**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
Кафедра інформаційної економіки, підприємництва та фінансів
(повна назва кафедри)

# Кваліфікаційна робота(проект)

магістра
(рівень вищої освіти)

на тему Моніторинг загроз інформаційної безпеки підприємства з використанням інформаційних технологій

Виконав: студент 2 курсу, групи 8.0519-ie
спеціальності 051 Економіка
(код і назва спеціальності)
спеціалізації _____
(код і назва спеціалізації)
освітньої програми Інформаційна економіка
(назва освітньої програми)
Н. І. Кан
(ініціали та прізвище)

Керівник доц., к.е.н., доц. Комазов П.В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя
2020

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

Інженерний навчально-науковий інститут
Кафедра інформаційної економіки, підприємництва та фінансів
Рівень вищої освіти магістр
Спеціальність 051 Економіка
(код та назва)
Спеціалізація _____
(код та назва)
Освітня програма Інформаційна економіка

**ЗАТВЕРДЖУЮ**
Завідувач кафедри_____
«_____»_____20____року

**З А В Д А Н Н Я**
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)СТУДЕНТОВІ (СТУДЕНТЦІ)

Кана Нікіфора Івановича
(прізвище, ім'я, по батькові)

1 Тема роботи (проекту) Моніторинг загроз інформаційної безпеки підприємства з використанням інформаційних технологій
_____
керівник роботи Комазов П. В., к.е.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від «____»_____20___року №_____
2 Строк подання студентом роботи _____
3 Вихідні дані до роботи показники інформаційної безпеки ТОВ «Южмаш груп»
_____
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Методологічні аспекти моніторингу загроз інформаційної безпеки підприємства. 2. Моделі оцінювання стану інформаційної безпеки підприємства. 3. Реалізація системи управління інформаційною безпекою підприємства.

4 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Концептуальна модель системи управління інформаційною безпекою на підприємстві. Основи інформаційної безпеки. Напрямки інформаційної безпеки. Етапи створення СЗІ. Процес формування СЗІ з використанням матриці знань.

5 Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| 1 | доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В. | | |
| 2 | доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В. | | |
| 3 | доцент, к.е.н. доцент кафедри інформаційної економіки, підприємництва та фінансів Комазов П.В. | | |

6 Дата видачі завдання_____

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Призначення наукових керівників. Затвердження тем дипломних робіт | | |
| 2 | Напрацювання теоретичного матеріалу: дослідження сутності об'єкту та предмету дослідження, критичний аналіз існуючих методологічних засад, вибір та обґрунтування напрямку проведення дослідження | | |
| 3 | Апробація результатів на Міжнародних та Всеукраїнських конференціях | | |
| 4 | Розробка економіко-математичного забезпечення основних елементів концептуального підходу | | |
| 5 | Збір та систематизація статистичного та нормативного матеріалу дослідження. | | |
| 6 | Узагальнення отриманих результатів. Оформлення роботи | | |
| 7 | Надання роботи та автореферату до рецензії. Нормоконтроль | | |
| 8 | Прилюдний захист дипломної роботи на засіданні ЕК | | |

Студент _____ Н. І. Кан
(підпис) (ініціали та прізвище)

Керівник роботи (проєкту) _____ П. В. Комазов
(підпис) (ініціали та прізвище)

**Нормоконтроль пройдено**

Нормоконтролер _____ _____
(підпис) (ініціали та прізвище)

# АНОТАЦІЯ

Кан. Н. І. Моніторинг загроз інформаційної безпеки підприємства з використанням інформаційних технологій.

Кваліфікаційна випускна робота для здобуття ступеня вищої освіти магістра за спеціальністю 051 – Економіка, науковий керівник П. В. Комазов. Інженерний навчально-науковий інститут ЗНУ, кафедра інформаційної економіки, підприємництва та фінансів, 2020.

Магістерська робота присвячена методологічним розробкам, теоретичним та практичним дослідженням процесу моніторингу загроз інформаційної безпеки підприємства з використанням інформаційних технологій. В дослідженні проаналізовано існуючі підходи до моніторингу загроз інформаційної безпеки підприємства. Розроблено концептуальну схему моніторингу стану інформаційної безпеки на підприємстві. Удосконалено комплекс моделей моніторингу системи захисту інформації на підприємстві. Практично реалізовано удосконалений комплекс моделей моніторингу системи захисту інформації на прикладі ТОВ «Южмаш груп».

Ключові слова: ЗАГРОЗА, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОНІТОРИНГ, МОДЕЛЮВАННЯ.

# ABSTRACT

Can. N. Monitoring of information security threats of the enterprise with the use of information technologies.

Qualification final work for obtaining a master's degree in specialty 051 – Economics, supervisor P. Komazov. Engineering Educational and Scientific Institute of ZNU, Department of Information Economics, Entrepreneurship and Finance, 2020.

The master's thesis is devoted to methodological developments, theoretical and practical research of the process of monitoring information security threats of the enterprise with the use of information technologies. The study analyzes the existing approaches to monitoring threats to information security of the enterprise. Conceptual provisions for monitoring the state of information security at the enterprise have been

developed. The set of models for monitoring the information protection system at the enterprise has been improved. An improved set of models for monitoring the information protection system on the example of Yuzhmash Group LLC has been practically implemented.

Key words: THREAT, INFORMATION, INFORMATION SYSTEM, INFORMATION SECURITY, INFORMATION PROTECTION SYSTEM, MONITORING, SIMULATION.

## АННОТАЦИЯ

Кан. Н. И. Мониторинг угроз информационной безопасности предприятия с использованием информационных технологий.

Квалификационная выпускная работа для получения степени высшего образования магистра по специальности 051 – Экономика, научный руководитель П. В. Комазов. Инженерный учебно-научный институт ЗНУ, кафедра информационной экономики, предпринимательства и финансов, 2020.

Магистерская работа посвящена методологическим разработкам, теоретическим и практическим исследованием процесса мониторинга угроз информационной безопасности предприятия с использованием информационных технологий. В исследовании проанализированы существующие подходы к мониторингу угроз информационной безопасности предприятия. Разработана концептуальная схема мониторинга состояния информационной безопасности на предприятии. Усовершенствован комплекс моделей мониторинга системы защиты информации на предприятии. Практически реализовано усовершенствованный комплекс моделей мониторинга системы защиты информации на примере ООО «Южмаш групп».

Ключевые слова: УГРОЗА, ИНФОРМАЦИИ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, МОНИТОРИНГ, МОДЕЛИРОВАНИЕ.

ЗМІСТ

ВСТУП……..…….. 7
РОЗДІЛ 1 МЕТОДОЛОГІЧНІ АСПЕКТИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА…… 10
1.1. Методологія управління інформаційною безпекою підприємства……...…….. 10
1.2. Сучасні підходи до класифікації загроз інформаційній безпеці……..……. 16
1.3. Стандарти, орієнтовані на управління ризиками інформаційної безпеки …….…… 31
1.4. Висновки до розділу 1……..…… 40
РОЗДІЛ 2 МОДЕЛІ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА….…….…… 42
2.1. Концептуальна схема системи управління інформаційною безпекою на підприємстві……..…… 42
2.2. Обґрунтування показника якості системи захисту інформації……..…….. 64
2.3. Модель моніторингу системи захисту інформації..…….. 69
2.4. Висновки до розділу 2…….……. 79
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА……...…….. 82
3.1. Аналіз стану інформаційної безпеки ТОВ «Южмаш груп»…….…. 82
3.2. Моніторинг якості системи захисту інформації ТОВ «Южмаш груп»…….. 93
3.3. Моделювання стану інформаційної безпеки ТОВ «Южмаш груп»……..... 99
3.4. Висновки до розділу 3……..…… 108
ВИСНОВКИ……..……..…….. 109
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..…….. 112
ДОДАТКИ……..…….. 118

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІС – інформаційна система

ІПС – інформаційно-пошукова система

ІДС – інформаційно-довідкова система

НСД – несанкціонований доступ

ПК – персональний комп’ютер

ІБ – інформаційна безпека

БІТ – безпека інформаційних технологій

ЗІ – захист інформації

СЗІ – система захисту інформації

ІТ – інформаційні технології

СУІБ – система управління інформаційною безпекою

# ВСТУП

*Актуальність*. За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу підприємствам реалізовувати власні інтереси, пришвидшують процеси обміну та співпраці. Проте неефективне використання інформації здатне послабити або завдати значної шкоди безпеці конкурентного підприємства, яке не має дієвої системи захисту від негативних інформаційних впливів.

Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Таким чином, інформаційна безпека є невід'ємною складовою ефективної діяльності підприємства.

Питанням інформаційної безпеки приділяється зараз більш ніж пильна увага, оскільки випадки втрати і крадіжки інформації можуть привести до краху підприємства або втрати конкурентних переваг на ринку. Таким чином, захист інформації від крадіжки, зміни або знищення придбала в цей час першочергове значення.

Безпека – не тільки технічна проблема, а також – проблема менеджменту.

Інформаційна безпека – організаційно-технологічна система організації, спрямована на ідентифікацію загроз та попередження негативних наслідків загроз для бізнесу. Основним завданням інформаційної безпеки є захист інформаційних ресурсів підприємства від внутрішніх та зовнішніх навмисних і ненавмисних загроз.

Постійно наростаючі кількісні та якісні зміни в сфері інформатизації, які мали місце в останні роки, слугували мотивом до проведення досліджень в області захисту інформації.

*Об'єкт дослідження*: інформаційна безпека підприємства.

*Предмет дослідження*: методи та моделі оцінювання інформаційної безпеки підприємства.

*Метою дослідження є* розробка концептуальних положень моніторингу загроз інформаційної безпеки підприємств.

Для досягнення мети були поставлені та вирішені такі *завдання*:

1. Проаналізовано існуючі підходи до моніторингу загроз інформаційної безпеки підприємства.
2. Розроблено концептуальну схему моніторингу стану інформаційної безпеки на підприємстві.
3. Удосконалено комплекс моделей моніторингу системи захисту інформації на підприємстві.
4. Практично реалізовано удосконалений комплекс моделей моніторингу системи захисту інформації на прикладі ТОВ «Южмаш груп».

*Методи дослідження.* Для вивчення та узагальнення наукових розробок використані методи порівняння, аналізу і синтезу, індукції і дедукції, статистичні й експертні методи дослідження. Застосовані методи економіко-математичного моделювання (розробка моделей), абстрактно-логічний метод (теоретичні узагальнення та формулювання висновків), статистико-економічний (аналіз статистичних даних, вибіркове спостереження, групування), економічні методи дослідження.

Наукова новизна одержаних результатів полягає у наступному:

*удосконалено:*

− підходи до побудови системи моніторингу інформаційної безпеки підприємства на основі «процесної моделі», що розглядається в Міжнародному стандарті ISO/IEC 27001:2005 «Інформаційні технології.

Технології безпеки. Система керування інформаційною безпекою. Вимоги». Це дозволяє координувати та керувати системою інформаційного захисту на всіх етапах створення і функціонування СУІБП.

*дістало подальшого розвитку:*

− застосування системного підходу при побудові інформаційного захисту, який відтворений в концептуальній схемі системи моніторингу інформаційної безпеки на підприємстві.

− застосування методу оцінювання якості системи захисту інформації в трьохмірному вимірюванні, а саме по: основам інформаційної безпеки, напрямкам інформаційної безпеки та етапам побудови систем захисту інформації.

Результати теоретичного аналізу проблеми інформаційного захисту інформації висвітлено на XXV науково-технічній конференції студентів, магістрів, аспірантів і викладачів ІННІ.

# РОЗДІЛ 1
# МЕТОДОЛОГІЧНІ АСПЕКТИ МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 1.1. Методологія управління інформаційною безпекою підприємства

Розвиток інформаційного суспільства і, як результат, перетворення в різних сферах суспільних відносин, включаючи й економічні, призвели до появи ряду позитивних і негативних наслідків. До позитивних наслідків відносять такі: пришвидшення передачі інформації значного обсягу, прискорення її обробки та впровадження [31], своєрідну трансформацію інформації, яка в наш час ототожнюється з цифровим або віртуальним простором.

Б. Кормич зазначає, що основні дії щодо збирання, зберігання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки та техніки ці інформаційні засоби і технології перетворилися на один із найважливіших компонентів інформаційних процесів, одночасно із самою інформацією та суб'єктами інформаційних відносин [21]. Значною мірою розвиток вищезгаданих інформаційних засобів й технологій має одночасні негативні прояви – як то збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку [31].

У зв'язку з цим окремим предметом наукових дискусій є питання щодо безпеки та захищеності відносин, пов'язаних зі збором, обробкою, зберіганням й використанням інформації. У співвідношенні з поняттями

«безпека» та «захищеність» «загрозою» можна вважати можливу небезпеку, тобто будь-які дії чи події, які можуть настати за різних обставин у навколишньому середовищі та стати передумовою порушення безпеки і завдання збитків.

Узагалі в інформаційних відносинах протягом останніх років сформувався та закріпився термін «інформаційна безпека», під яким розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдано шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [31]. Тобто вже в цьому визначенні закладено певні підстави для класифікації, однак про це згодом.

На думку В. Ліпкана, загрози національним інтересам та національній безпеці в інформаційній сфері є синонімом поняття «інформаційна безпека» [26]. Інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, а й шляхом глибокого усвідомлення усіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави [4].

Щодо правової науки, то, на думку А. Марущака, поглиблення досліджень з проблем інформаційної безпеки потрібно віднести до пріоритетів розвитку інформаційного права України. Загрози національній безпеці України, що виникають у сфері національних інформаційних ресурсів, зумовлюють актуальність наукових пошуків з проблем

правомірного використання телекомунікацій у сучасному інформаційному суспільстві, юридичних механізмів протидії кібернетичним загрозам [33].

Рівень сучасних викликів і загроз в інформаційній сфері наочно підтверджує справедливість і виключну значущість положень статті 17 Конституції України про те, що захист державного суверенітету і забезпечення інформаційної безпеки є однією з основних функцій держави і всього українського народу [36].

Інформаційна безпека як складова національної безпеки відповідно до сучасного розвитку її теорії в узагальненому вигляді ґрунтується на таких базових елементах: національні інтереси – загроза – захист [35]. Саме загрози стану захищеності суспільних відносин є важливим елементом процесу забезпечення інформаційної безпеки.

На нашу думку, це пояснюється тим, що інформаційну небезпеку створюють інформаційні загрози, які поширюються в інформаційному просторі. При цьому, інформаційні загрози – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в інформаційній сфері.

Враховуючи те, що інформаційна безпека є невід'ємною складовою національної безпеки, її регулювання потребує дієвих механізмів у формі політичних рішень або прийнятих нормативно-правових актів. Функціонування відповідного механізму, на нашу думку, можливе лише за умови належного рівня наукового осмислення теоретичних положень щодо інформаційної безпеки взагалі та сутності загроз зокрема. Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер. Таким чином, на практиці аналіз загроз – це завжди суб'єктивний процес сприйняття певною особою чи соціальною групою певних факторів через призму власних інтересів і фахового рівня. Разом із тим, об'єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище

втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу [5].

Водночас, звертаючись до визначення терміну «інформаційна безпека», слід визнати, що у науковій літературі відсутня єдина думка щодо його змісту. Так, А. Л. Корсунський під інформаційною безпекою України розуміє стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави [14].

Схоже визначення поняття «інформаційна безпека» пропонує А. В. Шубіна, яка вважає, що стан захищеності національних інтересів України в інформаційній сфері складається із сукупності збалансованих інтересів особистості, суспільства і держави із приводу захисту від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері [53].

З точки зору О. Л. Сорокіна, інформаційна безпека становить стан захищеності особистості, суспільства, держави від інформації, що носить шкідливий або протиправний характер, від інформації, що надає негативний вплив на свідомість особистості, перешкоджає сталому розвитку особистості, суспільства і держави. Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп’ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства і держави [45].

Дана позиція не підтримується іншими дослідниками, які вважають, що визначати «безпеку» через «захищеність» не зовсім коректно, оскільки ці слова – синоніми, а тому дані визначення є тавтологією. І.Ф. Бінько вважає, що звернення до поняття «стан захищеності» є цілком виправданим, якщо його немає, то немає і безпеки. У цьому сенсі мова йде про розуміння

безпеки у правовому, охоронному аспекті [3]. П. Д. Косач зазначає, що суть інституту інформаційної безпеки у системі інформаційного права полягає у здійсненні правових, організаційних, технічних заходів, що забезпечують безпечний стан всіх складових інформаційно-комунікаційного комплексу держави, окремих організацій і кожної людини [22].

Водночас у даному визначенні знову присутній елемент тавтології, знову поняття «безпека» визначається через поняття «безпечний стан».

Цимбалюк В. характеризує інформаційну безпеку як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [51].

Фурашев В. вважає, що інформаційна безпека – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності [52].

Гуцу С. пропонує розглядати інформаційну безпеку як стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [10].

Литвиненко О. під інформаційною безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [27].

Цікавим та водночас дискусійним є визначення Кормича Б., який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією України умови існування і розвитку людини, всього суспільства та держави [20].

Харченко Л., Ліпкан В., Логінов О. визначили, що інформаційна безпека – це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими

громадянами, за якого забезпечується інформаційний суверенітет України [49].

Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору. О. Сороківська визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [44]. М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації; доступність – це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність – це властивість захищеності точності та повноти даних; конфіденційний – це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи – це знання чи дані, які мають цінність для організації [46]. Враховуючи дані визначення, ми погоджуємося з А. Марущаком, що інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [32]. Отже, підсумовуючи вищезазначене, вважаємо за необхідне наголосити, що пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг.

## 1.2. Сучасні підходи до класифікації загроз інформаційній безпеці

Досліджуючи відносини у сфері забезпечення інформаційної безпеки, науковці звертають свою увагу на таке поняття, як «загрози інформаційній безпеці». Подальше заглиблення в процес наукового пізнання згаданого питання дало змогу виявити відсутність єдності у поглядах, що стосуються класифікації відповідних загроз як на нормативно-правовому, так і на науковому рівнях.

Відповідно до Закону України «Про основи національної безпеки України» до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [40].

Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України, класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, в екологічній сферах [12].

У Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки» загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження,

використання і порушення цілісності, конфіденційності та доступності інформації [39].

У Державному стандарті України «Захист інформації. Технічний захист інформації. Основні положення» – ДСТУ 3396.0-96 безпосереднє формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). У частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів [16].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» містить пункт 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [38].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз. Державний стандарт України «Захист інформації. Технічний захист інформації. Терміни та визначення» – ДСТУ 3396.2-97 містить ряд термінів, пов'язаних з інформаційною безпекою, які мають пряме відношення до класифікації загроз [47].

Так, пункт 5 «Загроза для інформації» містить наступні визначення:

5.1. Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

5.2. Порушення цілісності інформації – спотворення інформації, її руйнування або знищення.

5.3. Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено.

Така різноманітність класифікацій в чинному законодавстві обумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, а й відсутність належного теоретичного обґрунтування сутності загроз інформаційній безпеці. З метою узагальнення існуючих наукових поглядів щодо класифікації загроз інформаційній безпеці

та визначення концептуального підходу до формулювання цього елементу правовідносин пропонуємо розглянути окремі з них.

Згадуваний вище професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об'єктивні та суб'єктивні; за об'єктом впливу – особа; суспільство; держава [26].

В іншій праці, інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання, запропоновано такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання [25].

Схожі погляди на перелік загроз інформаційній безпеці висловлює: А. Логінов у власному дисертаційному дослідженні. Зокрема, вчений визначає загрози як:

– розкриття інформаційних ресурсів;

– порушення цілісності інформаційних ресурсів;

– збій у роботі обладнання [29].

Б. Кузьменко та О. Чайковська пропонують класифікацію загроз, яка ґрунтується на визначенні властивостей інформації:

– загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб'єкту, що не володіє повноваженнями для ознайомлення з нею;

– загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем;

– загрози порушення доступності інформації, що виникають в тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується [17, 23].

У свою чергу С. Гуцу [11] та О. Литвиненко [28] сходяться на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Л. Євдоченко, формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [15, 17].

Визначальною для процесу наукового пізнання є теза, що:

– трактування проблем, пов’язаних з інформаційною безпекою, для різних категорій суб’єктів може істотно відрізнятися, наприклад, безпека для закритих державних організацій та комерційних структур;

– інформаційна безпека не полягає винятково у захисті інформації. Це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (отримати матеріальні і/або моральні збитки) не тільки від несанкціонованого доступу до інформації, а й від пошкодження системи, що зумовить перерву в роботі [2, 17].

Тому цілком логічними та вартими на увагу є класифікації загроз які мають більш вузький або, іншими словами, спеціальний характер, зокрема загрози інформаційній безпеці мережевих ресурсів.

Наприклад, М. Макарова виділяє такі ймовірні загрози в мережі:

– дані навмисно перехоплюються, читаються або змінюються;

– користувачі ідентифікують себе неправильно (з шахрайською метою);

– користувач отримує несанкціонований доступ з однієї мережі до іншої [17, 30].

У цьому ж контексті ширшу класифікацію пропонує А. Погребняк, який зазначає, що загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз відносяться:

– помилки обслуговуючого персоналу і користувачів;

– втрата інформації внаслідок неправильного її збереження;

– випадкове знищення або заміна;

– збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі;

– некоректна робота програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо [17, 37].

До навмисних загроз відносяться:

– несанкціонований доступ до інформації і мережевих ресурсів;

– розкриття і модифікація даних і програм, їх копіювання;

– розкриття, модифікація або підміна трафіка обчислювальної мережі;

– розробка і поширення комп'ютерних вірусів, введення в програмне забезпечення логічних бомб;

– крадіжка магнітних носіїв і розрахункових документів;

– руйнування архівної інформації або навмисне її знищення;

– фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому;

– перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку [17, 18].

Загрози можна класифікувати за кількома критеріями:

– по аспекту інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;

– по компонентах інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримуюча інфраструктура);

– за способом здійснення (випадкові/навмисні, дії природного / техногенного характеру);

– по розташуванню джерела загроз (всередині/поза інформаційною системою) [40].

В якості основного критерію ми будемо використовувати перший, по аспекту інформаційної безпеки, залучаючи, при необхідності, інші. Найчастішими є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Інколи такі помилки і є власне загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (помилки адміністрування).

За деякими даними, до 65% втрат – наслідок ненавмисних помилок. Пожежі та повені не приносять стільки бід, скільки безграмотність і недбалість у роботі. Очевидно, самий радикальний спосіб боротьби з ненавмисними помилками – максимальна автоматизація і строгий контроль.

Інші загрози доступності класифікуємо за компонентами ІС, на які націлені загрози:

– відмова користувачів;

– внутрішня відмова інформаційної системи;

– відмова підтримуючої інфраструктури.

Зазвичай щодо користувачів розглядаються наступні загрози:

– небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості і при розходженні між запитами користувачів і фактичними можливостями та технічними характеристиками);

– неможливість працювати з системою через відсутність відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);

– неможливість працювати з системою в силу відсутності технічної підтримки (неповнота документації, недолік довідкової інформації та інше).

Основними джерелами внутрішніх відмов є:

– відступ (випадковий або навмисний) від встановлених правил експлуатації;

– вихід системи з штатного режиму експлуатації в силу випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації тощо);

– помилки при конфігуруванні системи;

– відмови програмного і апаратного забезпечення;

– руйнування даних;

– руйнування або пошкодження апаратури [50].

По відношенню до підтримуючої інфраструктури рекомендується розглядати наступні загрози:

– порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо-та / або теплопостачання, кондиціонування;

– руйнування або пошкодження приміщень;

– неможливість або небажання обслуговуючого персоналу та / або користувачів виконувати свої обов'язки.

Досить небезпечні так звані «скривджені» співробітники - нинішні і колишні. Часто вони прагнуть завдати шкоди організації – «кривднику», наприклад:

– зіпсувати обладнання;

– вбудувати логічну бомбу, яка з часом зруйнує програми та/або дані;

– видалити дані.

Колишні співробітники знайомі з порядками в організації і здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного та фізичного) до інформаційних ресурсів анулювалися [8].

Небезпечні, зрозуміло, стихійні лиха та події, що сприймаються як стихійні лиха, – пожежі, повені, землетруси, урагани. За статистикою, на частку вогню, води і тому подібних «зловмисників» (серед яких найпоширеніший перебій електроживлення) припадає 13% втрат, завданих інформаційним системам.

Загрози доступності можуть виглядати грубо – як ушкодження або навіть руйнування обладнання (в тому числі носіїв даних). Таке пошкодження може викликатися природними причинами (найчастіше – грозами).

На жаль, масово розповсюджені на сьогодні джерела безперебійного живлення не захищають від потужних короткочасних імпульсів, і випадки вигоряння устаткування – не рідкість.

В принципі, потужний короткочасний імпульс, здатний зруйнувати дані на магнітних носіях, можна згенерувати і штучним чином – за допомогою так званих високоенергетичних радіочастотних гармат. Але, напевно, в наших умовах подібну загрозу варто все ж визнати надуманою. Дійсно небезпечні протікання водопроводу і опалювальної системи. Часто організації, щоб заощадити на орендній платі, знімають приміщення в будинках старої споруди, роблять косметичний ремонт, але не змінюють старі комунікації. Влітку, в сильну спеку, схильні ламатися кондиціонери,

встановлені в серверних залах, набитих дорогим обладнанням. У результаті значної шкоди наноситься і репутації, і коштам організації [8].

