний етап - оцінка важливості активів за таким видом впливу на актив, як «блокування активу» або А4 з коефіцієнтом 18 по напрямку - «витрати для ліквідації наслідків» (див. Таблицю 3.15).

Таблиця 3.15

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації С1 | Вплив на репутацію організації С2 | Порушення законодавчих вимог або договорів С3 | Порушення вимог регулюючих або наглядових орган | Підсумок |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |

| | | | | | | |
|---|---|---|---|---|---|---|
| АРМ бухгалтерії | Інформація по керівних документах | 8 | 4 | 4 | 288 | 1152 |
| | Інформація про клієнтів | 8 | 4 | 8 | 360 | |
| | Інформація по реєстраційних даних | 8 | 4 | 4 | 288 | |
| | Інформація про директора | 4 | 4 | 4 | 216 | |
| Сервер БД | Інформація по керівних документах | 8 | 12 | 12 | 576 | 1800 |
| | Інформація про клієнтів | 12 | 12 | 12 | 648 | |
| | Інформація по реєстраційних даних | 8 | 12 | 12 | 576 | |
| Персонал | Інформація про клієнтів | 4 | 4 | 8 | 288 | 576 |
| | Інформація про головного лікаря | 4 | 4 | 8 | 288 | |
| Терминалы | Інформація про керівних | 4 | 4 | 4 | 216 | 216 |

При блокуванні даних найбільші витрати понесе Сервер БД, так як персонал має можливість працювати і на паперових носіях, в той час як відновлення доступу необхідно для поліклініки у зв'язку з великим обсягом інформації, яка необхідна поліклініці в стислі терміни.

Наступний етап - оцінка важливості активів за таким видом впливу на актив, як Знищення активу або А5 з коефіцієнтом 20 по напрямку - «витрати для ліквідації наслідків» (див. Таблицю 3.16).

Таблиця 3.16

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації С1 | Вплив на репутацію організації С2 | Порушення законодавчих вимог або договорів С3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документа | 3 | 3 | 3 | 3 | 216 | 8864 |
| | Інформація про клієнтів | 3 | 3 | 3 | 3 | 216 | |
| | Інформація про реєстраційних даних | 3 | 3 | 3 | 3 | 216 | |
| | Інформація про директора | 3 | 3 | 3 | 3 | 216 | |
| АРМ бухгалтерії | Інформація про керівних документах | 3 | 6 | 3 | 3 | 270 | 1134 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про клієнтів | 3 | 6 | 3 | 3 | 270 | |
| | Інформація про реєстраційних даних | 3 | 6 | 6 | 3 | 324 | |
| | Інформація про директора | 3 | 6 | 3 | 3 | 270 | |
| Сервер БД | Інформація про керівних документах | 3 | 6 | 6 | 6 | 378 | 1242 |
| | Інформація про клієнтів | 6 | 6 | 6 | 6 | 432 | |
| | Інформація про реєстраційних даних | 6 | 6 | 6 | 6 | 432 | |
| Персонал | Інформація про клієнтів | 3 | 3 | 3 | 3 | 216 | 432 |
| | Інформація про директора | 3 | 3 | 3 | 3 | 216 | |
| Термінали | Інформація про керівних документах | 3 | 3 | 3 | 3 | 216 | 216 |

При знищенні даних найбільші витрати понесе Сервер БД, в зв'язку з тим, що втрата інформації призведе до додаткових тимчасовим, людських і матеріальних витрат по відновленню даних. Якщо врахувати, що дані були втрачені безповоротно і буде потрібно відновлення всього обсягу даних з паперових носіїв, то один

перенесення даних в електронний вигляд даних клієнтів обійдеться у величезні часові витрати.

Після того, як висновок за всіма трьома показниками для кожного з п'яти різних можливих впливів даного напрямку оцінки інформаційного активу були зібрані, розраховується важливість активу для організації за напрямом «витрати, необхідні для ліквідації наслідків». Підсумкове значення важливості і проміжні розрахунки зведемо в таблицю (див. Таблицю 3.17).