Загальновідомо, що періодично необхідно проводити резервне копіювання даних. Однак навіть якщо ця пропозиція виконується, резервні носії часто зберігають недбало (до цього ми ще повернемося при обговоренні загроз конфіденційності), не забезпечуючи їх захист від шкідливого впливу навколишнього середовища. Перейдемо тепер до загроз доступності, перш за все – до програмних атак на доступність. В якості засобу виведення системи з штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). За розташуванням джерела загрози таке споживання поділяється на локальне і віддалене. При прорахунках в конфігурації системи локальна програма здатна практично монополізувати процесор або фізичну пам'ять, звівши швидкість виконання інших програм до нуля. Найпростіший приклад віддаленого споживання ресурсів – атака, що отримала найменування «SYN-повінь». Вона являє собою спробу переповнити таблицю «напіввідкритих» TCP-з'єднань сервера (встановлення з'єднань починається, але не закінчується). Така атака щонайменше ускладнює встановлення нових з’єднань з боку легальних користувачів, тобто сервер виглядає як недоступний [57].

По відношенню до атаки «Papa Smurf» уразливі мережі, що сприймають ping-пакети з широкомовними адресами. Відповіді на такі пакети «з'їдають» смугу пропускання. Віддалене споживання ресурсів останнім часом проявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання та/або обслуговування. Часом початку «моди» на подібні атаки можна вважати лютий 2000 року, коли жертвами виявилися кілька найбільших систем електронної комерції (точніше – власники і користувачі систем).

Відзначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною спроможністю мережі і продуктивністю сервера, то захиститися від розподілених атак на доступність вкрай важко [56].

Для виведення систем зі штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних та апаратних помилок.

Наприклад, відома помилка в процесорі Intel дає можливість локальному користувачеві шляхом виконання певної команди «підвісити» комп'ютер, так що допомагає тільки апаратний RESET. Програма «Teardrop» віддалено «підвішує» комп'ютери, експлуатуючи помилку в збірці фрагментованих IP-пакетів [58].

Одним із найнебезпечніших способів проведення атак є впровадження в системи, що атакуються, шкідливого програмного забезпечення. Ми виділимо наступні межі шкідливого програмного забезпечення:

– шкідлива функція;

– спосіб розповсюдження;

– зовнішнє уявлення.

Частина, що здійснює руйнівну функцію, будемо називати «бомбою».

Взагалі кажучи, спектр шкідливих функцій необмежений, оскільки «бомба», як і будь-яка інша програма, може володіти як завгодно складною логікою, але зазвичай «бомби» призначаються для:

– впровадження іншого шкідливого програмного забезпечення;

– отримання контролю над системою, яка атакується;

– агресивного споживання ресурсів;

– зміни або руйнування програм або даних.

По механізму розповсюдження розрізняють:

– віруси – коди, що володіють здатністю до поширення (можливо, зі змінами) шляхом впровадження в інші програми;

– «черв'яки» – код, здатний самостійно, тобто без впровадження в інші програми,
викликати поширення своїх копій по інформаційній системі та їх виконання (для активізації вірусу потрібно запуск зараженої програми).

Віруси-коди зазвичай поширюються локально, в межах вузла мережі; для передачі по мережі їм потрібна зовнішня допомога, така як пересилання зараженого файлу. «Черв'яки», навпаки, орієнтовані в першу чергу на пересування по мережі. Іноді саме поширення шкідливого програмного забезпечення викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, «черв'яки» «з'їдають» смугу пропускання мережі і ресурси поштових систем. З цієї причини для атак на доступність вони не потребують вбудовування спеціальних «бомб». Шкідливий код, який виглядає як функціонально корисна програма, називається троянським конем, або трояном. Наприклад, звичайна програма, будучи ураженою вірусом, стає троянською; деколи троянські програми виготовляють вручну і підсовують довірливим користувачам у привабливій упаковці. Вікно небезпеки щодо шкідливого програмного забезпечення з'являється з випуском нового різновиду «бомб», вірусів-кодів або «черв'яків» і перестає існувати з оновленням бази даних антивірусних програм [58].

За традицією, з усього шкідливого програмного забезпечення найбільшу увагу громадськості приділено вірусам. Дотримання нескладних правил «комп'ютерної гігієни» практично зводить ризик зараження до нуля. Там, де працюють згідно правил, число заражених комп'ютерів складає зазвичай лише долі відсотка.

На другому місці за розмірами збитку (після ненавмисних помилок і упущень) стоять крадіжки і підробки. За даними газети USA Today, ще в 1992 році в результаті подібних протиправних дій з використанням персональних комп'ютерів американським організаціям було завдано загальний збиток у розмірі 882 мільйонів доларів. Можна припустити, що реальний збиток був набагато більше, оскільки багато організацій зі зрозумілих причин

приховують такі інциденти; не викликає сумнівів, що в наші дні збиток від такого роду дій виріс багаторазово [57].

У більшості випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи і заходами захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні. Раніше ми проводили різницю між статичною та динамічною цілісністю. З метою порушення статичної цілісності зловмисник (як правило, штатний співробітник) може:

– ввести неправильні дані;

– змінити дані.

Потенційно уразливі з точки зору порушення цілісності не тільки дані, але й програми.

Загрозами динамічної цілісності є порушення транзакцій, крадіжка, дублювання даних або внесення додаткових повідомлень (мережевих пакетів тощо). Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

Конфіденційну інформацію можна розділити на предметну і службову.

Службова інформація (наприклад, паролі користувачів) не відноситься до визначеної предметної області, в інформаційній системі вона грає технічну роль, але її розкриття особливо небезпечне, оскільки воно загрожує отриманням несанкціонованого доступу до всієї інформації, в тому числі предметної. Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер. Багатьом людям доводиться виступати в якості користувачів не однієї, а цілого ряду систем (інформаційних сервісів). Якщо для доступу до таких систем використовуються багаторазові паролі чи інша конфіденційна інформація, то напевно ці дані будуть зберігатися не тільки в голові, але і в записнику або на листках паперу, які користувач часто залишає на робочому столі, а то й просто втрачає. І справа тут не в неорганізованості людей, а в недоліках

парольної схеми. Неможливо пам'ятати багато різних паролів; рекомендації по їх регулярній зміні тільки погіршують становище, змушуючи застосовувати нескладні схеми чергування або взагалі намагатися звести справу до двох-трьох легких паролів [58].

Описаний клас вразливих місць можна назвати розміщенням конфіденційних даних у середовищі, де їм не забезпечено (найчастіше – і не може бути забезпечено) необхідний захист. Крім паролів, що зберігаються в записниках користувачів, в цей клас потрапляє передача конфіденційних даних у відкритому вигляді (в розмові, в листі, по мережі), яка робить можливим перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі тощо), але ідея одна – здійснити доступ до даних в той момент, коли вони найменш захищені. Загрозу перехоплення даних слід брати до уваги не тільки при початковому конфігуруванні інформаційних систем, але і, що дуже важливо, при всіх змінах. Вельми небезпечною загрозою є виставки, на які багато організацій, недовго думаючи, відправляють обладнання з виробничої мережі, з усіма даними, що зберігаються на ньому. Залишаються колишніми паролі, при віддаленому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть в межах захищеної мережі організації; в об'єднаній мережі виставки – це занадто суворе випробування чесності всіх учасників. Ще один приклад зміни, про який часто забувають, – зберігання даних на резервних носіях. Для захисту даних на основних носіях застосовуються розвинені системи управління доступом; копії же нерідко просто лежать у шафах і отримати доступ до них можуть багато [1].

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються по багатьох каналах, їх захист може виявитися досить складним і дорогим. Технічні засоби перехоплення добре опрацьовані, доступні, прості в експлуатації, а встановити їх, наприклад, на кабельну мережу, може хто-завгодно, так що цю загрозу потрібно брати до

уваги по відношенню не тільки до зовнішніх, але і до внутрішніх комунікацій.

Крадіжки обладнання є загрозою не лише для резервних носіїв, але і для комп'ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто втрачають. Небезпечною нетехнічною загрозою конфіденційності є методи морально-психологічного впливу, такі як «маскарад» - виконання дій під виглядом особи, яка володіє повноваженнями для доступу до даних. До загроз, від яких важко захищатися, можна віднести зловживання повноваженнями. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, отримати доступ до пошти будь-якого користувача тощо. Інший приклад - нанесення збитку при сервісному обслуговуванні. Зазвичай сервісний інженер одержує необмежений доступ до устаткування і має можливість діяти в обхід програмних захисних механізмів. Такі основні загрози, які завдають найбільшої шкоди суб'єктам інформаційних відносин [58].

Правовідносини, що виникають у зв’язку із необхідністю забезпечувати безпеку інформаційних систем, найкраще врегульовані законодавством США. Ключову роль відіграє американський «Закон про інформаційну безпеку». Його мета – реалізація мінімально достатніх дій по забезпеченню безпеки інформації в федеральних комп'ютерних системах, без обмежень всього спектру можливих дій. Характерно, що вже на початку Закону називається конкретний виконавець – Національний інститут стандартів і технологій (NIST), відповідальний за випуск стандартів та настанов, спрямованих на захист від знищення і несанкціонованого доступу до інформації, а також від крадіжок і підробок, виконуваних за допомогою комп'ютерів. Таким чином, мається на увазі як регламентація дій фахівців, так і підвищення інформованості всього суспільства. Згідно Закону, всі оператори федеральних інформаційних систем, які містять конфіденційну інформацію, повинні сформувати плани забезпечення інформаційної безпеки.

Обов'язковим є і періодичне навчання всього персоналу таких інформаційних систем. NIST, у свою чергу, зобов'язаний проводити дослідження природи і масштабу вразливих місць, виробляти економічно виправдані заходи захисту. Результати досліджень розраховані на застосування не тільки в державних системах, але і в приватному секторі. Закон зобов'язує NIST координувати свою діяльність з іншими міністерствами і відомствами, включаючи Міністерство оборони, Міністерство енергетики, Агентство національної безпеки (ANS) та інші, щоб уникнути дублювання і несумісності.

## 1.3. Стандарти, орієнтовані на управління ризиками інформаційної безпеки

В загальному в світі існує кілька десятків різного роду методик і підходів до оцінки ризиків ІБ, таких як: Austrian IT Security Handbook, AS / NZS4360, BSI 100-3, CRISAM, EBIOS, HB167: 200X, ISF IRAM, CRAMM, ISO 27005, MAGERIT, MARION, MEHARI, NIST SP800-30, OCTAVE, OSSTMMRAV, SOMAP та інші, але частина з них вже застаріла і не розвивається, частина не володіє актуальними перекладами на англійську мову з мови країни походження, що робить складним їх вивчення для широкої аудиторії. В даній роботі будуть розглянуті саме ті методики, які містять розгорнутий підхід, досить широко відомі в Україні і продовжують розвиватися (або ще не втратили своєї актуальності) і відносно легко доступні.

Вибір тієї чи іншої методики залежить від рівня вимог, що ставить перед собою підприємство до забезпечення безпеки інформації, характеру загроз, що беруться до уваги, і ефективності контрольних заходів щодо захисту інформації.

ДСТУ ISO/IEC 27005:2015. ISO 27005 – це стандарт із серії 2700x, що описує підхід до організації всього процесу з управління ризиками інформаційної безпеки. Представлена в стандарті методика оцінки є

класичною і має за недоліки зайву академічність і загальність формулювань. Даний стандарт описує настанови і рекомендується до ознайомлення з метою формування загального уявлення про організацію процесу з управління ризиками ІБ [55]. Що мається на увазі під «ризиком» в даному стандарті: ризик – ефект невизначеності на цілі (ефект – це відхилення від передбачуваного (позитивного і / або негативного). Ризик зазвичай виражається у вигляді комбінації наслідків події ІБ і відповідної ймовірності її виникнення. Невизначеність-це недостатність (навіть часткова) інформації, пов’язаної зрозумінням події або знаннями про подію, її наслідками або можливістю виникнення.

Процес менеджменту ризиків інформаційної безпеки складається з визначення обставин, оцінки ризику, обробки ризику, прийняття ризику,обміну інформацією щодо ризику, а також моніторингу та перегляду ризику (рис. 1.1).

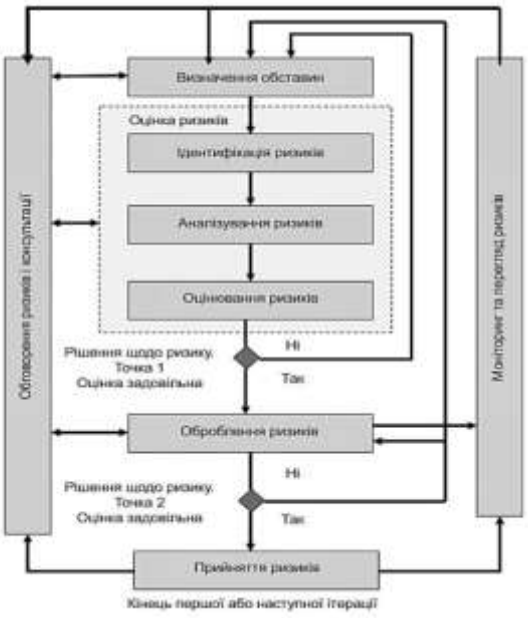


Рисунок 1.1 – Ілюстрація процесу управління ризиками ІБ за стандартом ISO 27005

*Джерело: [9]*

На етапі визначення обставин визначаються зовнішні та внутрішні обставини для управління ризиками ІБ, що передбачає встановлення базових критеріїв, необхідних для управління ризиками інформаційної

безпеки,визначення сфери застосування та її меж й забезпечення функціонування управління ризиками інформаційної безпеки прийнятого для організації. Базові критерії:

– критерії зіставлення ризиків;

– критерії впливу;

– критерії приймання ризиків.

Оцінка ризиків складається з таких дій:

– ідентифікація ризику;

– аналіз ризиків;

– зіставлення ризиків.

Метою ідентифікації ризику є визначення того, що могло б статися, щоб спричинити потенційні втрати, і щоб отримати уявлення про те, як, де і чому ці 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 для організації 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.

Для оцінювання ризиків підприємства виміряні ризики повинні порівнюватися з критеріями оцінювання ризику.

Для обробки ризику є чотири варіанти: модифікація ризику, прийняття ризику, усунення ризику і розподілення ризику.

NIST SP800-30. В NIST SP800-30 представлені підходи не тільки до оцінки ризиків, а й до організації діяльності з управління ризиками

інформаційної безпеки на різних рівнях (від стратегічного до прикладного на рівні окремих інформаційних систем). На відміну від ISO 27005 даний документ містить більш розгорнуті описи кожного з елементів, а також рекомендації щодо застосування на практиці в різних ситуаціях.

Методика NIST SP800-30 передбачає попереднє оцінювання двох параметрів [19]: потенційного збитку і ймовірності реалізації загрози. Застосування системи управління ризиками безпосередньо пов’язано з можливістю підприємств виконувати свої основні функції в умовах постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків охоплює широке коло завдань, які пов’язані зі стратегією управління ризиками і є основою для розробки власної системи управління ризиками. Запропонований процес оцінювання ризику інформаційної безпеки, представляється у вигляді таблиці, яка відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної,зокрема ризику, оцінюється за трирівневою шкалою. Такий механізм отримання оцінок ризику істотно обмежує точність результатів.

Управління ризиком являє собою процес ідентифікації ризику, процес оцінки рівня ризику і процес здійснення заходів, спрямованих на зменшення ризику до прийнятного рівня.

Мета виконання процесів управління ризиком полягає в тому, щоб дати можливість підприємству виконати свою місію за рахунок:

Підвищення безпеки IT-систем, які зберігають, обробляють або передають інформацію в межах і поза організацією;

Підвищення інформованості та обізнаності керівництва щодо прийнятих рішень з управління ризиком для отримання обґрунтованих обсягів витрат, які повинні ставати невід’ємною частиною загального бюджету IT;

Надання допомоги керівництву в авторизації своїх IT-систем на основі результатів, що випливають з виконання процесів управління ризиком.

Управління ризиками є ітеративним процесом і його дії відбуваються на кожній стадії життєвого циклу розвитку ІТ-системи. Зменшення негативного впливу на організацію і потреба в нормальній базі для прийняття рішення становлять фундаментальні передумови для того, щоб організації здійснювали процес управління ризику для своїх ІТ-систем. Використання такої методики передбачає наступні етапи:

– опис характеристик системи;

– ідентифікація загроз;

– ідентифікація вразливостей;

– аналіз наявних засобів захисту;

– визначення значення ймовірності;

– аналіз впливу;

– визначення значення ризику;

– вибір засобів захисту;

– документування отриманих результатів.

Методологія оцінки ризику охоплює дев’ять головних кроків (табл. 1.1).

OCTAVE. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – методика проведення оцінки ризиків в організації, що була розроблена інститутом Software Engineering Institute (SEI) при університеті Карнегі Меллон (Carnegie Mellon University).

Цей підхід був створений, щоб допомогти організаціям ідентифікувати і оцінити ризики інформаційних систем, поліпшити їх можливості і захистити себе від цих ризиків.

Особливість даної методики полягає в тому, що весь процес аналізу проводиться силами співробітників організації, без залучення зовнішніх консультантів. Для цього створюється спільна група, що включає як технічних фахівців, так і керівників різного рівня, що дозволяє всебічно оцінити наслідки для бізнесу можливих інцидентів в області безпеки і розробити контрзаходи.

*Таблиця 1.1*

**Загальна схема оцінки ризику за NIST SP800-30**

| Вхід | Дії оцінки ризику | Результати |
|---|---|---|
| • Комп'ютерне обладнання<br>• Програмне забезпечення<br>• Системні інтерфейси<br>• Дані та інформація<br>• Люди | Крок 1. Характеристика системи | • Межі системи<br>• Функції системи<br>• Критичність системи і даних<br>• Чутливість |
| • Історія атак на систему<br>• Дані від розвідувальних агентств, NIPC, OIG, FedCIRC, ЗМІ | Крок 2.Ідентифікація загроз | • Формулювання загроз |
| • Звіти за попередніми оцінками ризиків<br>• Результати аудитів<br>• Вимоги до безпеки<br>• Результати тестування безпеки | Крок 3. Ідентифікація вразливостей | • Перелік потенційних точок вразливостей |
| • Поточний стан контролю<br>• Плановані заходи щодо контролю | Крок 4. Аналіз контролю | • Перелік поточних і планованих заходів щодо проведення контролю |
| • Мотивація джерел загроз<br>• Ймовірність загроз<br>• Природа уразливості<br>• Поточний стан контролю | Крок 5. Визначення ймовірності | • Рейтинги ймовірності здійснення загроз |
| • Аналіз впливу на роботу<br>• Оцінка критичності активів<br>• Критичність даних<br>• Чутливість даних | Крок 6.Аналіз впливу | • Рейтинги впливу загроз |
| • Ймовірність загрози для експлуатації<br>• Розміри впливу<br>• Адекватність планованих або поточних заходів з контролю | Крок 7. Визначення ризику | • Ризики і рівні допустимих ризиків |
| Н/З | Крок 8. Рекомендації з контролю | • Рекомендовані заходи щодо контролю |
| Н/З | Крок 9.Документальне оформлення результатів | • Звіт по оцінці ризиків |

OCTAVE передбачає наступні фази аналізу [54] (рис. 1.2):

1. Встановлення критеріїв оцінки ризику;

2. Розробка профілю загроз, пов'язаних з активом та місцями його зберігання;

3. Ідентифікація інфраструктурних вразливостей;

4. Розробка стратегії і планів безпеки.

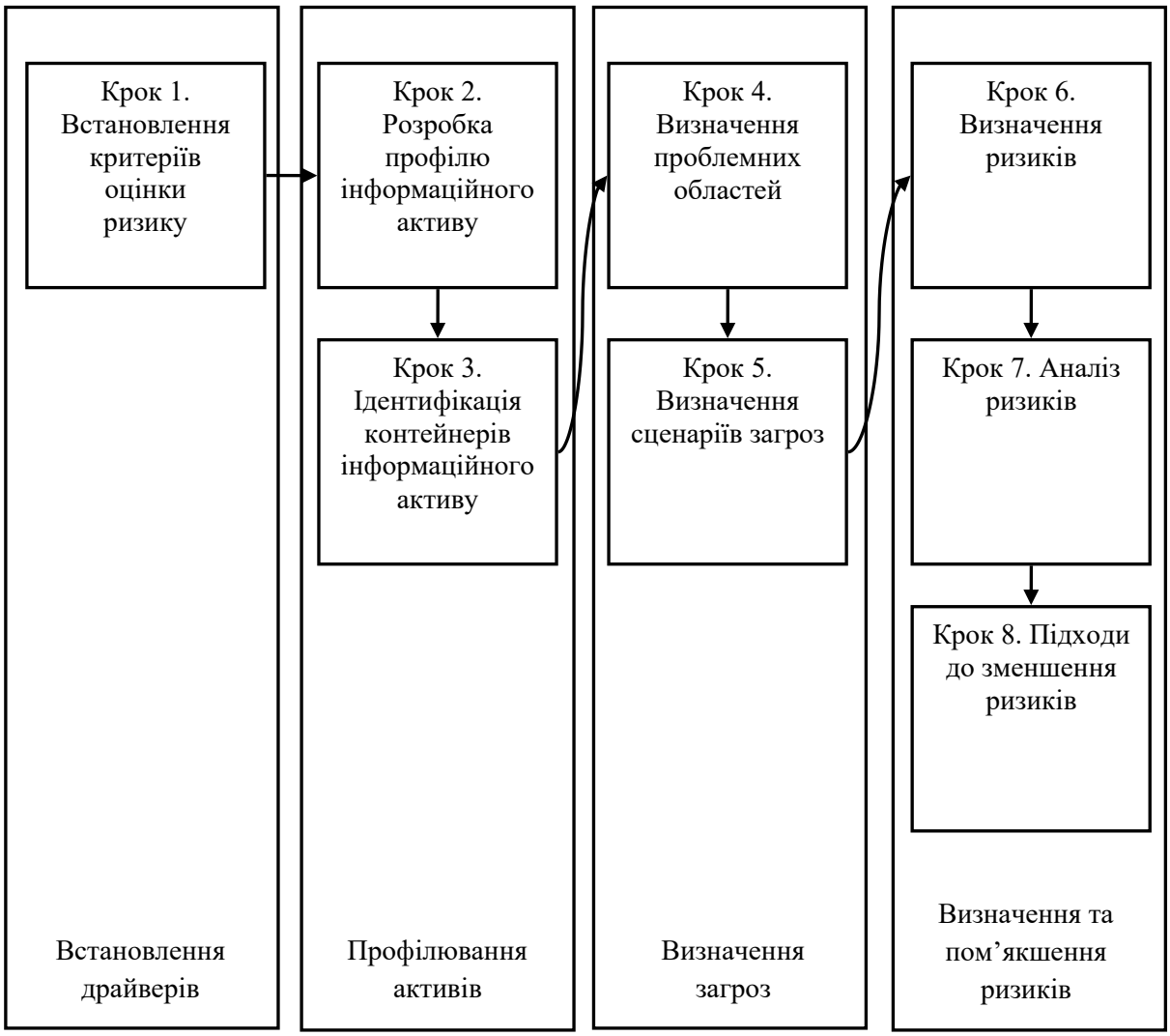


Рисунок 1.2 – Модель OCTAVE

*Джерело: [9]*

Профіль загрози включає в себе актив, тип доступу до активу, джерело загрози, тип порушення або мотив, результат і посилання на опис загрози в загально-доступних каталогах. За типом джерела, загрози в OCTAVE діляться на:

– загрози, які виходять від людини-порушника, який діє через мереж у передачі даних;

– загрози, які виходять від людини-порушника, який використовує фізичний доступ;

– загрози, пов'язані зі збоями в роботі системи.

Результатом може бути розкриття, модифікація, втрата або руйнування інформаційного ресурсу або розрив підключення, відмова в обслуговуванні.

Методика OCTAVE пропонує при описі профілю використовувати «дерево варіантів» (приклад подібного дерева для загроз типу 1 наведено на рис. 1.3. При створенні профілю загроз рекомендується уникати великої кількості технічних деталей-це завдання другого етапу дослідження. Головне завдання першої стадії-стандартизованим чином описати поєднання загрози і ресурсу.

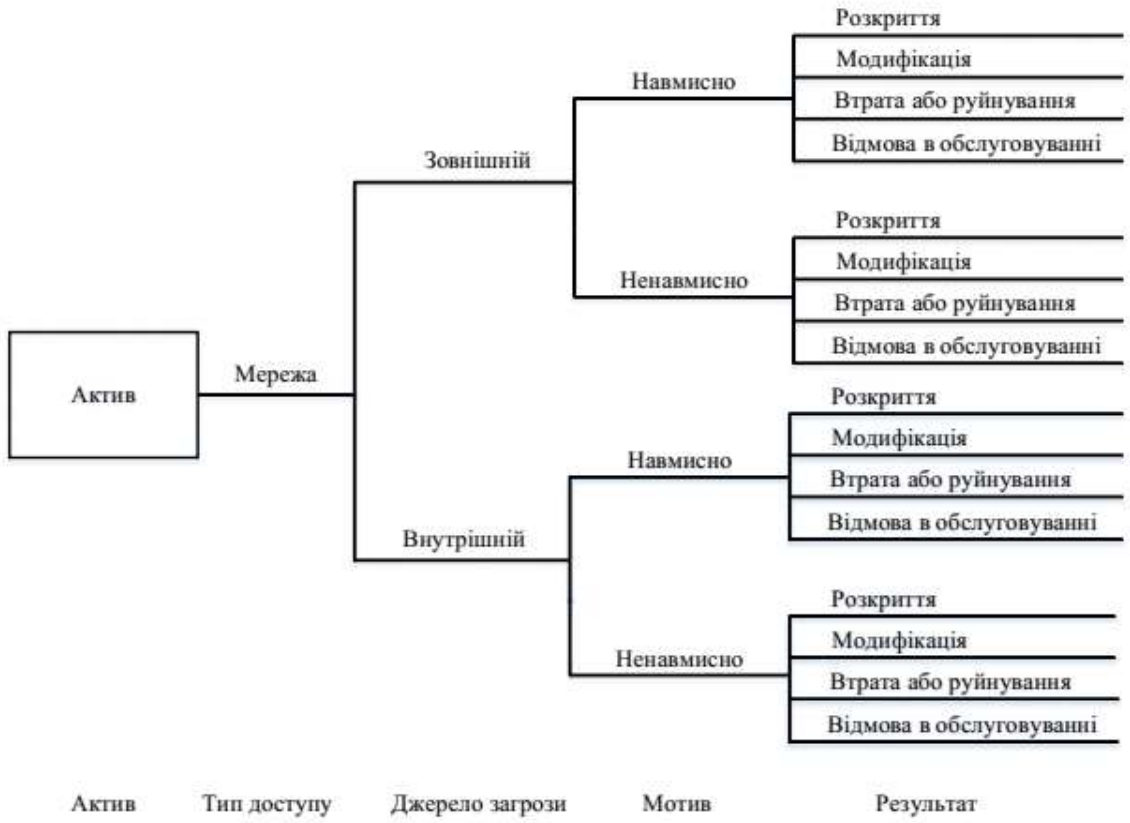


Рисунок 1.3 – Дерево варіантів, що використовується при описі профілю

*Джерело: [9]*

Друга фаза дослідження системи відповідно до методики-ідентифікація інфраструктурних вразливостей. В ході цієї фази визначається інфраструктура, що підтримує існування активу (наприклад, якщо це база даних відділу кадрів, то для роботи з нею потрібен сервер, на якому розміщена БД, робоча станція співробітника відділу кадрів) і те оточення, яке може дозволити отримати до неї доступ (наприклад, відповідний сегмент

локальної мережі). Розглядаються компоненти наступних класів: сервери; мережеве обладнання; СЗІ; персональні комп'ютери; домашні персональні комп'ютери користувачів, що працюють віддалено, але мають доступ до мережі організації; мобільні комп'ютери; системи зберігання; бездротові пристрої;інше.