Таблиця 3.17

Вплив активу на діяльність організації

| Найменування активу | Допоміжний актив | Вплив на безперервність діяльності організації в1 | Вплив на репутацію організації в2 | Порушення законодавчих вимог або договорів в3 | Порушення вимог регулюючих або наглядових органів в4 | Підсумок | Важливість активу |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| АРМ директора | Інформація про керівних документах | 144 | 210 | 288 | 216 | 300 | 4302 (Н) |
| | Інформація про клієнтів | 144 | 168 | 288 | 216 | 300 | |
| | Інформація про реєстраційних даних Інформація | 144 | 168 | 240 | 216 | 300 | |
| | Інформація про директора | 144 | 168 | 192 | 216 | 240 | |
| АРМ бухгалтерії | Інформація про керівних документах | 216 | 168 | 336 | 270 | 300 | 5016 (С) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Інформація про клієнтів | 216 | 210 | 288 | 270 | 480 | |
| | Інформація про реєстрацій них даних | 144 | 168 | 192 | 324 | 420 | |
| | Інформація про директора | 144 | 168 | 192 | 270 | 240 | |
| Сервер БД | Інформація про керівних документах | 18 | 37 | 48 | 37 | 60 | 6264 (В) |
| | Інформація про клієнтів | 0 | 8 | 0 | 8 | 0 | |
| | Інформація про реєстрацій них даних | 6 | 9 | 9 | 9 | 660 | |
| Персонал | Інформаці я про клієнтів | 180 | 168 | 240 | 216 | 360 | 2124 (Н) |
| | Інформація про директора | 144 | 168 | 192 | 216 | 240 | |
| Термінали | Інформація про керівних документах | 180 | 252 | 240 | 216 | 360 | 1248 (Н) |

Таким чином, підрахуємо підсумкову оцінку важливості інформаційних активів поліклініки підсумовуючи дані по напрямку

«Витрати, необхідні для ліквідації наслідків» і по напрямку

«Вплив активу на діяльність організації» (див. Таблицю 3.18).

Таблиця 3.18

Важливість активів організації

| Найменування активу | Допоміжний актив | S1 | S2 | S | Підсумок |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| АРМ директора | Інформація по керівних документах | 1158 | 1032 | 2190 | Н |
| | Інформація про клієнтів | 1116 | 1032 | 2148 | Н |
| | Інформація по реєстраційних даних | 1068 | 1032 | 2100 | Н |
| | Інформація про головного лікаря | 960 | 960 | 1920 | Н |
| АРМ бухгалтерії | Інформація по керівних документах | 1290 | 1160 | 2450 | С |
| | Інформація про клієнтів | 1464 | 1432 | 2896 | С |
| | Інформація по реєстраційних даних | 1248 | 1112 | 2360 | Н |
| | Інформація про головного лікаря | 1014 | 960 | 1974 | Н |
| Сервер БД | Інформація по керівних документах | 2016 | 2136 | 4152 | С |
| | Інформація про клієнтів | 2250 | 2456 | 4706 | В |
| | Інформація по реєстраційних даних | 1998 | 2328 | 4326 | В |
| Персонал | Інформація про клієнтів | 1164 | 1280 | 2444 | С |
| | Інформація про головного лікаря | 960 | 1216 | 2176 | Н |

| | | | | | |
|---|---|---|---|---|---|
| Термінали | Інформація по реєстраційних даних | 1248 | 1192 | 2440 | С |

Таким чином, проведена оцінка важливості показала важливість таких інформаційних активів:

- сервер БД - висока;
- термінали - середня;
- персонал - низька;
- АРМ бухгалтерії - середня;
- АРМ керівника - низька.

**Висновки до розділу 3**

В розділі 3 був проведений аналіз міжнародних і вітчизняних стандартів і практик в області ідентифікації і оцінки кібербезпеки в роподілених ІС, а також були розглянуті підходи і способи ідентифікації та оцінки важливості інформаційних активів організації при оцінці ризиків кібербезпеки.

# ВИСНОВКИ

В ході виконання дипломної роботи був проведений аналіз міжнародних і вітчизняних стандартів і практик в області ідентифікації і оцінки кібербезпеки в роподілених ІС, а також були розглянуті підходи і способи ідентифікації та оцінки важливості інформаційних активів організації при оцінці ризиків кібербезпеки.

Відповідно до мети роботи, було вирішено наступні завдання:

- аналіз існуючих світових стандартів у сфері кібербезпеки щодо ідентифікації ризиків та оцінки загроз;
- приведення даних до узагальненого;
- розробка алгоритму ідентифікації ризиків у ІС;
- синтез моделі ідентифікації ризиків на основі проаналізованих стандартів.
- аналіз адекватності синтезованої моделі

При проведенні експериментальної перевірки було виявлено, що найбільш цінний актив - сервер БД, на якому зберігається інформація про персонал і клієнтів поліклініки.

Результати оцінки важливості можуть бути використані при оцінки та обробки ризиків для зазначеної організації.

Таким чином, мета дипломної роботи була досягнута, завдання на дипломну роботу виконано в повному обсязі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Oleksii Kuchmai 2. Tetiana Shelest, Using open-source intelligence (OSINT) as one of the effective and legitimate ways to avoid threats to the corporation. // Scientific and practical cyber security journal | ISSN 2587-4667 - Режим доступу до ресурсу: https://journal.scsa.ge/wp-content/uploads/2021/03/5using-open-source-intelligence-osint-as-one-of-the-effective-and-legitimate-ways-to-avoid-threats-to-the-corporation-1.pdf

2. ДСТУ 3008:2015. Національний стандарт України. Інформація та документація. Звіти у сфері науки і техніки. Структура і правила оформлення. – Чинний від 2015-06-22. – К.: Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості», 2016. – 31 с.

3. ДСТУ 1.5:2003 - Національна стандартизація. Правила побудови, викладення, оформлення та вимоги до змісту нормативних документів. - Впров. 2003.01.10. - К.: Держстандарт України, 2003. - 40 с.

4. ДСТУ 7.1:2006. Національний стандарт України. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання (ГОСТ 7.1-2003, IDT). – К.: Держспоживстандарт України, 2007. – 48 с.

5. Бучик С. С. Методика оцінювання інформа- ційних ризиків в автоматизованій системі // С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. Житомир: ЖВІ ДУТ, 2015. Вип. 11. С. 33–43.

6. Гао Кунлун, Ванг, Ксу Руши. Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях // МКА: ВКС. 2015. №1. С. 51–60.

7. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко // Системи

обробки інформації. Л.: Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2015. Вип. 3 (128). С. 75–79.

8. Ковальов І. Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх / І. Ковальов. Дніпро, 2018. 78 с.

9. Козак Н., Цимбал П., Варшавець Я. Деякі аспекти виявлення і попередження інцидентів кібербезпеки. URL: http: // ir. nusta. edu. ua / jspui / bitstream / 123456789 / 2339 / 1/2219_IR. pdf. Дата звернення: 03.05.2021.

10. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія / О. Корченко, С. Казмірчук, Б. Ахметов. Київ, 2017. 435 с.

11. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія / О. Корченко, С. Казмірчук. К., 2017. 435 с.

12. Макеев А. С. Менеджмент рисков информационной безопасности как непрерывный процесс // Молодой ученый. 2016. №10. С. 62–66.

13. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства / М. Мельник, Г. Нікітин, К. Мезенцева // Системи обробки інформації. 2017. Вип. 2. С. 126–128.