Група, яка проводить аналіз для кожного сегмента мережі, зазначає, які компоненти в ньому перевіряються на наявність вразливостей. Вразливості перевіряються сканерами безпеки на рівні операційної системи, мережевими сканерами безпеки, спеціалізованими сканерами (для конкретних web-серверів, СУБД та ін.), за допомогою списків вразливостей, тестових скриптів.

Для кожного компонента визначається:

1. Список вразливостей, які треба усунути негайно;

2. Список вразливостей, які треба усунути найближчим часом;

3. Список вразливостей, щодо яких не потрібно негайних дій;

За результатами стадії готується звіт, в якому вказується, які вразливості виявлені, який вплив вони можуть надати на активи, які заходи треба вжити для усунення вразливостей.

Розробка стратегії і планів безпеки-третя стадія дослідження системи. Вона починається з оцінки ризиків, яка проводиться на основі звітів по двом попереднім етапам. У OCTAVE при оцінці ризику дається тільки оцінка очікуваного збитку, без оцінки ймовірності. Шкала: високий, середній,низький. Оцінюється фінансовий збиток, збиток для репутації компанії, життю та здоров'ю клієнтів і співробітників, збиток, який може викликати службове розслідування в результаті того чи іншого інциденту. Описуються значення,що відповідають кожній градації шкали (наприклад, для малого підприємства фінансовий збиток в $10000 – збиток високого рівня, для більшого-середнього).

Далі, розробляють плани зниження ризиків декількох типів:

– довгострокові;

– на середню перспективу;

– списки завдань на найближчий час.

Для визначення заходів протидії загрозам в методиці пропонуються каталоги засобів.

На відміну від інших методик, OCTAVE не передбачає залучення для дослідження безпеки ІС сторонніх експертів, а вся документація по OCTAVE загальнодоступна і безкоштовна, що робить методику особливо привабливою для підприємств з обмеженим бюджетом, виділеним на цілі забезпечення ІБ.

Таким чином, охарактеризувавши три найбільш поширені методики з управління ризиками в сфері інформаційної безпеки і здійснивши аналіз основних властивостей цих методик, стає можливим визначення відмінностей,основних переваг та недоліків методик ISO27005, NIST SP800-30, OCTAVE (табл. 1.2).

## 1.4. Висновки до розділу 1

У світовій практиці вже давно використовується таке поняття, як комплексна система захисту, під якою мається на увазі єдина сукупність законодавчих, організаційних і технічних заходів, спрямованих на виявлення, відбиття та ліквідацію різних видів загроз безпеки.

На основі принципів і положень державної політики забезпечення інформаційної безпеки повинні проводитися всі заходи щодо захисту інформації в політичній, економічній, оборонній й іншій сферах діяльності держави.

Генеральним напрямком пошуку шляхів захисту інформації є неухильне підвищення системності підходу до самої проблеми захисту інформації.

Різноманітність потенційних загроз інформації в ІС настільки велике, що не дозволяє передбачити кожну з них, тому аналізовані характеристики загроз варто вибирати з позицій здорового глузду,

одночасно виявляючи не тільки самі загрози, імовірність їхнього здійснення, розмір потенційного збитку, але і їхні джерела.

Для побудови системи управління інформаційної безпекою, аналіз загроз інформаційній безпеці є одним з основних етапів, які повинні бути успішно виконаними. Саме тому вкрай важлива можливість впровадження швидкого і порівняно простого управління загрозами інформаційній безпеці підприємства.

Було проаналізовані відомі методології з аналізу ризиків інформаційній безпеці, такі як ISO 27005, NIST SP800-30, OCTAVE. Проведено порівняльний аналіз даних методологій, виявлено їх недоліки та переваги. На основі проведеного аналізу, можна зробити висновок, що оптимальним варіантом для вибору методики управління загрозами інформаційної безпеки в контексті забезпечення безпеки інформації підприємства та місцям її зберігання, обробки та передачі є адаптація та удосконалення відомих методик логічним об’єднанням їх переваг і мінімізацією недоліків.

*Таблиця 1.2*

## Порівняння методів оцінки ризиків

| Методи оцінки ризиків | Наявність перекладу українською або російською мовою | Орієнтація на розмір підприємства | Наявність програмного інструментарію | Фази підходу | Тип оцінки ризику | Обробка ризиків | Необхідність вресурсах |
|---|---|---|---|---|---|---|---|
| ISO 27005 | + | Можливе застосування для організацій різного розміру і галузей | + | • Визначення обставин<br>• Ідентифікація ризику<br>• Аналізування ризику<br>• Оцінювання ризику<br>• Оброблення ризику<br>• Прийняття ризиків | Загальні настанови щодо якісної чи кількісної оцінки | • Модифікація<br>• Прийняття<br>• Усунення<br>• Розподілення | Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження |
| NIST SP800-30 | - | Застосовується для підприємств різного розміру. Розроблено, в першу чергу, для використання в федеральних організаціях США | + | • Характеристика системи<br>• Ідентифікація загроз<br>• Ідентифікація вразливостей<br>• Аналіз контролю<br>• Визначення ймовірності<br>• Аналіз впливу<br>• Визначення ризику<br>• Рекомендації з контролю<br>• Документальне оформлення | Змішана оцінка ризиків | • Прийняття<br>• Запобігання<br>• Обмеження<br>• Планування<br>• Дослідження і повідомлення<br>• Перенесення | Необхідне залучення співробітників як зі сторони IT, так і бізнесу. Можливе залучення третіх сторін для впровадження |
| OCTAVE | - | Можливе застосування для організацій різного розміру і галузей | + | • Встановлення критеріїв оцінки ризику<br>• Розробка профілю інформаційного активу<br>• Ідентифікація контейнерів інформаційних активів<br>• Визначення проблемних областей<br>• Визначення сценаріїв загроз<br>• Визначення ризиків<br>• Аналіз ризиків<br>• Підходи до зменшення ризику | Якісна оцінка ризиків | • Зниження<br>• Прийняття | Власні ресурси організації, не експерти. Необхідне залучення співробітників як зі сторони IT, так і бізнесу |

# РОЗДІЛ 2
# МОДЕЛІ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1. Концептуальна модель системи управління інформаційною безпекою на підприємстві

Труднощі дослідження питань забезпечення безпеки інформаційних технологій збільшується великою невизначеністю умов функціонування інформаційної системи.

Постановка задачі забезпечення захисту інформації, як правило, виявляється некоректною оскільки найчастіше формулюється в умовах непередбачуваності поводження системи в нестандартних, екстремальних ситуаціях. Вплив невизначеності особливо сильно проявляється в нестабільних, слабко організованих ІС через неповноту, несвоєчасність та низьку вірогідність інформації.

У зв’язку із цим задачі забезпечення безпеки інформації, як правило, не мають властивості одиничності рішення, ефективність та оптимальність якого визначаються ступенем обліку обмежень, характерних для конкретної ситуації. Для підвищення ступеня коректності постановки задач забезпечення безпеки інформації необхідно підвищувати знання про ІС у мінливих умовах її функціонування [24].

У зв’язку із цим одержання та використання знань повинні здійснюватися безпосередньо в процесі функціонування системи шляхом поступового нагромадження необхідної інформації, аналізу та її використання для ефективного виконання системою заданої цільової функції в умовах внутрішнього і зовнішнього мінливого середовища.

Відомі математичні моделі, використовувані для опису структури, поводження та керування СЗІ, в умовах некоректної постановки задач, не дають

бажаного результату. Тому необхідна розробка нових, орієнтованих на специфіку процесів захисту інформації, методів і засобів моделювання.

Для одержання інформації про поводження СЗІ потрібно виділити групи параметрів і визначити часи перевірки їхніх значень. При цьому розглядаються особливо значимі та важливі, з погляду реалізації мети функціонування системи, параметри.

Перевірка та аналіз значень зазначених параметрів, необхідних для підвищення знань про систему, повинні здійснюватися таким чином, щоб забезпечити можливість прийняття своєчасних і достовірних рішень та коректування поводження системи в процесі функціонування. Таким чином, в СЗІ обов'язково повинне бути передбачене виконання процедур контролю її працездатності та діагностування станів.

Прийняття рішень в більшості випадків базується на експертних оцінках. Однак в умовах невизначеності вхідних даних і некоректності постановки задач керування ці оцінки можуть внести додаткову некоректність у прийняте рішення, збільшивши тим самим вихідну невизначеність [6].

Вирішення проблем моделювання СЗІ вимагає поетапного виконання наступних досліджень:

1. Розробка принципів, методів і засобів скорочення розмірності опису СЗІ, що включає:

– аналіз інформаційної структури системи та взаємозв'язків між розв'язуваними в ній завданнями;

– аналіз динамічних характеристик рішення завдань;

– аналіз кореляційних залежностей між параметрами системи, що є результатами рішення окремих завдань;

– виділення на основі аналізу сукупностей завдань, результат рішення кожної з яких дозволяє визначити один з контрольованих параметрів системи.

У результаті розробки повинні бути сформульовані вимоги та рекомендації з раціональної організації структури СЗІ, декомпонованої по

рівнях контролю і керування. Це дозволить проводити подальші дослідження в умовах мінімізованої розмірності опису системи.

2. Розробка методології, методів і засобів рішення завдань забезпечення безпеки інформації в умовах невизначеності, що включає:

– дослідження питань коректності постановки задач при недостатнім розумінні кінцевих результатів і цілей рішення в різко мінливих умовах;

– дослідження питань використання невизначеності (неповноти, низької вірогідності) вхідних даних при рішенні завдань забезпечення безпеки інформації.

Результатом досліджень повинна з’явитися розробка методологічних основ, методів і засобів рішення некоректно поставлених завдань в умовах невизначеності [6].

Розробка ідеології, методів і засобів адаптивного контролю параметрів і діагностування станів системи, включає наступні завдання:

1. Формування динамічних зон (нормального функціонування, попередження, тривоги, катастрофи), що характеризують різні стани економічної системи та динамічних порогів, що розділяють ці зони, виділення інтегральних динамічних векторів індикації станів системи.

2. Розробку ідеології та стратегії виконання адаптивного (за часом проведення, кількості і номенклатури контрольованих параметрів) контролю векторів індикації, прогнозування тенденцій зміни їхніх значень у процесі функціонування системи.

3. Розробку методів та алгоритмів адаптивного одиночного і групового контролю та прогнозування значень компонентів векторів індикації.

4. Розробку методів та алгоритмів розпізнавання та ідентифікації належності станів системи динамічним зонам і порогам на підставі аналізу поточних і прогнозованих значень окремих компонентів і векторів індикації в цілому.

5. Розробку методів та алгоритмів діагностування системи на основі аналізу результатів ідентифікації по всіх векторах індикації.

Результатом розробки повинне бути створення ідеології, математичних методів і засобів для організації адаптивного контролю та діагностування станів СЗІ.

Розробка принципів, методів і засобів самоорганізації СЗІ, включає наступні завдання [42]:

1. Конструювання адаптивних моделей для опису структури та поводження системи, прогнозування значень її параметрів.

2. Конструювання адаптивних моделей для формування підмножин контрольованих параметрів і діапазонів значень зон їхнього контролю на основі заданих вимог до стійкості функціонування системи.

3. Конструювання адаптивних моделей контролю працездатності та діагностування порушень працездатності системи.

4. Самоорганізацію та саморозвиток сімейств моделей для опису структури, поводження, прогнозування, контролю та діагностування з урахуванням забезпечення необхідної стійкості системи в умовах впливу факторів внутрішнього й зовнішнього середовища.

Результатом досліджень повинні бути створені на основі відомих і спеціально розроблених методів і засобів адаптивні моделі для опису структури та поводження СЗІ, а також контролю, діагностування та прогнозування її станів.

Розробка методів і засобів підтримки прийняття рішень, включає наступні завдання:

1. Розробку методів і засобів вибору рішень із усієї безлічі альтернативних варіантів на підставі аналізу стану та поводження системи з урахуванням вимог керування, реального ресурсу, що задовольняє цим вимогам, оцінок близьких і віддалених наслідків виконання ухвалених рішень.

2. Розробку методів і засобів декомпозиції ухвалених рішень щодо рівнів керування системи.

3. Розробку методів і засобів підтримки прийняття рішень по самоорганізації системи в процесі її функціонування для вдосконалювання всіх видів перерахованих вище моделей та їхніх сімейств.

Дослідження базуються на використанні всіх отриманих раніше результатів і орієнтовані на створення банку знань про СЗІ.

Для рішення перерахованих інших теоретичних і прикладних проблем необхідна цілеспрямована, виконувана в рамках державних програм і на єдиній концептуальній та методологічній основі, організація комплексних досліджень проблем забезпечення безпеки інформації.

Загальними моделями систем і процесів захисту інформації названі такі, які дозволяють визначати (оцінювати) загальні характеристики зазначених систем та процесів на відміну від локальних моделей, які забезпечують визначення (оцінки) деяких локальних або часток характеристик систем чи процесів.

Системну класифікацію загальних моделей у цей час зробити практично неможливо, через мале число таких моделей (для цього немає достатніх даних). Тому класифікацію моделей представимо простим переліком і короткою характеристикою лише [13].

1. Загальна модель процесу захисту інформації. Дана модель у самому загальному виді для самого загального об’єкта захисту повинна відображати процес захисту інформації як процес взаємодії дестабілізуючих факторів, що впливають на інформацію, засобів захисту інформації, які перешкоджають дії цих факторів. Підсумком взаємодії буде той або інший рівень захищеності інформації.

2. Узагальнена модель системи захисту інформації. Це подальший розвиток загальної моделі процесу захисту. Вона повинна відображати основні процеси, здійснювані в цій моделі з метою раціоналізації процесів захисту. Зазначені процеси в самому загальному виді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяють на захист інформації.

3. Модель загальної оцінки загроз інформації. Основною спрямованістю цієї моделі є оцінка не просто загроз інформації, а ще й оцінка тих втрат, які можуть мати місце при проявів різних загроз. Моделі даного напрямку важливі ще й тим, що саме на них найбільшою мірою були виявлені ті умови, при яких такі оцінки можуть бути адекватні реальним процесам захисту інформації.

4. Моделі аналізу систем розмежування доступу до ресурсів ІС. Моделі цього класу призначені для забезпечення рішення завдань аналізу та синтезу систем (механізмів) розмежування доступу до різних видів ресурсів ІС і, насамперед, до масивів даних. Виділення цих моделей у самостійний клас загальних моделей обумовлене тим, що механізми розмежування доступу ставляться до числа найбільш істотних компонентів систем захисту інформації, від ефективності функціонування яких, значною мірою залежить загальна ефективність захисту інформації в ІС.

Основне призначення загальних моделей СЗІ складається в створенні передумов для об’єктивної оцінки загального стану ІС із погляду міри уразливості або рівня захищеності інформації в ній. Необхідність у таких оцінках звичайно виникає при аналізі загальної ситуації з метою вироблення стратегічних рішень при організації захисту інформації.

Останнім часом вимоги до захищеності інформації на підприємстві значно зросли. Це пов’язано з розвитком інформаційних технологій, що безпосередньо беруть участь на всіх етапах господарювання підприємства.

Життєвий цикл інформації містить у собі наступні етапи: збір або створення, зберігання, передача й одержання, обробка й знищення. Ці етапи проходять в умовах дії різних факторів, що прагнуть порушити природний плин інформаційних процесів. Узагальнюючої для різних факторів такого роду є поняття загроз інформаційної безпеки. Незважаючи на незмінність сутності загроз, конкретні способи порушення інформаційної безпеки постійно і активно розвиваються.

Загрози спрямовані на порушення основних властивостей інформації:

– конфіденційності;

– цілісності – точності й повноти інформації й комп’ютерних програм;

– доступності – для користувачів, коли це потрібно.

Саме ці властивості можуть мати особливе значення для забезпечення конкурентоспроможності, руху грошових коштів, рентабельності, відповідність правовим нормам й іміджу підприємства.

Будь-якій організації необхідно ідентифікувати та керувати багатьма задачами з метою ефективного функціонування. Будь-яка задача, що використовує ресурси та керована з метою отримання трансформації вхідних даних у вихідні, може бути розглянута як процес. Застосування системи процесів в межах підприємства разом з визначенням та взаємодією схожих процесів та їх керуванням, може розглядатися як «процесний підхід». Даний підхід до керування інформаційною безпекою розглянутий в Міжнародному стандарті ISO/IEC 27001 «Інформаційні технології. Технології безпеки. Система керування інформаційною безпекою. Вимоги» [34].

Розробка та забезпечення СУІБ підприємства визначається його потребами та цілями, вимогами безпеки, здійснюваними процесами та розміром і структурою підприємства. Враховуючі перераховані дані, державні, міжнародні стандарти та науково-методичні розробки формується політика СУІБП, яка виступає початковим етапом побудови СУІБП.

На рис. 2.1. початковим етапом побудови СУІБП є блок вхідних даних.

Функціональне призначення даного блоку полягає в накопиченні, систематизації та зведенні первинної інформації для постановки задачі моделювання.

Цей блок складається з наступних елементів:

1. Державні та міжнародні стандарти – це державні нормативно-правові акти та стандарти, що є обов’язковим при побудові СУІБП, та міжнародні стандарти, що несуть рекомендаційний характер.

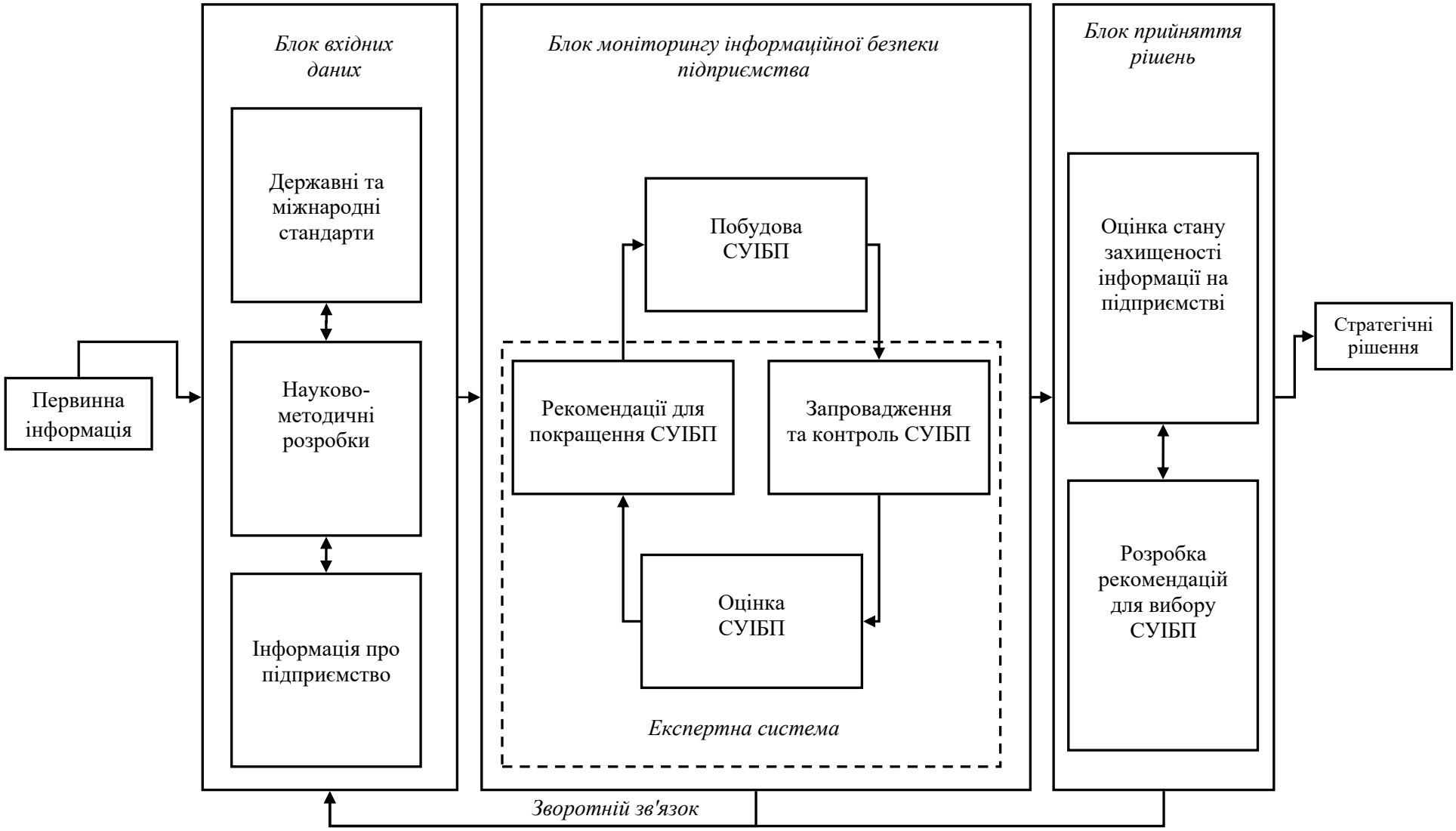


Рисунок 2.1 – Концептуальна модель системи управління інформаційною безпекою на підприємстві
*Джерело: [13, 34, 41 ]*

2. Науково-методичні розробки – включають в себе всю наукову літературу по даній темі та методики практичного застосування засобів інформаційної безпеки.

3. Інформація про підприємство зосереджує в собі:

– вимоги та побажання клієнта щодо побудови СУІБП, тобто: формування переліку інформації з обмеженим доступом, класифікація загроз інформаційної безпеки для конкретного підприємства;

– особливості діяльності та функціонування підприємства, а саме: форма власності, масштаб підприємства, його структура та функції підрозділів;

– зазначення рівня автоматизації захисту інформації на даному підприємстві.

Особливістю даного блоку є неповнота та невизначеність первинної інформації. Сформована інформація переходить до наступного блоку у вигляді задачі з кількісними та якісними показниками.

Наступний етап – моніторинг (моделювання) інформаційної безпеки підприємства, який представлений «процесною моделлю» СУІБП: побудова – запровадження та контроль – оцінка – вдосконалення. Під побудовою СУІБ розуміють застосування математичного апарату, розробку плану технічного захисту інформації (ТЗІ) та вибір програмного комплексу для реалізації побудованої СУІБП. Після реалізації розробленого плану ТЗІ та виконання основних організаційних заходів здійснюється керування роботою та ресурсами для СУІБ. Тому що організація та запровадження СУІБ на підприємстві є достатньо дорогою кампанією, виникає необхідність у постійному аналізі ефективності застосованої моделі СУІБ та оцінювання співвідношення «вартість-ефективність», тобто підсумковий фінансовий результат роботи моделі СУІБП. Із аналізу випливають висновки про зміну або покращення СУІБП. Особливість даного етапу – циклічність процесу моделювання, що пояснюється недосконалістю існуючих розробок по СУІБП, а нові розробки потребують багатої кількості експериментів для їх покращення та практичного застосування.

Саме «процесний підхід» підказує користувачам важливість [41]:

– розуміння вимог інформаційної безпеки підприємства та необхідності створення політики та цілей інформаційної безпеки;

– забезпечення і керування контролем та ризиками інформаційної безпеки в контексті усіх бізнес-ризиків підприємства;

– моніторингу і контролю за продуктивністю та ефективністю СКІБ;

– постійного вдосконалення, обґрунтованого переглядом цілей.

На рис. 2.1. цей етап визначений блоком моніторингу інформаційної безпеки підприємства.

Функціональне призначення цього блоку – розробити модель інформаційної безпеки підприємства через побудову нової або аналіз та удосконалення запровадженої СУІБП.

Цей блок складається з наступних елементів:

1. Побудова СУІБД включає:

– застосування математичного апарату – формування моделей загроз та моделей порушників;

– запровадження методів управління підприємством – розробка плану ТЗІ (технічний захист інформації), який складається з первинних технічних та організаційних заходів;

– вибір програмного комплексу для найкращої реалізації побудованої СУІБП.

2. Запровадження та контроль СУІБП – запровадження моделі через реалізацію розробленого плану ТЗІ, виконання основних технічних заходів, моніторинг безпеки при виконанні поставлених задач захисту інформації.