14. Микитенко Т. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах / Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2016. № 2. С. 24–31.

15. Миков Д. А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности / Д. А. Миков // Вопросы кибербезопасности. – 2014. – №4 (7). – С. 49–54.

16. Мохор В. В., Гончар С. Ф., Дибач О. М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. Ядерна та радіаційна безпека. 2019. № 2 (82). С. 57–61.

17. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційнотелекомунікаційних сис- тем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. Л.: Академія

сухопутних військ імені гетьмана Петра Сагайдачно го, 2014. Вип. 8 (124). С. 128–134.

18. Рудий Т. Засади захисту інформації в інформаційних системах підприємств / Т. Рудий, Л. Томаневич, О. Руда // Актуальні проблеми економіки. № 2 (152). 2014. С. 551–557.

19. Савельєва Т., Панаско О., Пригодюк О. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства / Т. Савельєва, О. Панаско, О. Пригодюк // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. 2018. Т. 1, № 4. С. 81–89.

20. Северина С. Інформаційна безпека та методи захисту інформації / С. Северина // Вісник Запорізького національного університету. Економічні науки. 2016. № 1. С. 155–161.

21. Твердохліб І. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Дипломна робота магістра / І. Твердохліб. Дніпро, 2018. 132 с.

22. Чунарьова А. В. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах / А. В. Чунарьова, І. І. Пархоменко, І. І. Сащук // Вісник Інже- нерної академії України. Х. 2014. Вип. 2. С. 138–142.

23. Выбор алгоритмов машинного обучения Microsoft Azure [[Электронный ресурс] – Режим доступа: https: // docs. microsoft. com / ruru / azure / machine-learning / studio / algorithm-choice. Дата звернення: 03.05.2021.

24. Azure Sentinel: офіційна сторінка сервісу [Електронний ресурс] // Сайт Microsoft. – Режим доступу: https: // azure. microsoft. com / en-us / services / azuresentinel. Дата звернення: 03.05.2021.

25. Вихідний код сервісу Azure Sentinel [Електронний ресурс] // Сайт GitHub. – Режим доступу: https: // github. com / Azure / Azure-Sentinel. Дата звернення: 03.05.2021.

26. Derek Young, Juan Lopez Jr., Mason Rice, Benjamin Ramsey, Robert McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection. Vol. 14. 2016. P. 43–57.

27. Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M. S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries. 2018. Vol. 53. P. 61–73.

28. Jinsoo Shin, Hanseong Son, Gyunyoung Heo. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. Nuclear Engineering and Technology. Vol. 49. Issue 3. 2017. P. 517–524.

29. Petar Radanlieva, David Charles De Rourea, Razvan Nicolescub, Michael Huthb, Rafael Mantilla Montalvoc, Stacy Cannadyc, Peter Burnap. Future developments in cyber risk assessment for the internet of things. Computers in Industry. Vol. 102. 2018. P. 14–22.

30. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. 2016. Vol. 253. Issue 1. P. 1–13.

31. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.

32. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology) [Текст]. – Gaithersburg: National Institute of Standards and Technology, 200.332. – 95 с.

33. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст] / R. A.Caralli, J. F. Stevens, L. R. Young, L. R. Wilson.– Бостон: Університет Карнегі-Меллон, 2007. – 0.3354 с.

34. Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust [Електронний ресурс] // Symantec White

Paper.200.335. Режим доступу до ресурсу: https://www.symantec.com/content/dam/symantec/docs/white- papers/cybersecurity-retail-en.pdf.

35. Cyber risk in retail: Protecting the retail business to secure tomorrow's growth [Електронний ресурс]. 200.337. Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/us-risk- 200.337-retail-cyber-risk-report-04070.335.pdf

36. Информационная безопасность и розничная торговля [Електронний ресурс].200.335Режим доступу до ресурса: https://www.cisco.com/c/ru_ru/about/press/press-releases/200.335/08- 20.33d.html

37. Security trends in the retail industry [Електронний ресурс]. – 200.336 – Режим доступу до ресурса: https://www.ibm.com/downloads/cas/DO8MZRV9

38. Cyber security concerns in the retail sector [Електронний ресурс]. – 200.337 – Режим доступу до ресурса: https://www.grantthornton.ie/globalassets/0.33.-member-firms/ireland/insights/factsheets/grant-thornton---cyber-security- concerns---retail.pdf.

39. Скачек Л. М. ЦІННІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Текст] / Л. М. Скачек. // Інформаційна безпека. – 200.333. – №0.33(9). – С. 0.3352–0.3354.

40. Кибербезопасность: больше чем защита? [Текст] // Международное исследование EY в области информационной безопасности. – 2018. – С. 32

41. Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – Режим доступу : //www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt- strtgy/cbr-scrt-strtgy-eng.pdf.

42. Gladysh S. Distribution of responsibility on telecommunication incidents in Ukraine // Матеріали III Міжнародної науково-практичної конференції «Інформаційні технології в наукових дослідженнях і навчальному процесі», Луганськ: ЛНПУ, 2012.

43. ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки» Полушкин А. В.

Информационное правонарушение: понятие и виды: дис. канд. юрид. наук: 12.00.14/ Александр Васильевич Полушкин. — Екатеринбург, 2009. — 223 с.

44. .Ліпкан В., Максименко Ю. Націобезпекознавство: проблеми формування категорійно-понятійного апарату / В. Ліпкан, Ю. Максименко // Підприємництво, господарство і право. — 2011. — № 8. — С. 7—11.

45. .Резолюции Генеральной Ассамблеи ООН от 30 января 2004 г. по докладу Второго комитета (A/58/481/Add.2)58/199. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур от 23 января 2002 по докладу Третьего комитета (A/56/574) 56/121. Борьба с преступным использованием информационных технологий. http://www:ifap.ru (дата обращения: 23.10.2010 г.).

46. .Овчинников С.А., Гришин С.Е. Формирование культуры кибербезопасности в обществе – актуальная задача современности //Вестник СГСЭУ. 2011. № 3 (37). 206.

47. .Максименко Ю.Є. Правове регулювання національної безпеки України: окремі аспекти // Імперативи розвитку юридичної та безпекової науки : матеріали міжнародної науково-практичної інтернет-конференції (Київ, 15 квітня 2010 р.). — К. : О.С. Ліпкан, 2010. — 102 с.

48. .Офіційний сайт Національного банка України [Електронний ресурс] – Режим доступу: http://www.bank.gov.ua/.

49. .Овчинников С.А., Семенов В.П. Проблемы стандартизации, совместимости и взаимодействия органов государственной власти, бизнес-процессов и граждан в условиях широкого внедрения информационных технологий // Информационно-коммуникационные технологии в сфере культуры: сб. мат. Международ. науч.-методич. конф. 19 – 24 сентября, 2011.

50. .Єрохін А.Л. Модель візуалізації нештатних подій у складних інформаційних системах // Зв'язок. — 2009. — № 6. — С. 52–56.

51. .Сакович Л.М., Політов В.І. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. — 2012. — № 5. — С. 37–39.

52. .Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв’язок. — 2011.— № 1. — С. 39–45.

53. .Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373. — 4 с.

# ДОДАТКИ

## ДОДАТОК А

1. Oleksii Kuchmai 2. Tetiana Shelest, Using open-source intelligence (OSINT) as one of the effective and legitimate ways to avoid threats to the corporation. // Scientific and practical cyber security journal | ISSN 2587-4667 - Режим доступу до ресурсу: https://journal.scsa.ge/wp-content/uploads/2021/03/5using-open-source-intelligence-osint-as-one-of-the-effective-and-legitimate-ways-to-avoid-threats-to-the-corporation-1.pdf