3. Оцінка СУІБП – використання системи показників, побудованої на основі вимог клієнта, для:

– аналізу стану інформаційної безпеки на даному підприємстві;

– оцінки ефективності застосованої моделі;

– розрахунку аналізу «вартість-ефективність», тобто економічної вигідності проекту СУІБП.

4. Рекомендації для покращення СУІБП – розробка висновків за результатами аналізу функціонування СУІБП та шляхів підвищення ефективності роботи побудованої моделі.

Особливості даного блоку:

1. Циклічність процесу моделювання, що пояснюється недосконалістю існуючих розробок по СУІБП, а нові розробки потребують багатої кількості експериментів для їх покращення та практичного застосування.

2. Останні три елементи блоку створюють експертну систему, що може обробляти вже існуючі та нові моделі інформаційної безпеки підприємства.

Стрімкий розвиток інформаційних технологій ставить перед спеціалістами з інформаційної безпеки новіші та складніші завдання. Це пояснює необхідність періодичного збору нової або перегляду існуючої інформації, що показано на схемі зворотнім зв’язком. Звернення до блоку вихідних даних може здійснюватися на будь-якому етапі моделювання інформаційної безпеки, так само, як і надходження до блоку моделювання оновленої інформації на потрібний етап.

Інформаційним потоком цього блоку буде виступати оцінка захищеності інформації на підприємстві та набір сценаріїв подальшого прийняття рішень.

Остаточною вихідною інформацією з блоку прийняття рішень будуть конкретні стратегічні рішення щодо вдосконалення, оновлення існуючої СУІБП або запровадження нових моделей та розробок у сфері інформаційної безпеки підприємства.

Завершальним етапом побудови СУІБП є прийняття стратегічних рішень у сфері інформаційної безпеки підприємства. Ці рішення ґрунтуються на оцінці стану захищеності інформації на підприємстві та розробці рекомендацій для вибору СУІБП: застосування існуючої, удосконалення існуючою або запровадження нової СУІБП.

На рис. 2.1. цей етап представлений блоком прийняття рішень.

Функціональним призначенням даного блоку є представлення результатів розгляду поставленої задачі, моделювання СУІБП та експертних висновків.

Цей блок складається з наступних елементів:

1. Оцінка стану захищеності інформації на підприємстві – аналіз стану інформаційної безпеки підприємства, який здійснюється через систему кількісних та якісних показників в процесі побудови СУІБП.

2. Розробка рекомендацій для вибору СУІБП – рекомендації для прийняття рішення: застосування існуючої, удосконалення існуючою або запровадження нової СУІБП, – з урахуванням порівнянності необхідності захисту інформації та платоспроможності підприємства.

Ці два елементи взаємопов’язані, бо прийняття рішення щодо запровадження та вибору СУІБП засновується на оцінці стану захищеності інформації на конкретному підприємстві.

Варіант спрацювання зворотного зв’язку з блоку прийняття рішень пояснюється застосуванням такого рішення, що включає перегляд або зміну вимог та побажань клієнта.

Таким чином моделювання інформаційної безпеки є складовим елементом поетапного формування та запровадження системи інформаційного менеджменту на підприємстві та представлено «процесною моделлю» СУІБП: побудова – запровадження та контроль – оцінка – вдосконалення.

## 2.2. Обґрунтування показника якості системи захисту інформації

Зловмисник за допомогою деякого джерела загроз генерує сукупність загроз ІС (нехай вона буде кінцевою та лічильною; $i = \overline{1,n}$). Кожна $i$-та загроза характеризується ймовірністю появи $P_{i погр}$ і збитком $\Delta q_i^{погр}$, що наноситься інформаційній системі.

Система захисту інформації виконує функцію повної або часткової компенсації загроз для ІС. Основною характеристикою СЗІ є ймовірності усунення кожної $i$-ої загрози [13].

За рахунок функціонування СЗІ забезпечується зменшення збитку $W$, що наноситься ІС під впливом загроз. Позначимо загальний відвернений збиток ІС через $\overline{W}$, а відвернений збиток за рахунок ліквідації впливу $i$-ої загрози через $\overline{\omega_i}$.

Після уведених позначень сформулюємо в загальному виді задачу синтезу системі захисту інформації в ІС: необхідно вибрати варіант реалізації СЗІ, що забезпечуватиме максимум відверненого збитку від впливу загроз при припустимих витратах на СЗІ.

Формальна постановка задачі має вигляд:

$$\text{знайти } \begin{matrix} T^0 = \arg\max \overline{W}(T) \\ T^0 \in T^+ \end{matrix} \qquad (2.1)$$

$$\text{при обмеженні } C(T^0) \le C_{доп} \qquad (2.2)$$

де $T$ – деякий вектор, що характеризує варіант технічної реалізації СЗІ; $T^+, T^0$ – припустиме і оптимальне значення вектора $T$; $C_{доп}$ – припустимі витрати на СЗІ.

Для рішення задачі необхідно, насамперед, сформувати показник якості функціонування СЗІ $\overline{W}(T)$.

Очевидно, відвернений збиток у загальному виді виражається співвідношенням:

$$\overline{W}(T) = F(P_{i\,погр}; \Delta q_i^{погр}; P_{i\,погр}^{усун}; i = \overline{1,n})$$

Відвернений збиток за рахунок ліквідації впливу $i$-ої загрози

$$\overline{\omega_i} = P_{i\text{погр}} \cdot \Delta q_i^{\text{погр}} \cdot P_{i\text{погр}}^{\text{усун}}; i = \overline{1,n}$$

За умови незалежності загроз та адитивності їх наслідків одержуємо

$$\overline{W} = \sum_{i=1}^{n} P_{i\text{погр}} \cdot \Delta q_i^{\text{погр}} \cdot P_{i\text{погр}}^{\text{усун}} \tag{2.3}$$

Зупинимося більш докладно на співмножниках, що входять у формулу (2.3).

Імовірність появи $i$-ої загрози визначається статистично і відповідає відносній частоті її появи

$$P_{i\text{погр}} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda_i}$$

де $\lambda_i$ – частота появи $i$-ої загрози.

Збиток, нанесений $i$-ою загрозою $\Delta q_i$, може визначатися в абсолютних одиницях: економічних втратах, тимчасових витратах, обсязі знищеної або «зіпсованої» інформації тощо.

Однак, практично це зробити досить важко, особливо на ранніх етапах проектування СЗІ. Тому доцільно замість абсолютного збитку використати відносний збиток, що по суті являє собою ступінь небезпеки $i$-ої загрози для інформаційної системи. Ступінь небезпеки може бути визначена експертним методом у припущенні, що всі загрози для ІС становлять повну групу подій, тобто $0 \le \Delta q_i \le 1; \sum_{i=1}^{n} \Delta q_i = 1$.

Найбільш складним питанням є визначення ймовірності усунення $i$-ої загрози $P_{i\text{погр}}^{\text{усун}}$ при проектуванні СЗІ. Зробимо природне допущення, що ця ймовірність визначається тим, наскільки повно враховані якісні та кількісні вимоги до СЗІ при їх проектуванні, тобто

$$P_{i\,погр}^{усун} = f_i(x_{i1},...,x_{ij},...,x_{im}) \qquad (2.4)$$

де $x_{i1}$ – ступінь виконання $j$-ої вимоги до СЗІ для усунення $i$-ої загрози, $i=\overline{1,n};\ j=\overline{1,m}$.

Нехай перші «$k$» вимог будуть кількісними ( $j=\overline{1,k}$), а інші «$m-k$» – якісними ( $j=\overline{k+1,m}$).

Ступінь виконання $j$-ої кількісної вимоги визначається її близькістю до необхідного (оптимального) значення. Для оцінки ступеня виконання $j$-ої кількісної вимоги до СЗІ зручніше за все використати його нормоване значення $\bar{x}_{ij}(j=\overline{1,k}), 0 \le x_{ij} \le 1$.

Для нормування зручно використати функцію виду

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij}^{нх}}{x_{ij}^{нл} - x_{ij}^{нх}} \qquad (2.5)$$

де $x_{ij}$ – поточне значення $j$-ої вимоги; $x_{ij}^{нл}, x_{ij}^{нх}$ – найкраще та найгірше значення.

З урахуванням формули (2.5) одержуємо наступні розрахункові співвідношення:

при $x_{ij}^{нл} = x_{ij\max};\ x_{ij}^{нх} = x_{ij\min}$ $\qquad \bar{x}_{ij} = \dfrac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}}$

при $x_{ij}^{нл} = x_{ij\min};\ x_{ij}^{нх} = x_{ij\max}$ $\qquad \bar{x}_{ij} = \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}}$

$$\bar{x}_{ij} = \begin{cases} 0 & при\ x_{ij} \ge x_{ij\min};\ x_{ij} \ge x_{ij\max} \\ 1 & при\quad x_{ij} = x_{ij\,opt} \\ \dfrac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}} & при\quad x_{ij\min} \le x_{ij} \le x_{ij\,opt} \\ \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}} & при\quad x_{ij\,opt} \le x_{ij} \le x_{ij\max} \end{cases}$$

Ступінь виконання $j$-ої якісної вимоги визначається функцією приналежності до найкращого значення $\mu(x_{ij})$ [13].

Розклавши функцію (2.4) у ряд Макларена обмежившись лише першими членами ряду, отримуємо

$$P_{i\,погр}^{усун} = P_{i\,погр}^{усун}(0) + \sum_{\gamma=1}^{m} \frac{\partial P_{i\,погр}^{усун}}{\partial x_{ij}} \cdot x_{ij} \tag{2.6}$$

де $P_{i\,погр}^{усун}(0) = 0$ – імовірність усунення $i$-ої загрози при невиконанні вимог СЗІ; $\frac{\partial P_{i\,погр}^{усун}}{\partial x_{ij}} = \alpha_{ij}$ – величина, що характеризує ступінь впливу вимоги на ймовірність усунення $i$-ої загрози (важливість виконання $j$-ої вимоги для усунення $i$-ої загрози). Очевидно, що $0 \le \alpha_{ij} \le 1; \sum_{j=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1,n}$.

Після підстановки в (2.6) відповідних значень отримуємо

$$P_{i\,погр}^{усун} = \sum_{j=1}^{k} \alpha_{ij} \cdot \bar{x}_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij})$$

Остаточно формула (2.3) для оцінки величини $\overline{W}$ відверненого збитку приймає вигляд

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \overline{\lambda}_i \cdot \Delta q_i \cdot \alpha_{ij} \cdot \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \overline{\lambda}_i \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu(x_{ij})$$

Таким чином, завдання синтезу СЗІ у вигляді (2.1), (2.2) зводиться до оптимального обґрунтування кількісних і якісних вимог до СЗІ при припустимих витрат і приймають вигляд:

знайти $\max \overline{W}(x_{ij}; i = \overline{1,n}; j = \overline{1,m})$ (2.7)

при обмеженні $C(x_{ij}) \le C_{доп}; i = \overline{1,n}; j = \overline{1,m}$

Відповідно до формулювання завдання (2.7) основними етапами її рішення є:

1. Збір і обробка експертної інформації про характеристики загроз: частота появи $i$-ої загрози та збиток $\Delta q_i (i = \overline{1,n})$.

2. Збір і обробка експертної інформації для визначення важливості виконання $j$-ої вимоги для усунення $i$-ої загрози $\alpha_{ij}$ та функції приналежності $\mu(x_{ij}), (i = \overline{1,n}; j = \overline{1,m})$.

3. Оцінка вартості СЗІ для конкретного варіанта її реалізації, що залежить від ступеня виконання вимог $C(x_{ij}; i = \overline{1,n}; j = \overline{1,m})$.

4. Розробка математичної моделі і алгоритму вибору раціонального варіанта побудови СЗІ (раціонального завдання вимог) відповідно до постановки (2.7) як задачі нечіткого математичного програмування.

## 2.3. Модель комплексної оцінки системи захисту інформації

Практичне завдання забезпечення інформаційної безпеки складається в розробці моделі подання системи (процесів) ІБ, що на основі науково-методичного апарата, дозволяла б вирішувати завдання створення, використання й оцінки ефективності СЗІ для проектованих й існуючих унікальних ІС.

Основним завданням моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанта технічної реалізації системи захисту інформації.

Специфічними особливостями рішення завдання створення систем захисту є:

– неповнота і невизначеність вихідної інформації про склад ІС і характерних загрозах;

– багатокритеріальність завдання, пов’язана з необхідністю обліку великої кількості приватних показників (вимог) СЗІ;

– наявність як кількісних, так й якісних показників, які необхідно враховувати при рішенні завдань розробки й впровадження СЗІ;

– неможливість застосування класичних методів оптимізації.

Для того, щоб охопити всі аспекти проблеми, розглянемо три «координати вимірів» – три складові групи моделі СЗІ [13]:

– із чого складається (Основи);

– для чого призначена (Напрямки);

– як працюють (Етапи).

Основами або складовими частинами практично будь-якої складної системи (у тому числі і системи захисту інформації) є:

1. Законодавча, нормативно-правова і наукова база ($O_1$).

2. Структура та завдання органів (підрозділів), що забезпечують безпеку ІТ ($O_2$).

3. Організаційно-технічні та режимні заходи і методи (політика інформаційної безпеки) ($O_3$).

4. Програмно-технічні способи і засоби ($O_4$).

У вигляді схеми основи інформаційної безпеки представлені на рис. 2.2.


Рисунок 2.2 – Основи інформаційної безпеки

*Джерело: [13]*

Напрямки формуються виходячи з конкретних особливостей ІС як об’єкта захисту. У загальному випадку, з огляду на типову структуру ІС та історично сформовані види робіт із захисту інформації, пропонується розглянути наступні напрямки:

1. Захист об’єктів інформаційних систем ($H_1$).
2. Захист процесів, процедур і програм обробки інформації ($H_2$).
3. Захист каналів зв’язку ($H_3$).
4. Приглушення побічних електромагнітних випромінювань ($H_4$).
5. Керування системою захисту ($H_5$).

Схематично напрямки інформаційної безпеки показані на рис. 2.3.

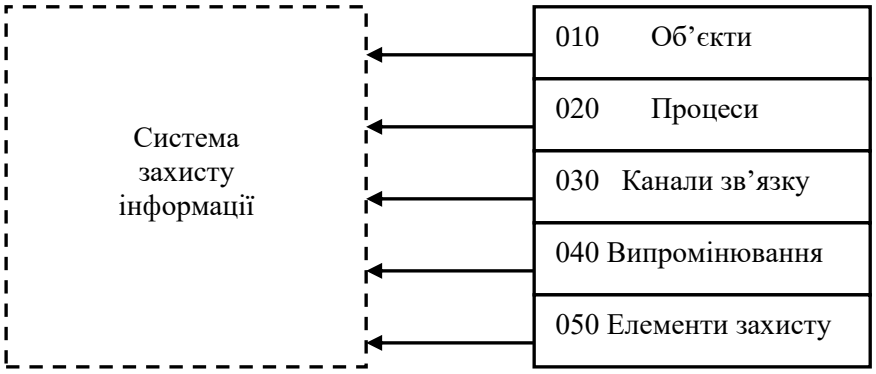


Рисунок 2.3 – Напрямки інформаційної безпеки

*Джерело: [13]*

Але, оскільки кожний із цих напрямків базується на перерахованих вище основах, то елементи основ і напрямків, розглядаються нерозривно один з одним. Наприклад, одну з основ за назвою «Законодавча база...» необхідно розглядати в усіх напрямках, а саме:

– «Законодавча база захисту об’єктів...» ;

– «Законодавча база захисту процесів, процедур і програм...» ;

– «Законодавча база захисту каналів зв’язку...» ;

– «Законодавча база придушення побічних електромагнітних випромінювань...» ;

– «Законодавча база по керуванню і контролю самої системи захисту...».

Для формування самого загального подання про конкретну систему захисту необхідно відповісти мінімум на 20 найпростіших запитань. Далі необхідно розглянути етапи (послідовність кроків) створення СЗІ, які необхідно реалізувати рівною мірою для кожного окремого напрямку з обліком зазначених вище основ.

Проведений аналіз існуючих методик (послідовностей) робіт зі створення СЗІ дозволяє виділити наступні етапи:

1. Визначення інформаційних і технічних ресурсів, а також об'єктів ІС підметів захисту ($M_1$).

2. Виявлення повної безліч потенційно можливих загроз і каналів витоку інформації ($M_2$).

3. Проведення оцінки уразливості і ризиків інформації (ресурсів ІС) при наявній безлічі загроз і каналів витоку ($M_3$).

4. Визначення вимог до системи захисту інформації ($M_4$).

5. Здійснення вибору засобів захисту інформації і їхніх характеристик ($M_5$).

6. Впровадження та організація використання обраних мір, способів і засобів захисту ($M_6$).

7. Здійснення контролю цілісності та керування системою захисту ($M_7$).

У вигляді схеми етапи інформаційної безпеки представлені на рис. 2.4.

Оскільки етапів сім, і по кожному треба освітити 20 уже відомих вам питань, то в цілому для формування подання про конкретну систему захисту необхідно відповісти на 140 простих питань. Зовсім очевидно, що по кожному питанню (елементу) виникне кілька десятків уточнень.

Структурно процес формування СЗІ з використанням матриці знань зображений на рис.2.5.

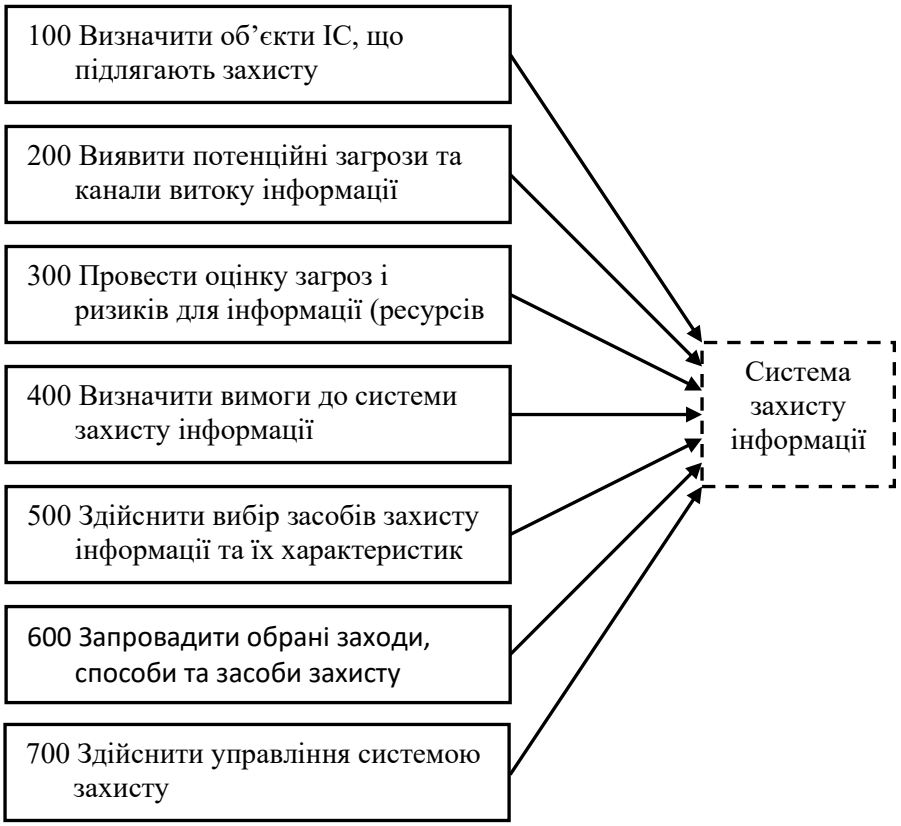


Рисунок 2.4 – Етапи створення СЗІ
*Джерело: [13]*

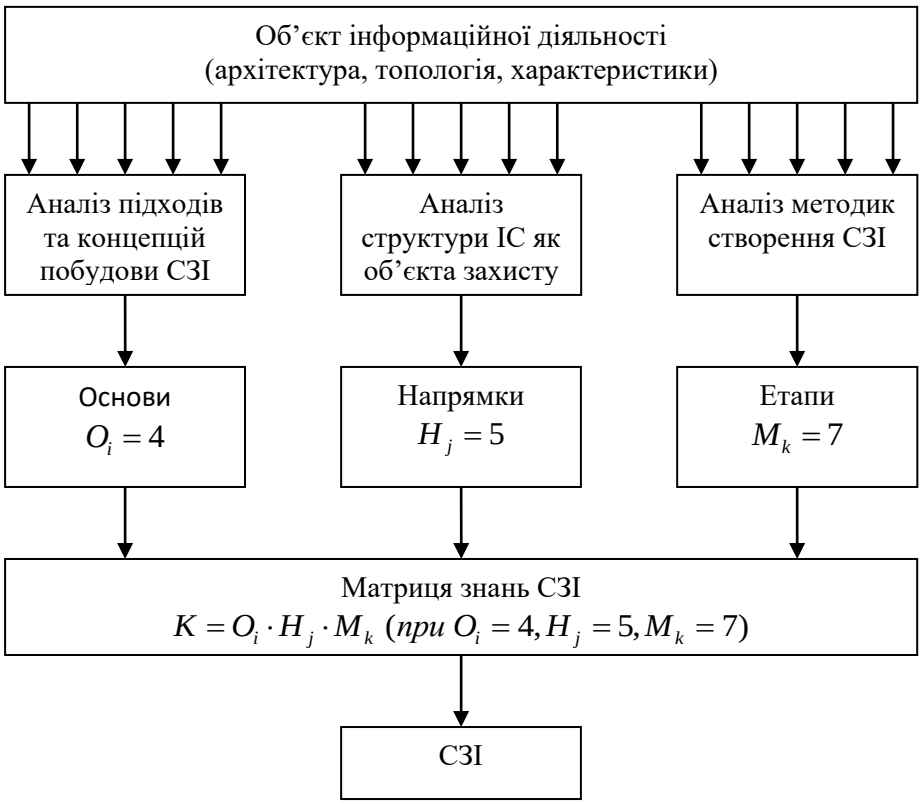


Рисунок 2.5 – Процес формування СЗІ з використанням матриці знань
*Джерело: [13]*

Елементи матриці мають відповідну нумерацію. Варто звернути увагу на позначення кожного з елементів матриці, де:

– перший знак (Х00) відповідає номерам складових блоку «етапи»,

– другий знак (0Х0) відповідає номерам складових блоку «напрямки»,

– третій знак (00Х) відповідає номерам складових блоку «основи».

Матриця знань (оцінок) дозволяє визначити ефективність заходів, що проводяться з захисту інформації. Матриця знань (оцінок) у вигляді таблиці показників представлена у табл. 2.1.

Приведемо приклад змісту інформації для елементів матриці № 321, 322, 323, 324, які поєднують наступні складові:

– № 3 (300 проведення оцінки уразливості й ризиків) блоку «етапи»,

– № 2 (020 захист процесів і програм) блоку «напрямки»

– № 1, 2, 3, 4 (001 нормативна база, 002 структура органів, 003 заходу, 004 використовувані засоби) блоку «основи».

Результати:

1. Елемент № 321 містить інформацію про те, наскільки повно відбиті в законодавчих, нормативних і методичних документах питання, що визначають порядок проведення оцінки уразливостей та ризиків для інформації, що використовується в процесах і програмах конкретної ІС?

2. Елемент № 322 містить інформацію про те, чи є структура органів (співробітників), відповідальна за проведення оцінки уразливостей та ризиків для процесів і програм ІС?

3. Елемент № 323 містить інформацію про те, чи визначені режимні заходи, що забезпечують своєчасне і якісне проведення оцінки уразливостей та ризиків для інформації, що використовується в процесах і програмах ІС?

4. Елемент № 324 містить інформацію про те, чи застосовуються технічні, програмні або інші засоби, для забезпечення оперативності і якості проведення оцінки уразливостей та ризиків у процесах і програмах ІС?

*Таблиця 2.1*

## Матриця знань (оцінок)

| Етапи | Напрямки | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Захист об’єктів ІС | | | | Захист процесів та програм | | | | Захист каналів зв’язку | | | | Захист випромінювань | | | | Управляння системою захисту | | | |
| | Основи | база | структура | заходи | Засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Визначення інформації, що підлягає захисту | 111 | 112 | 113 | 114 | 121 | 122 | 123 | 124 | 131 | 132 | 133 | 134 | 141 | 142 | 143 | 144 | 151 | 152 | 153 | 154 |
| 200 | Виявлення загроз та каналів витоку інформації | 211 | 212 | 213 | 214 | 221 | 222 | 223 | 224 | 231 | 232 | 233 | 234 | 241 | 242 | 243 | 244 | 251 | 252 | 253 | 254 |
| 300 | Проведення оцінки уразливостей та ризиків | 311 | 312 | 313 | 314 | 321 | 322 | 323 | 324 | 331 | 332 | 333 | 334 | 341 | 342 | 343 | 344 | 351 | 352 | 353 | 354 |
| 400 | Визначення вимог до СЗІ | 411 | 412 | 413 | 414 | 421 | 422 | 423 | 424 | 431 | 432 | 433 | 434 | 441 | 442 | 443 | 444 | 451 | 452 | 453 | 454 |
| 500 | Здійснення вибору засобів захисту | 511 | 512 | 513 | 514 | 521 | 522 | 523 | 524 | 531 | 532 | 533 | 534 | 541 | 542 | 543 | 544 | 551 | 552 | 553 | 554 |
| 600 | Запровадження обраних заходів та засобів | 611 | 612 | 613 | 614 | 621 | 622 | 623 | 624 | 631 | 632 | 633 | 634 | 641 | 642 | 643 | 644 | 651 | 652 | 653 | 654 |
| 700 | Контроль цілісності та управляння захистом | 711 | 712 | 713 | 714 | 721 | 722 | 723 | 724 | 731 | 732 | 733 | 734 | 741 | 742 | 743 | 744 | 751 | 752 | 753 | 754 |

У загальному випадку кількість елементів матриці може бути визначене зі співвідношення

$$K = O_i \cdot H_j \cdot M_k$$

де $K$ – кількість елементів матриці; $O_i$ – кількість складових блоку «основи»; $H_j$ – кількість складових блоку «напрямки»; $M_k$ – кількість складових блоку «етапи».

У нашому випадку загальна кількість елементів матриці дорівнює 140 $K = 4 \cdot 5 \cdot 7 = 140$, оскільки $O_i = 4$, $H_j = 5$, $M_k = 7$.

Якість СЗІ визначається ступенем (повнотою) виконання вимог, пропонованих до СЗІ. В основу оцінки якості СЗІ покладемо вихідні дані, представлені у вигляді матриці знань, заповнюваної експертами.

Заповнення матриці знань здійснюється на основі інтервальних оцінок окремих елементів.

Особливістю приватних показників є те, що вони мають якісний характер, тобто не мають точного кількісного виміру. Тому при оцінці того самого показника декількома експертами можуть виникати різні думки. Крім того, експерт не завжди здатний словесно оцінити приватний показник, хоча інтуїтивно відчуває його рівень. Для подолання цих труднощів можна оцінювати приватні показники за принципом термометра.

Оцінка приватних показників за принципом термометра дає можливість використати як показник оцінки СЗІ адитивний, що для кількісної оцінки якості СЗІ дозволяє визначити кількість виконаних приватних показників. У цьому випадку показник якості має вигляд

$$Q = \frac{\sum_{k=1}^{5} \sum_{j=1}^{4} \sum_{i=1}^{7} z_{kji}}{140}$$

де $z_{kji} = \begin{cases} 1, \text{якщо } q_{kji} \geq q_{kji}^T \\ 0, \text{якщо } q_{kji} \leq q_{kji}^T \end{cases}$, $q_{kji}$ *та* $q_{kji}^T$ – дійсне і задане значення приватних показників відповідно.

Оцінка якості СЗІ має вигляд $Q = \sum_{i=1}^{m} \omega_i q_i$.

Однак велика кількість елементів матриці знань ($m = 140$) може привести до втрати об'єктивності визначення вагових коефіцієнтів. Тому більше перспективним шляхом є завдання вагових коефіцієнтів стовпців, рядків і напрямків матриці знань

$$Q = \sum_{k=1}^{5} \omega_k \sum_{j=1}^{4} \omega_j \sum_{i=1}^{7} \omega_i q_{kji} \; ; \; \sum_{k=1}^{5} \omega_k = 1 \quad \sum_{j=1}^{4} \omega_j = 1 \quad \sum_{i=1}^{7} \omega_i = 1 .$$

Розглянемо можливі варіанти подання експертних знань і відповідні їм методики розрахунку показника якості СЗІ [34].

Варіант 1.

Ступінь виконання кожної вимоги визначається як:

– вимога виконана $X_i = 1$;

– вимога не виконана $X_j = 0, j = 1, m$.

Важливість виконуваних вимог не враховується.

Тоді якість СЗІ оцінюється співвідношенням:

$$W = \frac{\sum_{j=1}^{m} X_j}{m}; 0 \leq W \leq 1 . \qquad (2.8)$$

Варіант 2.

Ступінь виконання з урахуванням важливості вимог.

Важливість виконання кожної вимоги, обумовлене експертним шляхом, ураховується. Тоді якість СЗІ оцінюється співвідношенням:

$$W = \sum_{j=1}^{m} a_j x_j;\ 0 \le W \le 1;\ 0 \le a \le 1;\ \sum_{j=1}^{m} a_j = 1. \qquad (2.9)$$

Варіант 3.

Ступінь виконання вимог оцінюється по бальній шкалі.

Наприклад, у найпоширенішій п’ятибальній шкалі:

1. $B_j = 5$ – відмінно.

2. $B_j = 4$ – добре.

3. $B_j = 3$ – задовільно.

4. $B_j = 2$ – не задовільно.

5. $B_j = 1$ – досить не задовільно.

З погляду ступеня задоволення вимог бальну оцінку можна інтерпретувати в такий спосіб:

– відмінно – СЗІ повністю задовольняє вимогам;

– добре – майже задовольняє;

– задовільно – задовольняє в основному;

– не задовільно – не задовольняє;

– досить не задовільно – повністю не задовольняє.

Якість СЗІ оцінюється середнім балом.

$$\overline{B} = \frac{\sum_{j=1}^{m} b_j}{m};\quad 1 \le \overline{B} \le 5,\ j = 1, \overline{m} \qquad (2.10)$$

Варіант 4.

Ступінь виконання вимог оцінюється по бальній шкалі, додатково визначається важливість кожної вимоги.

Тоді якість СЗІ визначається з вираження:

$$\overline{B} = \sum_{j=1}^{m} a_j b_j;\quad 1 \le \overline{B} \le 5;\quad 0 \le a \le 1;\quad \sum_{j=1}^{m} a_j = 1. \qquad (2.11)$$

Дуже часто при бальній оцінці ступеня виконання вимог зручно підсумкову оцінку мати в шкалі від 0 до 1.

Тоді треба сформувати шкалу відповідності. Зразок такої шкали наведений у табл. 2.2. [53].

*Таблиця 2.2*

**Шкала відповідності**

| Бальна оцінка | Лінгвістична оцінка | Інтервальна оцінка |
|---|---|---|
| 5 – відмінно | Повністю задовольняє | 0,9 – 1 |
| 4 – добре | Майже задовольняє | 0,7 – 0,9 |
| 3 – задовільно | Задовольняє в основному | 0,5 – 0,7 |
| 2 – не задовільно | Не задовольняє | 0,3 – 0,5 |
| 1 – досить не задовільно | Повністю не задовольняє | 0 – 0,3 |

Оцінка якості СЗІ проводиться по формулах аналогічним (2.10) і (2.11).

$$Q = \frac{\sum_{j=1}^{m} q_j}{m}; \tag{2.12}$$

$$Q = \sum_{j=1}^{m} a_j q_j . \tag{2.13}$$

Якщо лінгвістична змінна «Якість СЗІ» визначена на універсальній множині варіантів СЗІ $u_i; i = \overline{1,n}$, то використовуючи функції приналежності за допомогою табл. 2.2, можна одержати оцінку якості СЗІ:

$$B_i = \frac{\sum_{j=1}^{m} B_{ij}}{m} = \frac{\sum_{j=1}^{m}\sum_{b_j=1}^{5} b_j \mu(u_i b_j)}{m} \tag{2.14}$$

$$B_i = \sum_{j=1}^{m} \alpha_j \sum_{b_j=1}^{5} b_j \mu(u_i b_j). \quad (2.15)$$

На основі отриманих за наведеними формулами оцінок можна зробити аналіз якості СЗІ.

## 2.4. Висновки до розділу 2

Оцінки параметрів СЗІ в умовах високої невизначеності умов її функціонування повинні обчислюватися з використанням не однієї математичної моделі, а погодженого сімейства моделей, що адаптивно конструюватиме одна з іншою таким чином, щоб безупинно вдосконалюватися на основі оптимального вибору даних.

Під ефективністю систем захисту інформації розуміється ефективність її використання в якості активного засобу в операції забезпечення конфіденційності обробки, зберігання і передачі інформації.

Оцінка ефективності операції полягає у виробленні оцінного судження щодо придатності заданого способу дій фахівців із захисту інформації або пристосованості засобів захисту до рішення завдань.

Теоретичні основи побудови оптимальних систем захисту винятково складні і, незважаючи на інтенсивність досліджень у цій предметній області, ще далекі від досконалості.

Оптимальним уважається те рішення, яке у запропонованих обставинах найкраще задовольнить умовам розглянутого завдання. Оптимальність рішення досягається за рахунок найбільш раціонального розподілу ресурсів, затрачуваних на рішення проблеми захисту.

СЗІ, з одного боку, є складовою частиною інформаційної системи, а з іншого боку – представляє собою складну технічну систему. Рішення завдань аналізу та синтезу СЗІ ускладнюється завдяки її особливостям, основними з яких є:

– складний опосередкований взаємозв’язок показників якості СЗІ з показниками якості інформаційної системи;

– необхідність обліку великої кількості показників (вимог) СЗИ при оцінці і виборі їхнього раціонального варіанта;

– переважно якісний характер показників (вимог), що враховують при аналізі та синтезі СЗІ;

– істотний взаємозв’язок цих показників (вимог).ю що мають суперечливий характер.

– труднощі одержання вхідних даних, необхідних для рішення завдань аналізу та синтезу СЗІ, особливо на ранніх етапах їхнього проектування.

Зазначені особливості роблять практично неможливим застосування традиційних математичних методів, у тому числі методів математичної статистики і теорії ймовірностей, а також класичних методів оптимізації для рішення прикладних завдань аналізу та синтезу СЗІ.

Складність процесу прийняття рішень, відсутність математичного апарата приводять до того, що при оцінці та виборі необхідно використовувати і обробляти якісну експертну інформацію.

Перспективним напрямком розробки методів прийняття рішень при експертній вхідній інформації є лінгвістичний підхід на базі теорії нечітких множин та лінгвістичної змінної.

# РОЗДІЛ 3
# РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

## 3.1. Аналіз стану інформаційної безпеки ТОВ «Южмаш груп»

ТОВ «Южмаш груп» має у своєму розпорядженні потужні галузеві виробництва, серед яких металургійне, складальне, випробувальне, зварювальне, ливарне, ковальське та механообробне. На підприємстві освоєно та впроваджено унікальні технологічні рішення.

Багатопрофільність ТОВ «Южмаш груп» дозволяє виготовляти продукцію для таких напрямів діяльності, як: оборонна промисловість; авіаційний транспорт; сільськогосподарське машинобудування; теплові електростанції.

ТОВ «Южмаш груп» має великі переваги перед іншими підприємствами: потужний виробничий потенціал підприємства багатопрофільного характеру; унікальні і сучасні технології; наявність кваліфікованого персоналу за основними напрямами виробництва.

Впроваджуючи політику удосконалення та інновацій, підприємство продовжує створювати нові технології та поширює номенклатуру продукції, що випускається.

Обстеження питання захисту інформації на підприємстві проводилося шляхом співбесід зі спеціалістами:

– відділу автоматизованих систем управління виробництвом;

– аналітичних підрозділів дирекції з маркетингу та зовнішньоекономічної діяльності;

– по фінансово-економічним питанням;

– по кадрам та соціальним питанням;

– по технічним питанням;

– відділу економічної безпеки.

Підрозділ, до функцій якого входить вирішення інформаційної безпеки, відсутній. Фактично функції інформаційної безпеки виконують керівники перелічених підрозділів та системні адміністратори.

За результатами проведеного обстеження у відповідності до ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97, міжнародного стандарту ISO/IEC 27001:2005 зроблено загальний аналіз стану інформаційної безпеки:

1. Відсутність процедур незалежного аудита ІТ.

Недоліки:

неотримання кваліфікованих рекомендацій, відсутність упевненості у відповідності кращим світовим практикам, відсутність плану коригувальних дій.

2. Устаткування:

– прийняті заходи щодо забезпечення безперервності електропостачання недостатні і малоефективні;

– резервні копії даних зберігаються на тім же диску, що й основні;

– резервні сервери розміщаються в тих же приміщеннях, що й основні;

– багато місць концентрації ключового встаткування не забезпечуються резервним електроживленням і слабко захищені фізично;

– відсутні резервні процедури роботи ключових користувачів.

Недоліки:

ризик прямих і непрямих фінансових втрат при настанні форс-мажорних або позаштатних обставин.

3. Недостатнє усвідомлення персоналом ризиків і небезпек пов’язаних з поширенням комп’ютерних вірусів.

Недоліки:

ризик зараження комп’ютерним вірусом, поширення вірусів у мережі, групи і завдання збитків у формі:

– руйнування даних та систем;

– затрат часу кваліфікованого персоналу на віднавлення систем та усунення наслідків вірусної активності;

– розкриття конфіденційної інформації;

– судового розгляду, тому що розповсюдження комп'ютерних вірусів є карним злочином згідно ч.1 ст. 361 Кримінального кодексу України.

4. Відсутність контролю адекватності витрат на ІТ.

Недоліки:

надлишкові, або недостатні витрати на розвиток та підтримку ІТ.

5. Відсутність процедур одержання незалежного підтвердження.

Ризик, недоліки:

відсутність впевненості групи партнерів та інвесторів в тім, що рівень ефективності і безпеки використання інформаційних технологій перебуває на досить високому рівні.

6. Відсутність процедур оцінки адекватності внутрішніх контролів в області ІТ.

Недоліки:

невідповідність процесів ІТ внутрішнім і зовнішнім вимогам може привести до зниження продуктивності процесів, посиленню ризиків безпеки і судовому переслідуванню.

7. Відсутні затверджені регулярні процедури і програми навчання користувачів, тренінги по загальної інформованості та основах безпеки не проводяться.

Недоліки:

7.1. Низька ефективність використання ІТ.

7.2. Компрометація конфіденційних даних через низький рівень усвідомлення питань безпеки.

7.3. Втрата, або перекручування важливих даних через низький рівень кваліфікації.

7.4. Неефективність запровадження стандартів підприємства та політик через недостатнє інформування та розуміння важливості положень політик та стандартів.

7.5. Рівень виконання вимог стандартів та політик знижується, якщо тренінги не проводяться регулярно.

7.6. Надання доступу до інформаційних ресурсів групам ненавчених та погано проінформованих співробітниками є істотним ризиком.

7.7. Неоптимальний перелік задач, що вирішуються службою технічної підтримки.

8. Перевантаження устаткування:

– керування продуктивністю встаткування й каналів передачі даних виконується на реактивній основі;

– у ході виконання найбільш ресурсномістких обчислювальних операцій одним з користувачів, інші випробовують недолік продуктивності;

– відсутній план і процедури, що попереджають, забезпечення достатньої продуктивності;

– факти неприступності послуг, додатків і даних через перевантаження не реєструються й статистика не аналізується.

Недоліки:

8.1. Неприступність послуг, додатків і даних, викликаних перевантаженням приводять до:

– недостатньо ефективному використанню робочого часу;

– збільшенню часу обробки даних;

– збільшенню часу на прийняття управлінських рішень.

8.2. Перевантаження, що виникають у ході обробки даних можуть привести до серйозних системних збоїв манливим за собою втрату, або руйнування важливих даних.

9. Відсутність процедур моніторингу процесів ІТ.

Недоліки:

ризик стагнації, або незбалансованого розвитку процесів; відсутність вхідних даних для вироблення тактичних планів в області ІТ.

10. Відсутність формальних вимог по забезпеченню належних фізичних умов експлуатації обчислювальної техніки та мережного встаткування.

Недоліки:

– ризик компрометації конфіденційних даних, одержання несанкціонованого доступу до встаткування й мережних ресурсів;

– скорочення терміну служби встаткування;

– зниження надійності функціонування встаткування.

11. Відсутність формальних вимог до сховищ даних.

Недоліки:

– невиконання загальноприйнятих вимог до сховищ даних може привести до їхньої втрати через пожежу, повені, крадіжки і т.п.;

– невиконання умов експлуатації встаткування може привести зі збоям і аваріям устаткування.

12. Обслуговування користувачів:

– невизначеність у строках та якості відпрацьовування запитів користувачів;

– відсутність формально прийнятого рівня обслуговування користувачів;

– відсутність класифікації й обліку запитів користувачів й аналізу накопиченої статистики по запитах.

Недоліки:

– через відсутність регламенту служби технічної підтримки важко здійснювати контроль над роботою служби з боку керівництва;

– недостатній рівень обслуговування користувачів веде до:

– затримок у виконанні користувачами своїх обов’язків, втраті робочого часу.

– компрометації конфіденційної інформації.

13. Відсутня політика безпеки підприємства – документ, який би визначав концепцію забезпечення конфіденційності, цілісності й доступності інформації.

Недоліки:

при розробці специфічних політик, положень, стандартів підприємства в області IT і телекомунікацій, вимоги безпеки не враховуються в належному ступені.

14. Резервне копіювання даних виконується на той же диск, на якому перебувають основні копії, резервні сервери перебувають у тих же приміщеннях, що й основні.

Недоліки:

ризик втрати важливих даних у випадку виходу з ладу серверів, дискових накопичувачів, або в результаті пожежі, повені тощо.

15. Відсутність процедур керування знімними носіями даних (DVD-RW, ZIP, flash-memory).

Недоліки:

втрата або «зникнення» знімних носіїв може спричинити втрату конфіденційності секретних даних.

16. Відсутність багатьох важливих специфічних політик (правил) в області IT.

Недоліки:

відсутність регламенту для специфічних процесів IT може стати причиною слабкого розвитку цих процесів і реалізації пов’язаних із цим ризиків.

17. Відсутність процедур перевірки відомостей резюме/ рекомендацій кандидатів при прийомі на роботу.

Недоліки:

прийом на роботу на підставі неправдивих відомість у резюме приводить до ризику надання доступу до конфіденційних і ключових ресурсів осіб.

18. Всі канали передачі даних експлуатуються без застосування шифрування, тому вся фінансова інформація, електронна пошта, банківські виписки, пересилання відновлень 1С, реплікації БД передаються по незахищених каналах передачі даних.

Недоліки:

експлуатація незахищених каналів передачі даних для передачі конфіденційної й важливої інформації може привести до:

– перекручуванні / модифікації даних, які передаються по незахищеним каналам передачі даних;

– несанкціонований доступ до переданих даних може стати приводом до судового розгляду.

19. Відсутність процедур оцінки кваліфікації співробітників.

Недоліки:

недостатня кваліфікація персоналу може привести до ризиків втрати робочого часу на самоосвіту й неналежне виконання посадових обов'язків.

20. Відсутність формалізованих і документованих процедур керування інцидентами і проблемами.

Недоліки:

– неоптимальний час усунення проблем можуть привести до істотних простоїв каналів, устаткування та бізнес-додатків, втратам робочого часу, затримкам в одержанні оперативної інформації;

– відсутність аналізу причин, а також оповіщення про проблеми, може привести до повторення інцидентів і збільшенню втрат.

21. Відсутність формального процесу оцінки ризиків при плануванні й проектуванні в області IT, має місце лише неявний і неформальний підхід, а оцінка ризиків виконується від проекту до проекту.

Недоліки:

реалізація ризиків у вигляді інцидентів і проблем.

22. Керування доступом:

– відсутність формальних процедур керування доступом;

– слабкі процедури контролю за правами доступу користувачів (численні випадки надання надлишкових прав, прав адміністратора співробітникам);

– відсутність політики «чистого екрана».

Недоліки:

22.1. Слабке або неадекватне керування правами доступу та привілеями можуть привести до одержання несанкціонованого доступу до конфіденційної інформації й до важливих інформаційних ресурсів.

22.2. Інформація може бути скопійована з особами, перекручена, або (ненавмисно або навмисно) знищена.

22.3. Несанкціонований доступ до додатків і систем може привести до їхньої некоректної роботи, збоям або відмовам.

22.4. Через незаблокований термінал можливе одержання несанкціонованого доступу з рівнем, яким володіє санкціонований користувач.

23. Багато важливих політик є неформальними вимогами, існуючі політики недостатньо ефективно доводять до персоналу, відповідального за їхнє дотримання.

Недоліки:

недостатнє усвідомлення персоналом цілей керівництва, виражених у політиках і правилах створює умови для недотримання політик.

24. Економічно ефективні контролі безпеки не враховуються при проектуванні автоматизованих рішень.

Недоліки:

ризик збільшення витрат на забезпечення безпеки в ході експлуатації рішення.

25. Недостатньо ефективний поділ обов’язків.

Недоліки:

зниження ефективності внутрішнього контролю.

26. Планово-попереджувальне обслуговування апаратного забезпечення не виконується, замість цього обслуговування виконується як реакція на інцидент.

Недоліки:

ризик передчасного виходу з ладу встаткування.

27. Взаємини з постачальниками встаткування і послуг не враховують питання безпеки.

Недоліки:

ризик розкриття конфіденційної інформації, прямі та непрямі втрати в результаті простоїв важливих комунікаційних каналів.

28. Відсутня класифікація інформаційних ресурсів підприємства, положення про комерційну таємницю (як документ про конфіденційність) не включає в перелік конфіденційної інформації логіни/ паролі доступу до додатків і систем, зміст ключових дискет систем клієнт-банк тощо.

Недоліки:

ризик розкриття конфіденційної інформації через відсутність класифікації, неможливо забезпечити адекватні та економічно ефективні заходи захисту конфіденційності й цілісності некласифікованої інформації.

29. Відсутня політика у відношення провайдерів послуг.

Недоліки:

– ризик одержання послуг неналежної якості;

– прямі та непрямі фінансові втрати в результаті простоїв, перевантажень;

– ризик втрати цілісності і погодженості в базах даних через низьку якість телекомунікаційних послуг.

Аналіз та забезпечення інформаційної безпеки підприємства проводиться за схемою, наведеною на рис. 3.1.

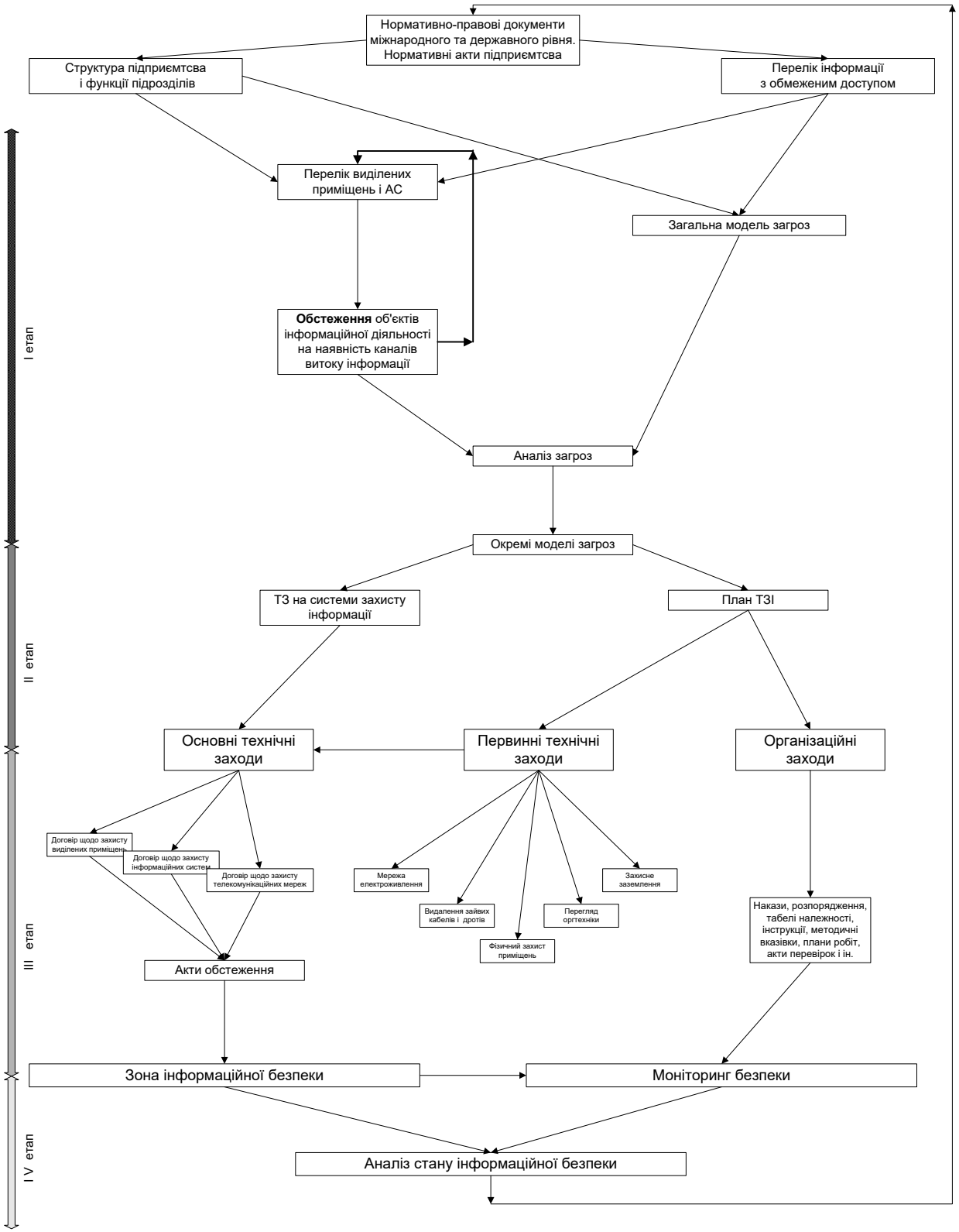


Рисунок 3.1 – Схема аналізу та забезпечення інформаційної безпеки на підприємстві

*Джерело: [13]*

Спираючись на проведене обстеження, віднесемо ТОВ «Южмаш груп» до відповідного рівня зрілості компанії з погляду забезпечення інформаційної безпеки. Американська компанія Gartner Group виділяє 4 рівні:

0 рівень:

0.1. ІБ в компанії ніхто не займається, керівництво компанії не усвідомлює важливості проблем ІБ.

0.2. Фінансування відсутнє.

0.3. ІБ реалізується штатними засобами операційних систем, СУБД і додатків (парольний захист, розмежування доступу до ресурсів і сервісів).

1 рівень:

1.1. ІБ розглядається керівництвом як чисто «технічна» проблема, відсутня єдина програма (концепція, політика) розвитку системи забезпечення інформаційної безпеки (СЗІБ) компанії.

1.2. Фінансування ведеться в рамках загального IT-бюджету.

1.3. ІБ реалізується засобами нульового рівня та засоби резервного копіювання, антивірусні засоби, міжмережеві екрани, засоби організації VPN (традиційні засоби захисту).

2 рівень:

2.1. ІБ розглядається керівництвом як комплекс організаційних і технічних заходів, існує розуміння важливості ІБ для виробничих процесів, є затверджена керівництвом програма розвитку системи захисту інформаційної безпеки компанії.

2.2. Фінансування ведеться в рамках окремого бюджету.

2.3. ІБ реалізується засобами першого рівня та засоби посиленої аутентифікації, засоби аналізу поштових повідомлень і web-контента, IDS (системи виявлення вторгнень), засоби аналізу захищеності, SSO (засоби одноразової аутентифікації), PKI (інфраструктура відкритих ключів) і організаційні заходи (внутрішній і зовнішній аудит, аналіз ризику, політика інформаційної безпеки, положення, процедури, регламенти і керівництво).

3 рівень:

3.1. ІБ є частиною корпоративної культури, призначений CISA (старший офіцер з питань забезпечення ІБ).

3.2. Фінансування ведеться в рамках окремого бюджету.

3.3. ІБ реалізується засобами другого рівня та системи управління ІБ, CSIRT (група реагування на інциденти порушення ІБ), SLA (угода про рівень сервісу).

У відповідності до даної класифікації ТОВ «Южмаш груп» по окремим напрямкам на 0 рівні, а по окремим – на 1 рівні, тобто на перехідному етапі.

Отже, стратегічним рішенням для підприємства є формування кінцевої мети в області інформаційної безпеки для підприємства – досягнення рівня зрілості СУІБП, що буде відповідати 3 рівню класифікації компанії Gartner Group та міжнародному стандарту ISO/IEC 27001:2005.

## 3.2. Моніторинг якості системи захисту інформації

Якість СЗІ визначається ступенем (повнотою) виконання вимог до СЗІ. Вихідні дані, представлені у вигляді приватних матриць знань, заповнених експертами по відповідних напрямках захисту.

Під профілем безпеки будемо розуміти графічне подання ступеня виконання вимог у системі координат:

по горизонталі – перелік вимог, пропонованих до СЗІ;

по вертикалі – ступінь виконання кожної вимоги.

Ступінь виконання кожної вимоги розраховується відповідно до формул (2.8) … (2.15).

Припустимо, що ступінь виконання вимог задається в шкалі $0 \le Q \le 1;\ J = 1, m$.

При цьому доцільно розглядати два профілі безпеки: необхідний і реально досягнутий.

Для побудови необхідного профілю безпеки використаються попередньо задані експертами значення $0 \le Q_j^{TP} \le 1;\ j = 1, m$.

Вхідні дані для побудови необхідного профілю безпеки представлені у вигляді матриці знань у додатку А.

В таблиці 3.1. представлені дані для оцінки захищеності об'єктів ІС (по першому напрямку захисту).

*Таблиця 3.1*

**Дані для оцінки СЗІ по напрямку «Захист об'єктів ІС»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,7 | 0,35 | 0 | 0,615 | 0,65 | 0,21 |
| | 2 | 112 | 0,2 | 0,8 | 0,5 | 0,1 | 0 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,5 | 0,075 | 0 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| 2 | 5 | 211 | 0,5 | 0,8 | 0,5 | 0,25 | 0 | 0,5 | | |
| | 6 | 212 | 0,3 | 0,8 | 0,5 | 0,15 | 0 | | | |
| | 7 | 213 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |
| | 8 | 214 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |
| 3 | 9 | 311 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | 0,66 | | |
| | 10 | 312 | 0,4 | 0,8 | 0,6 | 0,24 | 0 | | | |
| | 11 | 313 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 12 | 314 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,72 | | |
| | 14 | 412 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 15 | 413 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 16 | 414 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| 5 | 17 | 511 | 0,35 | 0,8 | 0,7 | 0,245 | 0 | 0,71 | | |
| | 18 | 512 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| 6 | 21 | 611 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | 0,71 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 23 | 613 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 24 | 614 | 0,2 | 0,8 | 0,5 | 0,1 | 0 | | | |
| 7 | 25 | 711 | 0,45 | 0,8 | 0,6 | 0,27 | 0 | 0,65 | | |
| | 26 | 712 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 27 | 713 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |
| | 28 | 714 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |

Пояснимо використовувані позначення:

1. Номер етапу з 1 по 7.

2. Перелік показників ($m$) для відповідних елементів (від 1 до 28).

3. Коефіцієнти важливості ($a_j$), які визначаються для показників кожного з етапів.

4. Показники необхідного профілю безпеки ($Q_{mp}$). Для всіх показників установлене значення 0,8.

5. Показники досягнутого профілю безпеки ($Q_д$). Їхні значення визначені експертами.

6. Показники досягнутого профілю безпеки з урахуванням коефіцієнтів важливості ($Q_{да_j}$).

7. Порівняння профілів ($S_{пр}$), яке робиться в такий спосіб:

($S_{пр}$) = 1 – якщо значення показника досягнутого профілю безпеки дорівнює або перевищує значення показника заданого;

($S_{пр}$) = 0 – якщо значення показника досягнутого профілю безпеки нижче значення показника заданого.

Порівняння профілів захисту об’єктів ІС можна побачити на графіку, який показано на рис. 3.2.

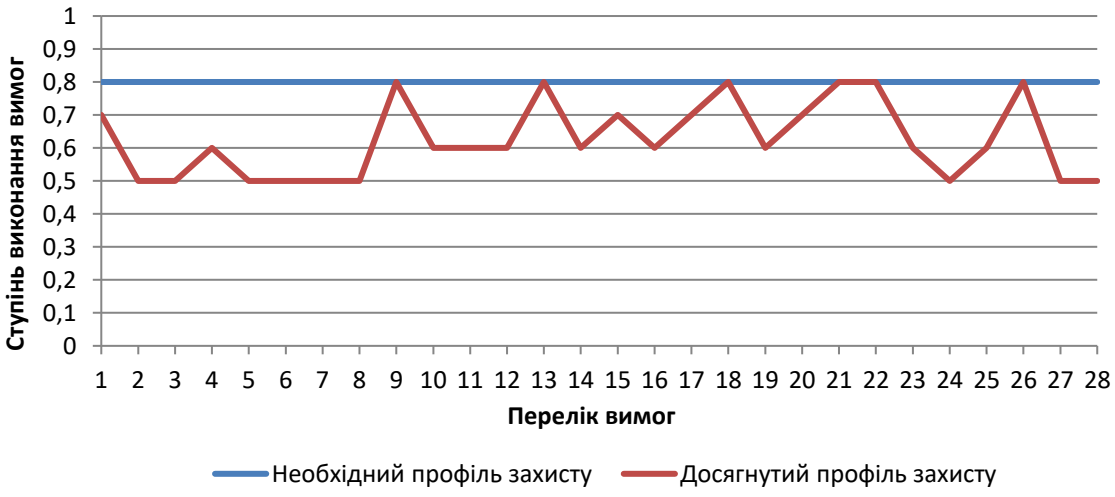


Рисунок 3.2 – Порівняння профілів захисту об’єктів ІС

Ступінь виконання груп вимог ($Q_{групп}$) визначається з урахуванням коефіцієнтів важливості ($Q_{да_j}$) для кожного з етапів: 1 – 0,615; 2 – 0,5; 3 – 0,66; 4 – 0,72; 5 – 0,71; 6 – 0,71; 7 – 0,65. Графічно ці значення зображені на діаграмі на рис. 3.3.

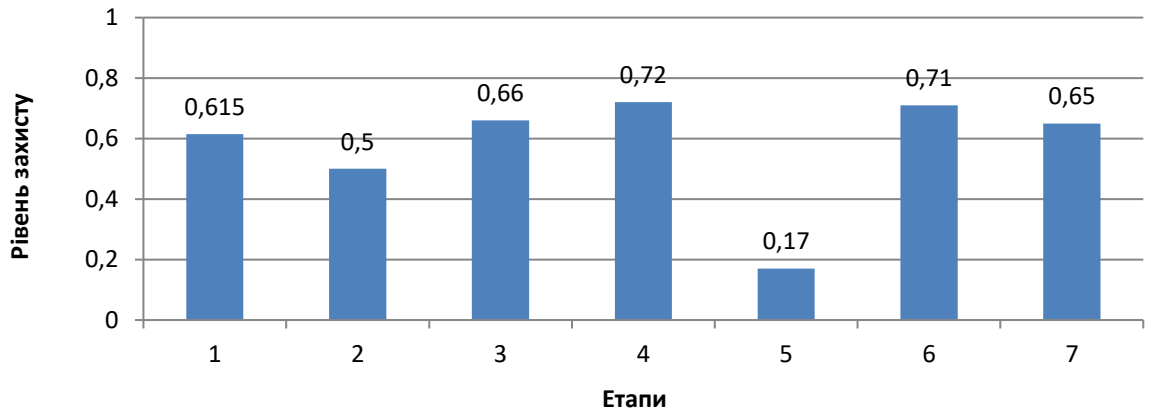


Рисунок 3.3 – Оцінка етапів захисту об’єктів ІС

Якісна оцінка ($Q$) визначається виходячи зі значень показників ($Q_{групп}$), що розраховані для відповідних етапів. У нашому випадку $Q = 0{,}65$.

Кількісна оцінка ($S$) визначається шляхом підрахунку значень ($S_{пр}$), а саме нулів та одиниць, отриманих при порівнянні профілів. Це більш груба оцінка, що визначає кількість виконаних (досягнутих) вимог $S = 0{,}21$.

Іншими словами в розглянутій інформаційній системі виконано 21% вимог по захисту об’єктів ІС. Однак, не відомо наскільки ці вимоги важливі.

Аналогічно розраховуємо ті самі показники для інших чотирьох напрямків інформаційної безпеки. Розрахункові та графічні результати наведені у додатках Б, В, Г і Д.

Далі, об’єднавши часткові показники (по напрямках) в узагальнений показник, одержуємо результуючий профіль безпеки $Q_{СЗІ}$ (таблиця 3.2) і його графічне зображення (рис. 3.4).

*Таблиця 3.2*

**Табличне подання узагальнених кількісних оцінок ступеню виконання вимог**

| | Напрямки захисту | | | | | $Q_{СЗІ}$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 0 | 1 | 1 | 0 | 0 | 0,4 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 5 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 6 | 0 | 0 | 0 | 0 | 1 | 0,2 |
| 7 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 8 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 9 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 10 | 0 | 0 | 0 | 0 | 1 | 0,2 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 1 | 1 | 0 | 0 | 0,4 |
| 13 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 14 | 0 | 1 | 0 | 0 | 0 | 0,2 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 1 | 1 | 1 | 0 | 0 | 0,6 |
| 19 | 0 | 0 | 0 | 0 | 1 | 0,2 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 22 | 1 | 0 | 0 | 0 | 0 | 0,2 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 |
| 28 | 0 | 0 | 0 | 0 | 0 | 0 |

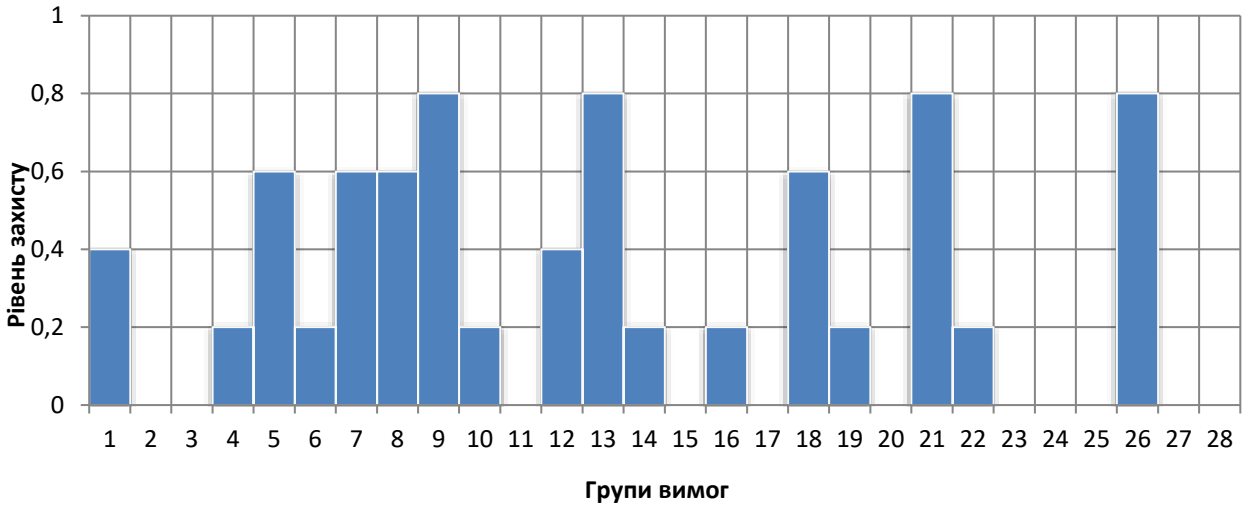


Рисунок 3.4 – Графічне зображення узагальнених кількісних оцінок ступеню виконання вимог

Зверніть увагу на те, що вимоги 2, 3, 11, 15, 17, 20, 23, 24, 25, 27 та 28 не виконані взагалі в усіх напрямках. Визначити які групи вимог по яких напрямках виконані, можна за допомогою діаграми, зображеної на рис. 3.5.

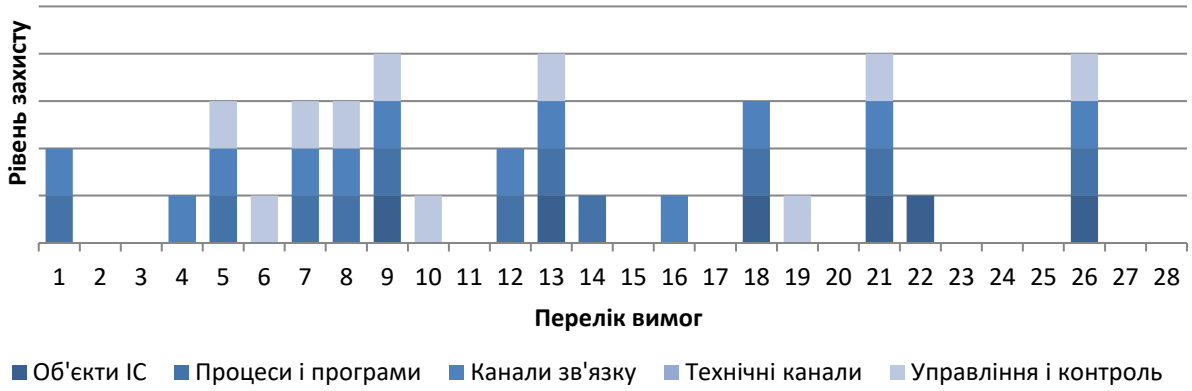


Рисунок 3.5 – Графічне зображення узагальнених кількісних оцінок ступеню виконання за окремими вимогами

Узагальнені показники рівня захищеності (якісний і кількісний) представлені в таблиці 3.3.

*Таблиця 3.*3

**Узагальнені показники рівня захищеності ІС**

| Показники | Напрямки захисту | | | | | $Q_{СЗІ}$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| | Коефіцієнти важливості по напрямкам | | | | | |
| | 0,3 | 0,1 | 0,2 | 0,1 | 0,3 | |
| Кількісний | 0,21 | 0,34 | 0,43 | 0 | 0,36 | 0,23 |
| Якісний | 0,65 | 0,73 | 0,72 | 0,23 | 0,67 | 0,64 |

Перевищення величини якісного показника над кількісним, свідчить про те, що виконані вимоги більше важливі за своїм значенням, чим невиконані.

## 3.3. Моделювання стану інформаційної безпеки

Вважаючи результати проведеної діагностики інформаційної безпеки на підприємстві, розглянутими у попередньому підрозділі, незадовільними, можна запропонувати наступні рекомендації для запровадження нових та вдосконалення існуючих методів і заходів забезпечення захисту інформації на ТОВ «Южмаш груп»:

1. Розробити корпоративну політику у відношення операторів зв’язку, провайдерів Інтернет та операторів передачі даних.

2. Розробити процедури тестування кваліфікації нового та підтвердження кваліфікації наявного персоналу.

3. Організувати періодичний незалежний аудит інформаційної системи.

4. Організувати періодичне незалежне підтвердження (сертифікація):

– відповідність законам та іншим зовнішнім вимогам;

– відповідність політикам та стандартам підприємства;

– відповідність постачальників обладнання та послуг, існуючим вимогам;

– оцінка ефективності ІТ;

– оцінка рівня безпеки.

5. Включити в політику безпеки специфічні вимоги по забезпеченню фізичної безпеки. Розробити вимоги до фізичних умов експлуатації обчислювальної техніки і мережного встаткування.

6. Виробити та прийняти угоду про рівень обслуговування між провайдером IT і користувачами інформаційної системи – з іншої сторони. Визначити кількісні і якісні критерії оцінки по кожному з видів послуг і продуктів. Організувати формальну процедуру періодичної оцінки відповідності рівня послуг заявленій якості.

7. Організувати моніторинг законодавства, що має вплив на сферу інформаційних технологій.

8. Розробити і запровадити методику та процедури оцінки ризиків при плануванні та проектуванні в області IT. Рекомендується, щоб процедури базувалися на звітах по інцидентах і проблемам та містили процеси:

– ідентифікації ризиків;

– аналізу та оцінки ризиків;

– вибору засобів скорочення ризиків.

9. Визначити сфери контролю. Організувати періодичний внутрішній аудит процесів IT на предмет їхньої відповідності внутрішнім і зовнішнім вимогам.

10. Розробити і запровадити процедури перевірки відомостей резюме, рекомендацій при прийомі на роботу співробітників відділів, що працюють з IT.

11. Організувати процедури моніторингу за процесами в області IT. Організувати збір і зберігання кількісних й якісних оцінок продуктивності по процесах в IT.

12. У процесі проектування автоматизованих рішень рекомендується враховувати майбутню необхідність здійснення контролю над безпекою обчислень та обміну даними.

13. Розробити правила обігу зі знімними носіями даних. Визначити коло осіб, яким дозволено користуватися знімними носіями для виконання

своїх обов’язків. Організувати облік і маркування використовуваних носіїв, а також контроль за внесенням/ винесенням носіїв.

14. Розробити і запровадити формальні процедури по планово-попереджувальному обслуговуванню встаткування.

15. Розробити регламент роботи служби технічної підтримки. Привести посадові інструкції задіяного персоналу у відповідність регламенту. Виробити погоджений з користувачами рівень обслуговування, що визначає кількісні і якісні критерії оцінки роботи служби технічної підтримки. Організувати процедури обліку користувальницьких запитів, строків і результатів їхнього відпрацьовування.

16. Розробити вимоги до сховищ даних. Рекомендується включити в них наступні положення:

– оснащення сховища датчиками проникнення;

– забезпечення фізичної безпеки приміщення.

17. Розробити процедури виконання резервних копій і післяаварійного відновлення даних і включити опис процедур у план по забезпеченню безперервності. Рекомендується:

– організувати виділене сховище резервних копій, відповідно до вимог сховищ даних;

– організувати резервне копіювання даних на знімні носії та забезпечити надійне і безпечне зберігання цих носіїв;

– організувати періодичне тестування плану по відновленню втрачених даних;

– організувати процедури контролю над виконанням вимог по резервуванню даних.

18. Розробити політику безпеки підприємства. При розробці специфічних політик, положень, стандартів та інструкцій в області інформаційних технологій і телекомунікацій, ураховувати вимоги політики безпеки.

19. Включити в політику безпеки підприємства вимоги забезпечення антивірусного захисту. Розробити політику антивірусного захисту. Рекомендується внести в неї наступні положення:

– процедури періодичного примусового сканування всіх файлів;

– розподіл відповідальності за антивірусний захист;

– процедури реагування на інциденти;

– звітність про виконання періодичних процедур.

20. Розробити методику обліку витрат на підтримку IT.

21. Розробити схему класифікації інформації по рівням конфіденційності (конфіденційно, для службового користування, відкрито) і приналежності. У ході розробки специфічних політик, положень, стандартів та інструкцій в області інформаційних технологій і телекомунікацій визначити належний рівень забезпечення захисту для кожного із класів інформації. На основі класифікації даних по приналежності розробити і задокументувати схему доступу до даних (створення, модифікація, читання тощо).

22. Розробити наступні специфічні політики:

– забезпечення безперервності роботи;

– правила керування доступом;

– вимоги до постачальників обладнання та послуг і політика взаємовідносин з ними.

23. На основі класифікації по рівнях конфіденційності, визначити адекватні міри захисту конфіденційної і службової інформації при її передачі по незахищених каналах передачі даних.

24. Організувати моніторинг за продуктивністю каналів передачі даних і обчислювальних ресурсів, що дозволяють реєструвати факти перевантажень, у тому числі заявлені користувачами. Забезпечити аналіз і регулярну звітність про збої та простої, викликаних перевантаженнями. Розробити і запровадити методику планування продуктивності. Зокрема,

включити до складу первісної установки систем і додатків процес настроювання оптимальних параметрів продуктивності.

25. Поліпшити розподіл обов’язків і відповідальність із погляду безпеки та внутрішнього контролю.

26. Розробити регламент керування інцидентами і проблемами. Організувати формальну реєстрацію інцидентів, процесу їхнього усунення та закриття. Затвердити стандартний формат звіту про інцидент. Організувати оповіщення зацікавлених служб IT в усуненні причин подібних інцидентів.

27. Організувати процес вивчення потреб користувачів у навчанні і тренінгах (періодичне проведення опитувань, web-форум і т.п.). Розробити програму навчання користувачів, що включала б у себе кілька тематичних програм. Забезпечити періодичне проведення тренінгів по темах.

28. Забезпечити розробку і ефективне доведення політик і правил до персоналу. Створити позитивне відношення до питань внутрішнього контролю та інформаційної безпеки. Розподілити відповідальність за дотриманням політик серед відповідальних за IT.

29. Рекомендується, щоб політика інформаційної безпеки охоплювала питання забезпечення безпеки при взаємодіях з постачальниками послуг, устаткування і програмного забезпечення.

30. Внести в політику безпеки вимоги по керуванню доступом до інформаційних ресурсів. Розробити правила надання доступу. Рекомендується, щоб вони враховували наступні положення:

– рівень доступу до будь-якого ресурсу визначається власником цього ресурсу;

– узгодженість прав доступу та привілеїв з посадовими обов’язками (мінімально необхідний доступ);

– порядок надання доступу (делегування привілеїв);

– формальне прийняття користувачам прав і привілеїв;

– порядок позбавлення прав доступу при звільненні;

– порядок документування фактів надання доступу, внесення змін та позбавлення доступу.

31. Включити в політику безпеки положення про забезпечення безперервності роботи. Рекомендуємо включити в політику наступні положення:

– філософія та стратегія забезпечення безперервності роботи;

– вимоги по наявності плану по забезпеченню безперервності роботи;

– вимоги підтримки плану в актуальному стані;

– розміщення пріоритетів в інформаційних ресурсах, підлягаючих резервуванню на основі їх класифікації, важливості тощо.

Виконавши всі вимоги, можна отримати нову матрицю знань та розрахувати якість СЗІ, або ступінь (повноту) виконання вимог до СЗІ, за новими вихідними даними. Нові дані змодельовані відповідно до рекомендацій, тобто стан захисту інформації теж змодельований.

Нові вхідні дані для побудови необхідного профілю безпеки представлені у вигляді матриці знань у додатку Е.

В таблиці 3.4. представлені дані для оцінки захищеності об’єктів ІС (по першому напрямку захисту).

Порівняння профілів захисту об’єктів ІС при дійсному стані та при моделюванні можна побачити на графіку, який показано на рис. 3.6.

Ступінь виконання груп вимог ($Q_{груп}$) визначається з урахуванням коефіцієнтів важливості ($Q_{да_j}$) для кожного з етапів: 1 – 0,715; 2 – 0,73; 3 – 0,73; 4 – 0,77; 5 – 0,785; 6 – 0,745; 7 – 0,78. Графічно ці значення, що ми отримали в ході моделювання, та дійсні значення порівняні на діаграмі на рис. 3.7.

Якісна оцінка ($Q$) визначається виходячи зі значень показників ($Q_{груп}$), що змодельовані для відповідних етапів. У нашому випадку $Q = 0{,}75$. Тобто, якісна оцінка збільшилася на 10%.

*Таблиця 3.4*

# Дані для оцінки СЗІ по напрямку «Захист об’єктів ІС»

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,715 | 0,75 | 0,43 |
| | 2 | 112 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| 2 | 5 | 211 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,73 | | |
| | 6 | 212 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | | | |
| | 7 | 213 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 8 | 214 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| 3 | 9 | 311 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | 0,73 | | |
| | 10 | 312 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | | | |
| | 11 | 313 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 12 | 314 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,77 | | |
| | 14 | 412 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 15 | 413 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 16 | 414 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| 5 | 17 | 511 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,785 | | |
| | 18 | 512 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 6 | 21 | 611 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | 0,745 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 23 | 613 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 24 | 614 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| 7 | 25 | 711 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,78 | | |
| | 26 | 712 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 27 | 713 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 28 | 714 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |


Рисунок 3.6 – Порівняння профілів захисту об’єктів ІС

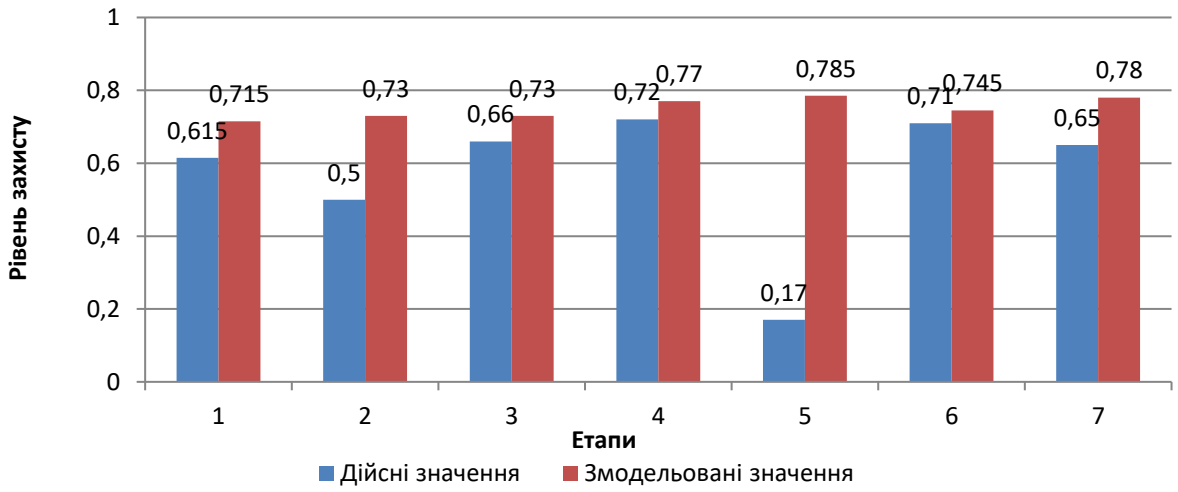


Рисунок 3.7 – Оцінка етапів захисту об’єктів ІС

Кількісна оцінка ($S$) визначається шляхом підрахунку значень ($S_{пр}$), а саме нулів та одиниць, отриманих при порівнянні профілів $S = 0{,}43$. Іншими словами в змодельованій інформаційній системі виконано 43% вимог по захисту об’єктів ІС. Цей результат перевищує дійсний (21%) в два рази.

Аналогічно розраховуємо ті самі показники для інших чотирьох напрямків інформаційної безпеки. Розрахункові та графічні результати наведені у додатках Ж, З, К і Л.

Далі, об’єднавши часткові показники (по напрямках) в узагальнений показник, одержуємо результуючий профіль безпеки $Q_{СЗІ}$ (таблиця М.1) і його графічне зображення (рис. М.1).

Зверніть увагу на те, що всі вимоги, хоча б в одному напрямку, виконуються. Визначити які групи вимог по яких напрямках виконані, можна за допомогою діаграми, зображеної на рис. 3.8.

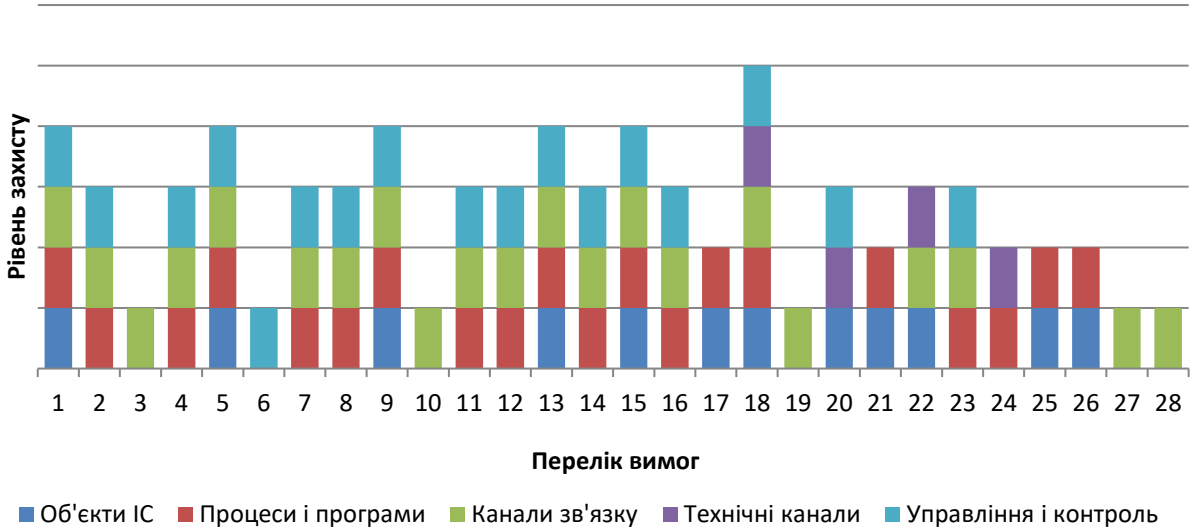


Рисунок 3.8 – Графічне зображення узагальнених кількісних оцінок ступеню виконання за окремими вимогами

Узагальнені показники рівня захищеності (якісний і кількісний) представлені в таблиці 3.5.

*Таблиця 3.5*

**Узагальнені показники рівня захищеності ІС**

| Показники | Напрямки захисту | | | | | $Q_{СЗІ}$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| | Коефіцієнти важливості по напрямкам | | | | | |
| | 0,3 | 0,1 | 0,2 | 0,1 | 0,3 | |
| Кількісний | 0,43 | 0,71 | 0,75 | 0,14 | 0,57 | 0,54 |
| Якісний | 0,75 | 0,78 | 0,77 | 0,58 | 0,76 | 0,74 |

Перевищення величини якісного показника над кількісним, свідчить про те, що виконані вимоги більше важливі за своїм значенням, чим невиконані.

При порівняні з дійсними значеннями узагальнених показників спостерігається збільшення з 0,23 до 0,54 кількісного показника та з 0,64 до 0,74 якісного показника.

У додатку Н представлена матриця кількісних оцінок рівня захищеності, що дозволяє наочно оцінити ступінь виконання вимог по захисту інформації. Це дає можливість визначити сильні та слабкі місця в СЗІ.

При моделюванні ситуації, при якій запроваджуються запропоновані рекомендацій щодо захисту інформації., можна побачити збільшення всіх показників якості СЗІ, що підтверджує необхідність застосування цих рекомендацій на практиці.

Цей перелік рекомендацій включає найнеобхідніші заходи інформаційної безпеки, які треба виконати першочергово. Недотримання елементарних вимог захисту інформації призводить до неефективності вже запроваджених заходів.

## 3.4. Висновки до розділу 3

У відповідності до класифікації американської компанії Gartner Group ТОВ «Южмаш груп» знаходиться на перехідному етапі між 0 та 1 рівнями. Для досягнення наступного рівня зрілості (не нижче 1, бажано 2) необхідно на підприємстві здійснити ряд заходів, що наведені у додатку В («Рекомендації»), та виконувати пропозиції і вимоги, розглянуті в міжнародному стандарті ISO 17799.

Для моделювання СУІБП рекомендовано використовувати «процесну модель», описану в міжнародному стандарті ISO/ IEC 27001:2005.

Як правило, головними перешкодами на шляху забезпечення інформаційної безпеки стає складність обґрунтування необхідних заходів і витрат на їхнє виконання. Компанії нерідко виділяють єдиний бюджет на задоволення всіх потреб по інформаційних системах (апаратне й програмне забезпечення, зарплата, консультанти й т.п.), що сприяє розвитку тенденції виділяти основну частину засобів на підвищення продуктивності, при цьому нерідко питання безпеки залишаються без уваги.

Вибіркова і безсистемна реалізація заходів, спрямованих на підвищення рівня інформаційної безпеки, не зможе забезпечити необхідного рівня захисту. Щоб сформувати розуміння пріоритетності заходів щодо підвищення рівня безпеки, необхідно розробити механізм керування ризиками інформаційної безпеки, що дозволить направити всі зусилля на захист від найнебезпечніших погроз і мінімізацію витрат.

Якщо топ-менеджер у стані оцінити витрати на заходи щодо мінімізації критичних ризиків, а також чітко представляє, скільки грошей компанія може втратити внаслідок реалізації погроз, які місця в системі найбільш уразливі, які міри можна почати для підвищення рівня безпеки, то досягнення необхідного ступеня захисту з мінімальними витратами стає більше реальним.

# ВИСНОВКИ

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Впливи, які призводять до зниження цінності інформаційних ресурсів, називаються несприятливими. А потенційно можливий несприятливий вплив називається загрозою.

Із всієї множини способів класифікації загроз інформаційної безпеки найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Інформатизація суспільства та інтенсивний розвиток інформаційних технологій збереження інформації та її цілісності, захист від копіювання і модифікації є завданнями державної важливості та забезпечують пріоритети держави в політичній, військовій, економічній і науково-технічній областях.

Правовою основою забезпечення інформаційного захисту в Україні є Конституція України, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію», інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Інформація може бути представлена в різних формах. Вона може перебувати в електронному виді, у паперовому, бути передана по електронній пошті, зафіксована у вигляді зображення на відеозаписі, розказана під час переговорів. Підприємство одержує інформацію з різних

джерел, як усередині організації, так і за її межами. Підприємство використає інформацію на кожному кроці будь-якого бізнесу-процесу. Зі збільшенням ролі інформаційних технологій у створенні, зберіганні, передачі інформації значно виросла кількість погроз, пов’язаних з інформацією.

Інформацію можна вважати надійно захищеною тільки тоді, коли для її захисту комплексно використовуються та органічно поєднуються усі види захисту: криптографічний, технічний, організаційних.

Впровадження системи керування інформаційною безпекою – важливий захід, метою якого є керування процесами інформаційного забезпечення організації та запобігання несанкціонованого використання інформації.

Політика безпеки інформації в ІС є частиною загальної політики безпеки організації і може успадковувати положення державної політики у галузі захисту інформації. Вона повинна визначати ресурси ІС, які потребують захисту, мають бути сформульовані основні загрози для ІС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Достатньо зрозуміла необхідність появи принципово нових методів та засобів для захисту інформації, які будуть розроблені з урахуванням цінності інформації, умов роботи, технічних і програмних можливостей ІС та інших засобів збору, передачі і обробки даних.

Перелік засобів захисту інформації настільки широкий за вартістю, призначенню і якістю продуктів, що вибір найбільш оптимальних з них для конкретного об’єкта представляється досить непростим завданням.

Складність процесу прийняття рішень, відсутність математичного апарата призводять до того, що при оцінці та виборі необхідно використовувати і обробляти якісну експертну інформацію.

Доволі перспективним напрямком розробки методів прийняття рішень при експертній вхідній інформації є лінгвістичний підхід на базі теорії нечітких множин та лінгвістичної змінної.

Теоретичні основи побудови оптимальних систем захисту винятково складні і, незважаючи на інтенсивність досліджень у цій предметній області, ще далекі від досконалості.

Оптимальним уважається те рішення, яке у запропонованих обставинах найкраще задовольнить умовам розглянутого завдання. Оптимальність рішення досягається за рахунок найбільш раціонального розподілу ресурсів, затрачуваних на рішення проблеми захисту.

Підприємства нерідко виділяють єдиний бюджет на задоволення всіх потреб по інформаційних системах (апаратне й програмне забезпечення, зарплата, консультанти й т.п.), що сприяє розвитку тенденції виділяти основну частину засобів на підвищення продуктивності, при цьому нерідко питання безпеки залишаються без уваги. Щоб сформувати розуміння пріоритетності заходів щодо підвищення рівня безпеки, необхідно розробити механізм керування ризиками інформаційної безпеки, що дозволить направити всі зусилля на захист від найнебезпечніших погроз і мінімізацію витрат.

Таким чином, забезпечення інформаційної безпеки автоматизованих систем комерційних структур має досить конкретний економічний сенс і здобуття стану захищеності інформації від загроз повинно здійснюватися економічно виправданими заходами. Тому в основі більшості методів оцінки ефективності вкладень в інформаційну безпеку лежить зіставлення витрат, що необхідні для створення та запровадження системи захисту інформації, та збитку, який може бути завданий підприємству через її відсутність або неефективність.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації*. 2013. Т. 15, № 4. С. 366–375.

2. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції. *Вісник Національного університету «Львівська політехніка».* 2018. № 610. С. 20–33.

3. Бінько І. Ф. Національна безпека України в умовах глобальної інформатизації. Київ : Національний ін–т стратегічних досліджень, 1996. Вип.61. 54 с.

4. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ. *Форум права.* 2009. № 1. С. 50–55.

5. Бодрук О. Структури воєнної безпеки : національний та міжнародний аспекти : монографія. Київ : НІПМБ, 2001. 300 с.

6. Борисов А. Н., Крумберг О. А., Федоров И. П. Принятие решения на основе нечетких моделей: примеры использования. Рига : «Знание», 1990. 184 с.

7. Глотов В. А. Метод определения коэффициентов относительной важности. *Приборы и системы управления*. 1976. №8. С.17–22.

8. Глушак В., Новіков О. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника. URL: https://ela.kpi.ua/bitstream/123456789/6875/1/09_Glush.pdf (дата звернення: 10.09.2020).

9. Гончаренко Є. О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі: дис…маг. : 125. Київ. 2019. 92 с.

10. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник. Харків : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. 48 с.

11. Гуцу С. Ф. Правові основи інформаційної діяльності. – Режим доступу URL: https://www.studmed.ru/gucu-sf-pravov-osnovi-nformacynoyi-dyalnost_69761ebeaf5.html (дата звернення: 10.09.2020).

12. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 14/2009. URL: www.president.gov.ua (дата звернення: 10.09.2020).

13. Домарёв В. В. Безопасность информационных технологий. Системный подход. Київ : ООО «ТИД «ДС», 2004. 992 с.

14. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки. *Політичний менеджмент.* 2010. № 5. С. 19–30.

15. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис… канд. наук з держ. упр. Львів, 2011. 24 с.

16. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. URL: //www.dstszi.gov.ua/dstszi/control/uk/publish/article; jsessionid=5D34EDB7C 9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=3883 (дата звернення: 10.09.2020).

17. Золотар О. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. №3(9). С. 105–112.

18. Зубок М. Інформаційна безпека в підприємницькій діяльності. Підручник. Київ : 2015. 216 с.

19. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій. Gaithersburg: National Institute of Standards and Technology, 2002. 95 с.

20. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса : Юридична література, 2013. 472 с.

21. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис… д-ра юрид. наук. : 12.00.07. Харків., 2004. 432 с.

22. Косач П. Д. Інформаційна безпека як основа національної безпеки. Київ : ЗАТ Видавничий дім «ДЕМЩ», 2002. 144 с.

23. Кузьменко Б. В. Захист інформації : навч. посіб. – Ч. 2. Київ : Видавничий відділ КНУКіМ, 2009. – 69 с.

24. Левашов М. Роль службы информационной безопасности во внутренней структуре современного предприятия. *CONNECT*. 2006. №12. С. 194–198.

25. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції. URL: //www.pidruchniki.ws/12800528/politologiya/ponyattya_ zagroz_informatsiyniy_bezpetsi (дата звернення: 10.09.2020).

26. Ліпкан В.А. Національна безпека України. – Режим доступу : URL: //www.pidruchniki.ws15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim _interesam_natsionalniy_bezpetsi_inform atsiyniy_sferi (дата звернення: 10.09.2020).

27. Литвиненко О. В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис… канд. політ. наук: спец. 23.00.04. Київ, 1997. 18 с.

28. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: //www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_ 7/lytvynenko.pdf (дата звернення: 10.09.2020).

29. Логінов А. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис… кандидата юридичних наук : 12.00.07. Київ, 2005. 244 с.

30. Макарова М. В. Електронна комерція : посібник для студентів вищ. навч. закладів. Київ : Видавничий центр «Академия», 2002. 272 с.

31. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис… канд. юрид. наук. : 12.00.01. Київ, 2007. 22 с.

32. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92–95.

33. Марущак А. І. Пріоритети розвитку інформаційного права України. *Інформація і право.* 2011. № 1. С. 20–24.

34. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології. Технології безпеки. Система керування інформаційною безпекою. Вимоги» URL: http://www.ni.din.de/sc27.html. (дата звернення: 10.09.2020).

35. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис… канд. юрид. наук : 12.00.07. Київ., 2006. 20 с.

36. Пилипчук В. Г. Системні проблеми розвитку правової науки в інформаційній сфері. *Вісник Академії правових наук Украї*ни. 2011. № 3. С. 16–27.

37. Погребняк А. В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.

38. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. № 373 // *Офіційний вісник України.* 2006. № 13. С. 20–22.

39. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки : Закон України : від 09.01.07 р. № 537-V. *Відомості Верховної Ради України.* 2007. № 12. С. 102–103.

40. Про основи національної безпеки України : Закон України : від 19.06.03 р. № 964-IV. *Відомості Верховної Ради України.* 2003. № 39. С. 11–23.

41. Романовский С. BS ISO/IEC 20000 – процессный подход к управлению информационной безопасностью современной организации. *CIO-информационная безопасность*. 2007. №2. С. 86–88.

42. Ротштейн А. П. Интеллектуальные технологии идентификации. Винница: «Универсум-Винница», 1999. 320 с.

43. Сваровский С. Т. Аппроксимация функций принадлежности значений лингвистической переменной. *Математические вопросы анализа данных.* 1980. №3. С.127–131.

44. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи. URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf (дата звернення: 10.09.2020).

45. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту. *Держава та право.* 2014. №8. С. 18–22.

46. Тацюра М. Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства. *«Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» :* матеріали Другої наук.-практ. конф. Сімферополь: Фенікс, 2010. С. 451–453.

47. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – URL: //www.dstszi.gov.ua/dstszi/control/uk/ publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id= 38836 (дата звернення: 10.09.2020).

48. Харламов В. П. Некоторые концептуальные аспекты защиты информации. *Вопросы защиты информации*. 2003. №1. С. 4–9.

49. Харченко Л. С. Інформаційна безпека України: Глосарій. Київ : Текст, 2004. 136 с.

50. Цвілій О. Безпека інформаційних технологій: сучасний стан стандартів ISO27k системи управління інформаційною безпекою. *Телекомунікаційні та інформаційні технології*. 2014. № 2. С. 73–79.

51. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2004. №8. С. 30–33.

52. Фурашев В. М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки. Інформація і право: науковий журнал. 2012. № 1(4). С.46–56.

53. Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту. Держава та права. 2014. №3. С. 26–31.

54. Introducing OCTAVE Allegro: Improving the Information Security RiskAssessment Process. Бостон: Університет Карнегі-Меллон, 2007. 154 с.

55. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Київ : ДП«УкрНДНЦ», 2005. 60 с.

56. Management of Federal InformationResources, Office of Managementand Budget 1996. OMB Circular A-130. Washington.

57. Parker, D. 1976. Crimeby Computer. NewYork: Chas Scribners Sons.

58. U.S. Department of Commerce, National Bureau of Standards, 1979.Guideline for Automatic Data Processing Risk Analysis, Federal Information Processing Standards Publication FIPS 65.

Додаток А

*Таблиця А.1*

**Матриця знань (оцінок) дійсного стану захисту інформації ТОВ «Южмаш груп»**

| Етапи | Напрямки | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Захист об’єктів ІС | | | | Захист процесів та програм | | | | Захист каналів зв’язку | | | | Захист випромінювань | | | | Управляння системою захисту | | | |
| | Основи | база | структура | заходи | Засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Визначення інформації, що підлягає захисту | 0,7 | 0,5 | 0,5 | 0,6 | 0,8 | 0,7 | 0,7 | 0,7 | 0,8 | 0,7 | 0,7 | 0,8 | 0,1 | 0,1 | 0,1 | 0,1 | 0,5 | 0,3 | 0,3 | 0,3 |
| 200 | Виявлення загроз та каналів витоку інформації | 0,5 | 0,5 | 0,5 | 0,5 | 0,8 | 0,6 | 0,8 | 0,8 | 0,8 | 0,6 | 0,8 | 0,8 | 0,3 | 0,3 | 0,2 | 0,2 | 0,8 | 0,8 | 0,8 | 0,8 |
| 300 | Проведення оцінки уразливостей та ризиків | 0,8 | 0,6 | 0,6 | 0,6 | 0,8 | 0,7 | 0,7 | 0,8 | 0,8 | 0,7 | 0,7 | 0,8 | 0,1 | 0,1 | 0,1 | 0,1 | 0,8 | 0,8 | 0,7 | 0,7 |
| 400 | Визначення вимог до СЗІ | 0,8 | 0,6 | 0,7 | 0,6 | 0,8 | 0,8 | 0,7 | 0,7 | 0,8 | 0,7 | 0,7 | 0,8 | 0,3 | 0,3 | 0,3 | 0,3 | 0,8 | 0,6 | 0,6 | 0,6 |
| 500 | Здійснення вибору засобів захисту | 0,7 | 0,8 | 0,6 | 0,7 | 0,7 | 0,8 | 0,6 | 0,6 | 0,7 | 0,8 | 0,5 | 0,5 | 0,2 | 0,6 | 0,3 | 0,6 | 0,7 | 0,6 | 0,8 | 0,7 |
| 600 | Запровадження обраних заходів та засобів | 0,8 | 0,8 | 0,6 | 0,5 | 0,8 | 0,7 | 0,7 | 0,5 | 0,8 | 0,7 | 0,6 | 0,5 | 0,3 | 0,6 | 0,3 | 0,6 | 0,8 | 0,5 | 0,5 | 0,4 |
| 700 | Контроль цілісності та управляння захистом | 0,6 | 0,8 | 0,5 | 0,5 | 0,7 | 0,8 | 0,6 | 0,6 | 0,6 | 0,8 | 0,7 | 0,7 | 0,4 | 0,5 | 0,3 | 0,3 | 0,7 | 0,8 | 0,6 | 0,6 |

Додаток Б

*Таблиця Б.1*

**Дані для оцінки СЗІ по напрямку «Захист процесів і програм»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,75 | 0,73 | 0,39 |
| | 2 | 112 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 3 | 113 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 4 | 114 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| 2 | 5 | 211 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,76 | | |
| | 6 | 212 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| 3 | 9 | 311 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,76 | | |
| | 10 | 312 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 11 | 313 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 12 | 314 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 4 | 13 | 411 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,78 | | |
| | 14 | 412 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 15 | 413 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 16 | 414 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| 5 | 17 | 511 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | 0,71 | | |
| | 18 | 512 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 20 | 514 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| 6 | 21 | 611 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | 0,675 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 23 | 613 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 24 | 614 | 0,25 | 0,8 | 0,5 | 0,125 | 0 | | | |
| 7 | 25 | 711 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | 0,68 | | |
| | 26 | 712 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 28 | 714 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |

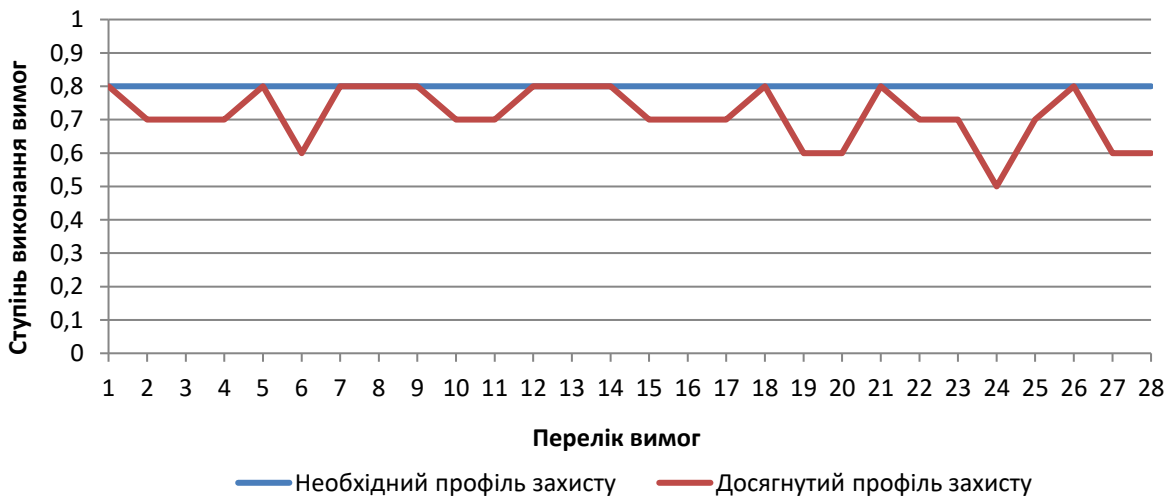


Рисунок Б.1 – Порівняння профілів захисту процесів та програм

Додаток В

*Таблиця В.1*

**Дані для оцінки СЗІ по напрямку «Захист каналів зв'язку»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | 0,745 | 0,72 | 0,43 |
| | 2 | 112 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| 2 | 5 | 211 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,75 | | |
| | 6 | 212 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 3 | 9 | 311 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,77 | | |
| | 10 | 312 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 11 | 313 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 12 | 314 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,76 | | |
| | 14 | 412 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | | | |
| | 15 | 413 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 16 | 414 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| 5 | 17 | 511 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | 0,64 | | |
| | 18 | 512 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,5 | 0,075 | 0 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,5 | 0,125 | 0 | | | |
| 6 | 21 | 611 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,715 | | |
| | 22 | 612 | 0,35 | 0,8 | 0,7 | 0,245 | 0 | | | |
| | 23 | 613 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 24 | 614 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |
| 7 | 25 | 711 | 0,5 | 0,8 | 0,6 | 0,3 | 0 | 0,67 | | |
| | 26 | 712 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 28 | 714 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |

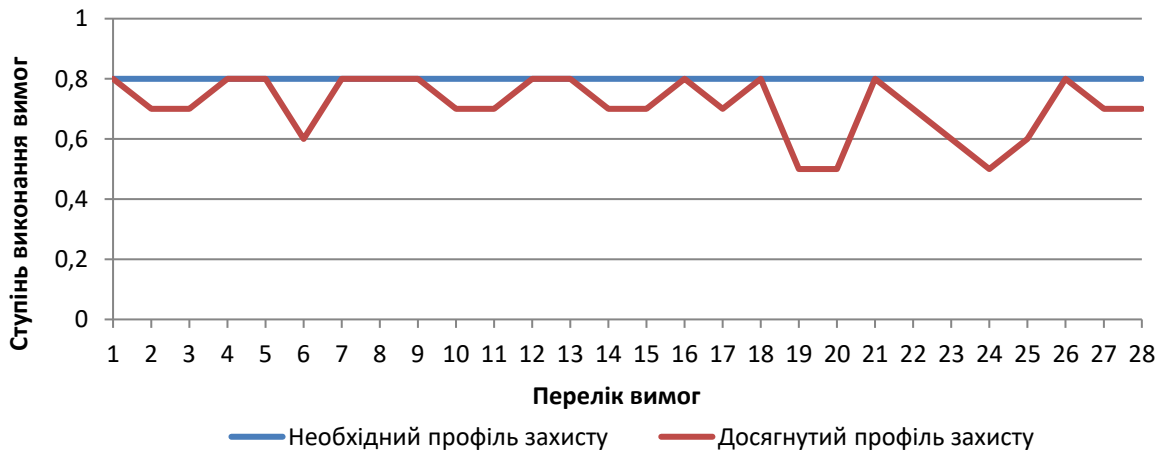


Рисунок В.1 – Порівняння профілів захисту каналів зв'язку

Додаток Г

*Таблиця Г.1*

**Дані для оцінки СЗІ по напрямку «Приглушення випромінювань»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,1 | 0,05 | 0 | 0,1 | 0,29 | 0 |
| | 2 | 112 | 0,2 | 0,8 | 0,1 | 0,02 | 0 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,1 | 0,015 | 0 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,1 | 0,015 | 0 | | | |
| 2 | 5 | 211 | 0,3 | 0,8 | 0,3 | 0,09 | 0 | 0,27 | | |
| | 6 | 212 | 0,4 | 0,8 | 0,3 | 0,12 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,2 | 0,03 | 0 | | | |
| | 8 | 214 | 0,15 | 0,8 | 0,2 | 0,03 | 0 | | | |
| 3 | 9 | 311 | 0,5 | 0,8 | 0,1 | 0,05 | 0 | 0,1 | | |
| | 10 | 312 | 0,1 | 0,8 | 0,1 | 0,01 | 0 | | | |
| | 11 | 313 | 0,2 | 0,8 | 0,1 | 0,02 | 0 | | | |
| | 12 | 314 | 0,2 | 0,8 | 0,1 | 0,02 | 0 | | | |
| 4 | 13 | 411 | 0,4 | 0,8 | 0,3 | 0,12 | 0 | 0,3 | | |
| | 14 | 412 | 0,2 | 0,8 | 0,3 | 0,06 | 0 | | | |
| | 15 | 413 | 0,15 | 0,8 | 0,3 | 0,045 | 0 | | | |
| | 16 | 414 | 0,25 | 0,8 | 0,3 | 0,075 | 0 | | | |
| 5 | 17 | 511 | 0,45 | 0,8 | 0,2 | 0,09 | 0 | 0,39 | | |
| | 18 | 512 | 0,35 | 0,8 | 0,6 | 0,21 | 0 | | | |
| | 19 | 513 | 0,1 | 0,8 | 0,3 | 0,03 | 0 | | | |
| | 20 | 514 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| 6 | 21 | 611 | 0,35 | 0,8 | 0,3 | 0,105 | 0 | 0,45 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |
| | 23 | 613 | 0,15 | 0,8 | 0,3 | 0,045 | 0 | | | |
| | 24 | 614 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |
| 7 | 25 | 711 | 0,5 | 0,8 | 0,4 | 0,2 | 0 | 0,41 | | |
| | 26 | 712 | 0,3 | 0,8 | 0,5 | 0,15 | 0 | | | |
| | 27 | 713 | 0,1 | 0,8 | 0,3 | 0,03 | 0 | | | |
| | 28 | 714 | 0,1 | 0,8 | 0,3 | 0,03 | 0 | | | |


Рисунок Г.1 – Порівняння профілів приглушення випромінювань

Додаток Д

*Таблиця Д.1*

**Дані для оцінки СЗІ по напрямку «Керування системою захисту»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,5 | 0,25 | 0 | 0,4 | 0,67 | 0,36 |
| | 2 | 112 | 0,3 | 0,8 | 0,3 | 0,09 | 0 | | | |
| | 3 | 113 | 0,1 | 0,8 | 0,3 | 0,03 | 0 | | | |
| | 4 | 114 | 0,1 | 0,8 | 0,3 | 0,03 | 0 | | | |
| 2 | 5 | 211 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,8 | | |
| | 6 | 212 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 3 | 9 | 311 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,78 | | |
| | 10 | 312 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 11 | 313 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 12 | 314 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,7 | | |
| | 14 | 412 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 15 | 413 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 16 | 414 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| 5 | 17 | 511 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | 0,695 | | |
| | 18 | 512 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| 6 | 21 | 611 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,63 | | |
| | 22 | 612 | 0,1 | 0,8 | 0,5 | 0,05 | 0 | | | |
| | 23 | 613 | 0,2 | 0,8 | 0,5 | 0,1 | 0 | | | |
| | 24 | 614 | 0,2 | 0,8 | 0,4 | 0,08 | 0 | | | |
| 7 | 25 | 711 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | 0,71 | | |
| | 26 | 712 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 28 | 714 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |

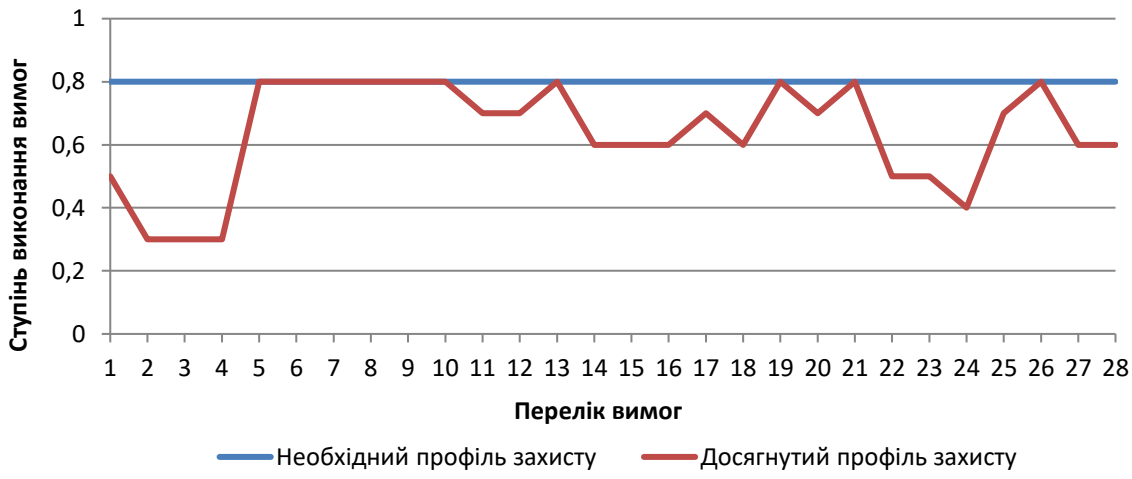


Рисунок Д.1 – Порівняння профілів керування системою захисту

Додаток Е

*Таблиця Е.1*

**Матриця знань (оцінок) стану захисту інформації на ТОВ «Южмаш груп» при моделюванні**

| Етапи | Напрямки | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Захист об'єктів ІС | | | | Захист процесів та програм | | | | Захист каналів зв'язку | | | | Захист випромінювань | | | | Управляння системою захисту | | | |
| | Основи | база | структура | заходи | Засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Визначення інформації, що підлягає захисту | 0,8 | 0,6 | 0,6 | 0,7 | 0,8 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,5 | 0,4 | 0,4 | 0,4 | 0,8 | 0,7 | 0,6 | 0,7 |
| 200 | Виявлення загроз та каналів витоку інформації | 0,8 | 0,7 | 0,6 | 0,6 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,7 | 0,8 | 0,8 | 0,6 | 0,6 | 0,4 | 0,4 | 0,8 | 0,8 | 0,8 | 0,8 |
| 300 | Проведення оцінки уразливостей та ризиків | 0,8 | 0,7 | 0,7 | 0,7 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,4 | 0,4 | 0,4 | 0,4 | 0,8 | 0,8 | 0,8 | 0,8 |
| 400 | Визначення вимог до СЗІ | 0,8 | 0,7 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,8 | 0,6 | 0,6 | 0,7 | 0,7 | 0,8 | 0,7 | 0,6 | 0,7 |
| 500 | Здійснення вибору засобів захисту | 0,8 | 0,8 | 0,7 | 0,8 | 0,8 | 0,8 | 0,7 | 0,7 | 0,8 | 0,8 | 0,6 | 0,7 | 0,5 | 0,8 | 0,6 | 0,8 | 0,8 | 0,7 | 0,8 | 0,8 |
| 600 | Запровадження обраних заходів та засобів | 0,8 | 0,8 | 0,7 | 0,6 | 0,8 | 0,7 | 0,8 | 0,7 | 0,8 | 0,8 | 0,7 | 0,6 | 0,6 | 0,8 | 0,6 | 0,8 | 0,8 | 0,6 | 0,7 | 0,6 |
| 700 | Контроль цілісності та управляння захистом | 0,8 | 0,8 | 0,7 | 0,7 | 0,8 | 0,8 | 0,7 | 0,7 | 0,7 | 0,8 | 0,8 | 0,8 | 0,7 | 0,7 | 0,6 | 0,6 | 0,8 | 0,8 | 0,7 | 0,7 |

Додаток Ж

*Таблиця Ж.1*

**Дані для оцінки СЗІ по напрямку «Захист процесів і програм»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,78 | 0,78 | 0,71 |
| | 2 | 112 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 3 | 113 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 4 | 114 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| 2 | 5 | 211 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,78 | | |
| | 6 | 212 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| 3 | 9 | 311 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,775 | | |
| | 10 | 312 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 11 | 313 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 12 | 314 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 4 | 13 | 411 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,8 | | |
| | 14 | 412 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 15 | 413 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| | 16 | 414 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| 5 | 17 | 511 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | 0,77 | | |
| | 18 | 512 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 20 | 514 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| 6 | 21 | 611 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | 0,775 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 23 | 613 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 24 | 614 | 0,25 | 0,8 | 0,5 | 0,125 | 0 | | | |
| 7 | 25 | 711 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | 0,76 | | |
| | 26 | 712 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 28 | 714 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |

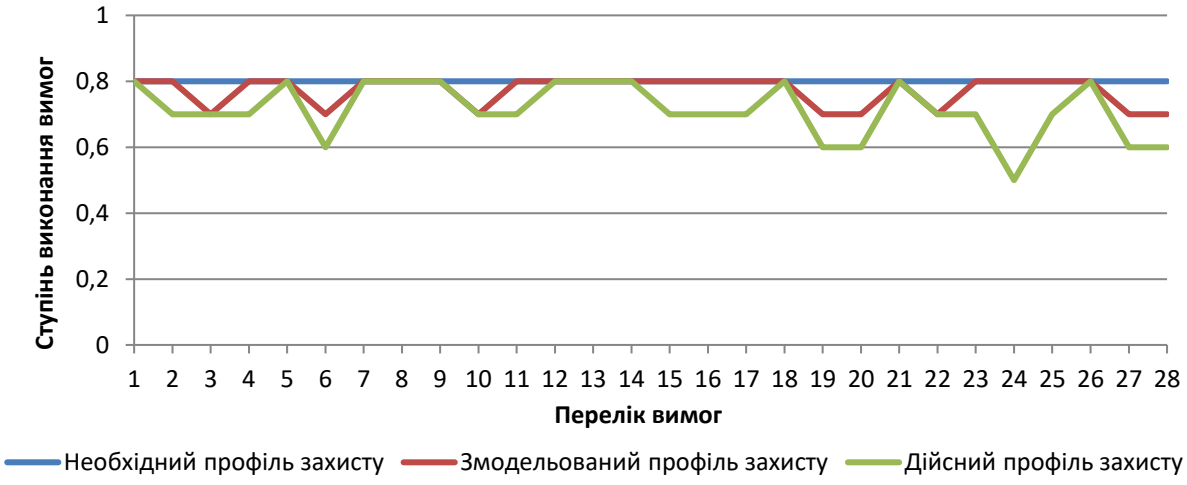


Рисунок Ж.1 – Порівняння профілів захисту процесів та програм

Додаток З

*Таблиця 3.1*

**Дані для оцінки СЗІ по напрямку «Захист каналів зв'язку»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | 0,8 | 0,77 | 0,75 |
| | 2 | 112 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| 2 | 5 | 211 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,775 | | |
| | 6 | 212 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 3 | 9 | 311 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,8 | | |
| | 10 | 312 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| | 11 | 313 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 12 | 314 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,8 | | |
| | 14 | 412 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | | | |
| | 15 | 413 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| | 16 | 414 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| 5 | 17 | 511 | 0,4 | 0,8 | 0,7 | 0,28 | 0 | 0,71 | | |
| | 18 | 512 | 0,2 | 0,8 | 0,8 | 0,16 | 1 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,6 | 0,15 | 0 | | | |
| 6 | 21 | 611 | 0,45 | 0,8 | 0,7 | 0,315 | 0 | 0,745 | | |
| | 22 | 612 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 23 | 613 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| | 24 | 614 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| 7 | 25 | 711 | 0,5 | 0,8 | 0,7 | 0,35 | 0 | 0,73 | | |
| | 26 | 712 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 28 | 714 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |

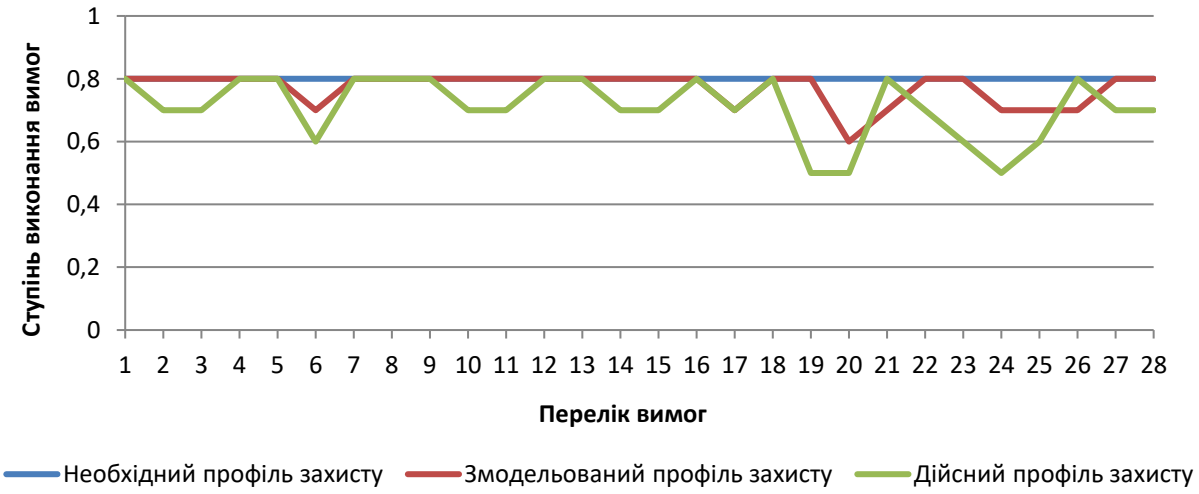


Рисунок 3.1 – Порівняння профілів захисту каналів зв'язку

Додаток К

*Таблиця К.1*

**Дані для оцінки СЗІ по напрямку «Приглушення випромінювань»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,5 | 0,25 | 0 | 0,45 | 0,58 | 0,14 |
| | 2 | 112 | 0,2 | 0,8 | 0,4 | 0,08 | 0 | | | |
| | 3 | 113 | 0,15 | 0,8 | 0,4 | 0,06 | 0 | | | |
| | 4 | 114 | 0,15 | 0,8 | 0,4 | 0,06 | 0 | | | |
| 2 | 5 | 211 | 0,3 | 0,8 | 0,6 | 0,18 | 0 | 0,54 | | |
| | 6 | 212 | 0,4 | 0,8 | 0,6 | 0,24 | 0 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,4 | 0,06 | 0 | | | |
| | 8 | 214 | 0,15 | 0,8 | 0,4 | 0,06 | 0 | | | |
| 3 | 9 | 311 | 0,5 | 0,8 | 0,4 | 0,2 | 0 | 0,4 | | |
| | 10 | 312 | 0,1 | 0,8 | 0,4 | 0,04 | 0 | | | |
| | 11 | 313 | 0,2 | 0,8 | 0,4 | 0,08 | 0 | | | |
| | 12 | 314 | 0,2 | 0,8 | 0,4 | 0,08 | 0 | | | |
| 4 | 13 | 411 | 0,4 | 0,8 | 0,6 | 0,24 | 0 | 0,64 | | |
| | 14 | 412 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| | 15 | 413 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 16 | 414 | 0,25 | 0,8 | 0,7 | 0,175 | 0 | | | |
| 5 | 17 | 511 | 0,45 | 0,8 | 0,5 | 0,225 | 0 | 0,645 | | |
| | 18 | 512 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 19 | 513 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 20 | 514 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| 6 | 21 | 611 | 0,35 | 0,8 | 0,6 | 0,21 | 0 | 0,7 | | |
| | 22 | 612 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 23 | 613 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 24 | 614 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 7 | 25 | 711 | 0,5 | 0,8 | 0,7 | 0,35 | 0 | 0,68 | | |
| | 26 | 712 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | | | |
| | 27 | 713 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 28 | 714 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |

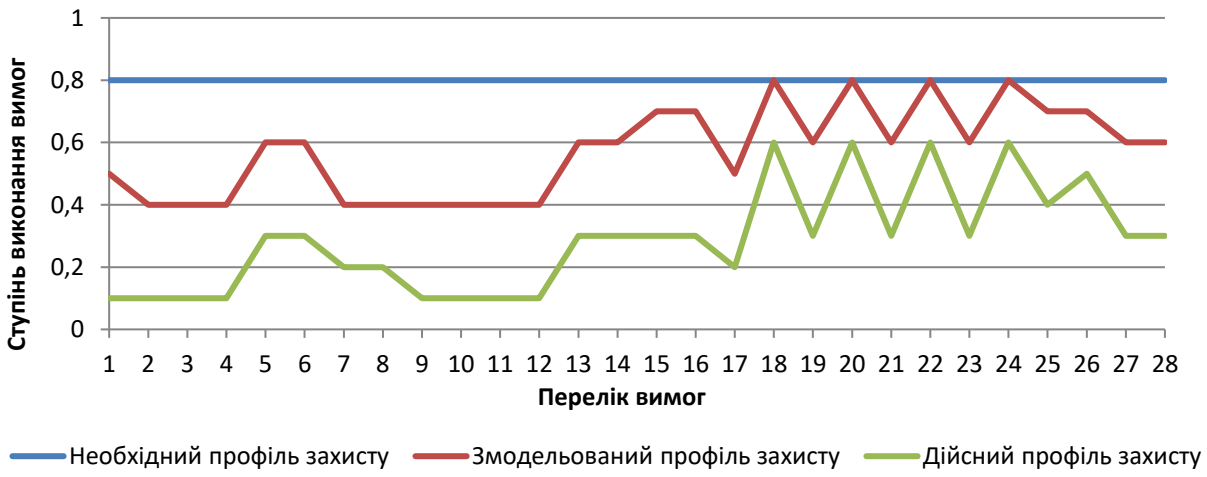


Рисунок К.1 – Порівняння профілів приглушення випромінювань

Додаток Л

*Таблиця Л.1*

**Дані для оцінки СЗІ по напрямку «Керування системою захисту»**

| № етапу | Перелік показників | № елементу матриці | Коефіцієнт важливості | Профіль безпеки необхідний | Профіль безпеки досягнутий | Qд х aj | Порівняння профілів | Ступінь виконання груп вимог | Якісна оцінка | Кількісна оцінка |
|---|---|---|---|---|---|---|---|---|---|---|
| | m | № | aj | Qн | Qд | Qд х aj | Sпр | Qгруп | Q | S |
| 1 | 1 | 111 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,74 | 0,76 | 0,57 |
| | 2 | 112 | 0,3 | 0,8 | 0,7 | 0,21 | 0 | | | |
| | 3 | 113 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 4 | 114 | 0,1 | 0,8 | 0,7 | 0,07 | 0 | | | |
| 2 | 5 | 211 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | 0,8 | | |
| | 6 | 212 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| | 7 | 213 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 8 | 214 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 3 | 9 | 311 | 0,45 | 0,8 | 0,8 | 0,36 | 1 | 0,8 | | |
| | 10 | 312 | 0,35 | 0,8 | 0,8 | 0,28 | 1 | | | |
| | 11 | 313 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| | 12 | 314 | 0,1 | 0,8 | 0,8 | 0,08 | 1 | | | |
| 4 | 13 | 411 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,735 | | |
| | 14 | 412 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 15 | 413 | 0,15 | 0,8 | 0,6 | 0,09 | 0 | | | |
| | 16 | 414 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| 5 | 17 | 511 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | 0,78 | | |
| | 18 | 512 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 19 | 513 | 0,15 | 0,8 | 0,8 | 0,12 | 1 | | | |
| | 20 | 514 | 0,25 | 0,8 | 0,8 | 0,2 | 1 | | | |
| 6 | 21 | 611 | 0,5 | 0,8 | 0,8 | 0,4 | 1 | 0,72 | | |
| | 22 | 612 | 0,1 | 0,8 | 0,6 | 0,06 | 0 | | | |
| | 23 | 613 | 0,2 | 0,8 | 0,7 | 0,14 | 0 | | | |
| | 24 | 614 | 0,2 | 0,8 | 0,6 | 0,12 | 0 | | | |
| 7 | 25 | 711 | 0,3 | 0,8 | 0,8 | 0,24 | 1 | 0,77 | | |
| | 26 | 712 | 0,4 | 0,8 | 0,8 | 0,32 | 1 | | | |
| | 27 | 713 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |
| | 28 | 714 | 0,15 | 0,8 | 0,7 | 0,105 | 0 | | | |

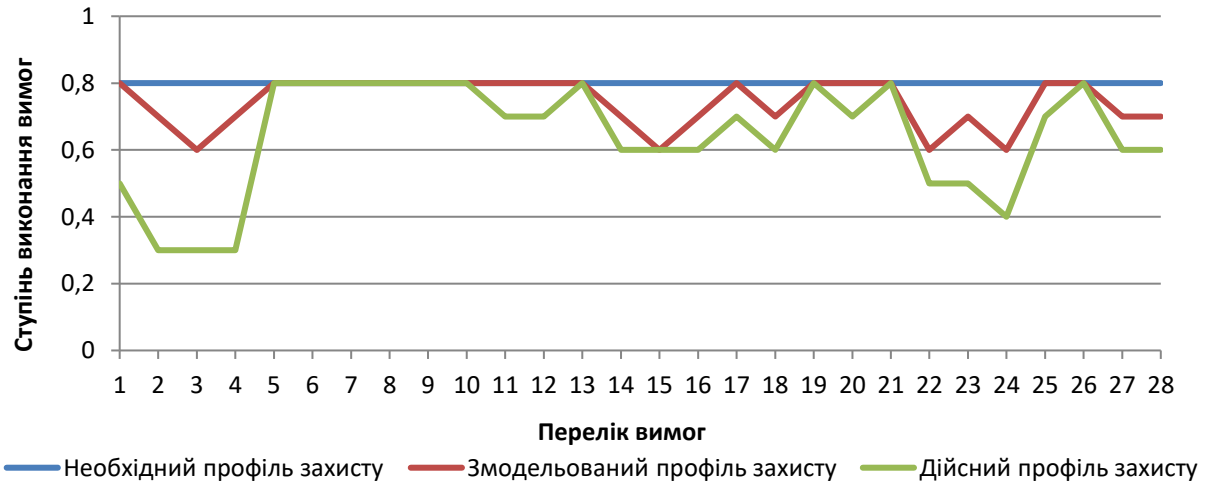


Рисунок Л.1 – Порівняння профілів керування системою захисту

Додаток М

*Таблиця М.1*

**Табличне подання узагальнених кількісних оцінок ступеню виконання вимог**

| | Напрямки захисту | | | | | $Q_{СЗІ}$ |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 2 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 3 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 4 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 5 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 6 | 0 | 0 | 0 | 0 | 1 | 0,2 |
| 7 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 8 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 9 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 10 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 11 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 12 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 13 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 14 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 15 | 1 | 1 | 1 | 0 | 1 | 0,8 |
| 16 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 17 | 1 | 1 | 0 | 0 | 0 | 0,4 |
| 18 | 1 | 1 | 1 | 1 | 1 | 1 |
| 19 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 20 | 1 | 0 | 0 | 1 | 1 | 0,6 |
| 21 | 1 | 1 | 0 | 0 | 0 | 0,4 |
| 22 | 1 | 0 | 1 | 1 | 0 | 0,6 |
| 23 | 0 | 1 | 1 | 0 | 1 | 0,6 |
| 24 | 0 | 1 | 0 | 1 | 0 | 0,4 |
| 25 | 1 | 1 | 0 | 0 | 0 | 0,4 |
| 26 | 1 | 1 | 0 | 0 | 0 | 0,4 |
| 27 | 0 | 0 | 1 | 0 | 0 | 0,2 |
| 28 | 0 | 0 | 1 | 0 | 0 | 0,2 |


Рисунок М.1 – Графічне зображення узагальнених кількісних оцінок ступеню виконання вимог

Додаток Н

*Таблиця Н.1*

**Матриця кількісних оцінок стану захисту інформації на ТОВ «Южмаш груп» при моделюванні**

| Етапи | Напрямки | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Захист об'єктів ІС | | | | Захист процесів та програм | | | | Захист каналів зв'язку | | | | Захист випромінювань | | | | Управляння системою захисту | | | |
| | Основи | база | структура | заходи | Засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби | база | структура | заходи | засоби |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Визначення інформації, що підлягає захисту | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 200 | Виявлення загроз та каналів витоку інформації | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 300 | Проведення оцінки уразливостей та ризиків | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 400 | Визначення вимог до СЗІ | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 500 | Здійснення вибору засобів захисту | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 600 | Запровадження обраних заходів та засобів | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 700 | Контроль цілісності та управляння захистом | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |