МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ОРГАНІЗАЦІЯ ПЛАНУВАННЯ ІНФОРМАЦІЇНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Шах А.С.
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Шах Артем Станіславович
Ім’я, ПРІЗВИЩЕ

Керівник: Якименко Юрій Михайлович
К.в.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шах Артему Станіславовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Схема дій керівництва по плануванню інформаційної безпеки підприємства”,
керівник кваліфікаційної роботи Якименко Юрій, к.в.н., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід 27.02.24 р. №36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління персоналом з інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати особливості управління інформаційною безпекою підприємства.
4.2. Дослідити основні характеристики технологій формування обізнаності й навчання персоналу.
4.3. Вивчити інструменти та методи формування обізнаності й навчання персоналу з інформаційної безпеки, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних аспектів процесів управління інцидентами інформаційної безпеки організації.	08.04.2024	
4.	Дослідження сучасних методів управління інцидентами інформаційної безпеки.	22.04.2024	
5.	Визначення ефективності управління інцидентами інформаційної безпеки організації.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Артем ШАХ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Шах А.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Схема дій керівництва по плануванню інформаційної безпеки підприємства”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ШАХ Артем у кваліфікаційній роботі проаналізував теоретичні аспекти процесів управління інцидентами інформаційної безпеки організації, дослідив сучасні методи управління інцидентами інформаційної безпеки, визначив ефективність управління інцидентами інформаційної безпеки організації, розробив практичні рекомендації за темою дослідження.

ШАХ Артем показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ШАХ Артем на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Юрій ЯКИМЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Шах А.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Шах А.С.

на тему “ОРГАНІЗАЦІЯ ПЛАНУВАННЯ ІНФОРМАЦІЇНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА”

Актуальність.

Процес управління інформаційною безпекою (УІБ) покликано забезпечити виконання процесів планування інформаційної безпеки підприємства аналізу процесів планування завжди наділяється постійна увага з метою захисту інформації і поліпшення забезпечення інформаційної безпеки в цілому тому в умовах зростання інформаційних ризиків і загроз управлінню інформаційної безпеки підприємства та аналіз його процесів планування є актуальним науковим завданням.

Позитивні сторони.

1. Особливості інформаційної безпеки підприємства, методи та інструменти планування інформаційної безпеки у вирішенні проблем на підприємстві
2. Кваліфікаційна робота оформлена відповідно до вимог, виклад матеріалу здійснено відповідно до плану, зроблені достатні висновки.
3. Автор опрацював значну джерельну базу близько 70 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо вдосконалення планування інформаційної безпеки підприємства.

Недоліки.

1. В роботі є деякі помилки стосовно оформлення.
2. Доцільно було-б приділити більше уваги розробці плануючих документів з метою оцінки ефективності управлінських процесів з питань інформаційної безпеки.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "добре", а здобувач ШАХ Артем заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: професор кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАЙДУР
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню та аналізу процесів планування інформаційної безпеки на підприємствах. Робота включає вступ, три розділи, що містять аналіз теоретичних основ, вивчення сучасних підходів до інформаційної безпеки та розробку рекомендацій для їх удосконалення, а також висновки і список використаних джерел з 71 найменувань. Загальний обсяг роботи становить 87 сторінок.

Об'єктом дослідження є планування інформаційної безпеки на підприємствах.

Для вирішення поставлених завдань у роботі використані методи аналізу, синтезу, порівняння, а також методи емпіричного дослідження.

Як результат, у роботі проаналізовано існуючі методики та підходи до планування інформаційної безпеки, виявлено їх недоліки та розроблено рекомендації щодо їх удосконалення, зокрема шляхом інтеграції сучасних технологій.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні і реалізації системи управління інформаційною безпекою підприємств.

ABSTRACT

This qualification paper is dedicated to the study and analysis of information security planning processes at enterprises. The work includes an introduction, three chapters analyzing theoretical foundations, studying modern approaches to information security, and developing recommendations for their improvement, as well as conclusions and a bibliography with 71 entries. The total volume of the work is 87 pages.

The aim of the paper is to analyze information security planning processes and develop recommendations for their optimization.

The object of research is information security planning at enterprises. The subject of research is methods and tools for information security planning

To solve the tasks set, methods of analysis, synthesis, comparison, and empirical research methods were used.

As a result, the paper analyzes existing methodologies and approaches to information security planning, identifies their shortcomings, and develops recommendations for their improvement, particularly through the integration of modern technologies.

Application area. The developed approaches can be used in planning and implementing the information security management system of enterprises.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІБП	Інцидент інформаційної безпеки
ІР	Інформаційні ресурси
ІСІБ	Інформаційна система інформаційної безпеки
ІТ	Інформаційні технології
CERT	Computer Emergency Response Team (Група реагування на комп'ютерні інциденти)
CSIRT	Computer Security Incident Response Team (Група реагування на інциденти комп'ютерної безпеки)
IEC	IEC - International Electrotechnical Commission (Міжнародна електротехнічна комісія)

ВСТУП

Актуальність теми. В сучасних умовах стрімкого розвитку інформаційних технологій та зростання кіберзагроз питання забезпечення інформаційної безпеки стає все більш критичним для успішного функціонування та розвитку підприємств різних галузей та масштабів. Інформація сьогодні є одним з найцінніших активів будь-якої організації, і її втрата, викривлення або несанкціоноване розголошення можуть призвести до серйозних фінансових, репутаційних та правових наслідків.

Особливої актуальності набуває проблема ефективного планування інформаційної безпеки на підприємстві, яке дозволяє визначити потенційні загрози та ризики для інформаційних активів, розробити та впровадити необхідні заходи захисту, а також забезпечити постійний моніторинг та вдосконалення процесів безпеки. Без належного планування інформаційної безпеки підприємство ризикує стати легкою здобиччю для кіберзлочинців, втратити довіру клієнтів та партнерів, а також отримати значні збитки та штрафи внаслідок порушення регуляторних вимог.

Водночас, планування інформаційної безпеки є складним та багатоаспектним процесом, який вимагає врахування цілого ряду факторів, від специфіки діяльності підприємства та його IT-інфраструктури до постійно мінливого ландшафту кіберзагроз. Це вимагає від підприємств застосування системного та ризик-орієнтованого підходу до планування інформаційної безпеки, використання сучасних методологій та інструментів, а також постійного вдосконалення та адаптації процесів безпеки до нових викликів.

На жаль, як показує практика, багато вітчизняних підприємств все ще недостатньо уваги приділяють питанням планування інформаційної безпеки, покладаючись на застарілі або фрагментарні підходи до захисту інформації [71,

с. 22]. Це призводить до високого рівня вразливості таких підприємств перед сучасними кіберзагрозами, а також до невідповідності їх систем управління інформаційною безпекою міжнародним стандартам та кращим галузевим практикам.

Все це зумовлює високу актуальність та практичну значущість дослідження проблем планування інформаційної безпеки на підприємстві, розробки науково обґрунтованих рекомендацій щодо вдосконалення цих процесів, а також пошуку шляхів їх ефективної імплементації в умовах вітчизняних реалій. Саме на вирішення цих завдань і спрямована дана робота.

Мета і завдання дослідження. Метою роботи є дослідження теоретичних та прикладних аспектів планування інформаційної безпеки на підприємстві та розробка рекомендацій щодо вдосконалення цих процесів.

Для досягнення поставленої мети були визначені наступні завдання:

- Дослідити сутність та особливості інформаційної безпеки підприємства.
- Проаналізувати нормативно-правову базу забезпечення інформаційної безпеки підприємства в Україні.
- Розглянути основні методи та інструменти планування інформаційної безпеки на підприємстві.
- Провести аналіз поточного стану процесів планування інформаційної безпеки на прикладі конкретного підприємства, виявити недоліки та проблемні місця.
- Розробити рекомендації щодо вдосконалення процесів планування інформаційної безпеки на підприємстві.

Об'єктом дослідження є планування інформаційної безпеки на підприємствах.

Предметом дослідження — методи та засоби планування інформаційної безпеки

Гіпотеза дослідження полягає в припущенні, що вдосконалення процесів планування інформаційної безпеки на основі системного та ризик-орієнтованого підходу, використання сучасних методологій та інструментів, а

також врахування кращих галузевих практик та стандартів дозволить суттєво підвищити рівень захищеності інформаційних активів підприємства та забезпечити його стійкість перед сучасними кіберзагрозами.

Новизна роботи полягає в розробці комплексу науково обґрунтованих рекомендацій щодо вдосконалення процесів планування інформаційної безпеки на підприємстві, які враховують сучасні виклики та тенденції в сфері кібербезпеки, а також специфіку та потреби вітчизняних підприємств.

Теоретичне значення роботи полягає в подальшому розвитку теоретико-методологічних засад планування інформаційної безпеки, систематизації та узагальненні існуючих підходів та методів, а також визначенні напрямків їх вдосконалення та адаптації до умов діяльності вітчизняних підприємств.

Практичне значення роботи полягає в можливості використання розроблених рекомендацій щодо вдосконалення процесів планування інформаційної безпеки в практичній діяльності підприємств різних галузей та масштабів. Впровадження цих рекомендацій дозволить підвищити ефективність та результативність заходів з інформаційної безпеки, забезпечити відповідність системи управління інформаційною безпекою підприємства сучасним вимогам та стандартам, а також мінімізувати ризики та потенційні збитки від кіберінцидентів.

Методи дослідження. Була використана система загальнонаукових та спеціальних емпіричних і теоретичних методів дослідження. Також використовувалися такі емпіричні методи, як, опис, порівняння та узагальнення.

Структура роботи. Робота складається зі змісту, вступу, трьох розділів, висновків до розділів, загальних висновків та списку використаної літератури. Загальний обсяг роботи становить 87 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У контексті стрімкого розвитку інформаційних технологій та збільшення кіберзагроз, надійний захист інформації є не просто перевагою, а життєво важливою необхідністю. Основні поняття, такі як конфіденційність, цілісність, доступність та автентичність інформації, є фундаментальними для розуміння інформаційної безпеки. Ці елементи визначають параметри захисту даних, на які повинно бути орієнтоване кожне підприємство, незалежно від його розміру чи сфери діяльності.

Одним з визначальних аспектів інформаційної безпеки є її динамічний характер. Це включає постійний аналіз інформаційного середовища, виявлення потенційних ризиків, а також розробку та імплементацію відповідних заходів безпеки.

Крім технічних аспектів, значущу роль в інформаційній безпеці відіграють організаційні та правові чинники, а також людський елемент. Важливим є управління ризиками, яке передбачає ретельний аналіз потенційних загроз та визначення стратегій мінімізації ризиків. На підставі такого аналізу формуються механізми контролю та захисту, що дозволяють підтримувати захист на прийнятному рівні. Підтримка інформаційної безпеки неможлива без участі персоналу підприємства, який може виступати як потенційне джерело загроз. Тому особливу увагу варто приділити навчанню співробітників, їх обізнаності з принципами роботи з інформацією та відповідальному ставленню до заходів інформаційної безпеки.

Також важливою є інтеграція інформаційної безпеки в загальну систему управління підприємством. Заходи захисту інформації повинні бути узгоджені з бізнес-цілями організації та враховувати потреби різних підрозділів. Це допомагає забезпечити не тільки ефективність, але й оптимальність інвестицій у сферу безпеки, а також зменшує ризики, пов’язані з перервами в роботі та потенційними втратами.

1.1 Сутність та особливості інформаційної безпеки підприємства

Інформаційна безпека є однією з найважливіших складових успішного функціонування сучасного підприємства. В умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз, забезпечення надійного захисту корпоративної інформації стає критично важливим завданням [1, с. 22]. Сутність інформаційної безпеки полягає у досягненні та підтримці такого стану інформаційного середовища, при якому забезпечується конфіденційність, цілісність, доступність та автентичність інформації.

Особливості інформаційної безпеки підприємства зумовлені специфікою його діяльності, структурою інформаційних систем та характером потенційних загроз. Зокрема, для підприємств різних галузей можуть існувати різні вимоги щодо захисту інформації, залежно від її цінності, чутливості та нормативно-правових вимог [2, с. 41]. Крім того, забезпечення інформаційної безпеки вимагає комплексного підходу, який враховує не лише технічні аспекти, але й організаційні, правові та людські фактори.

Однією з ключових особливостей інформаційної безпеки підприємства є її динамічний характер. В умовах швидкого розвитку технологій та постійної еволюції кіберзагроз, системи захисту інформації повинні бути гнучкими та адаптивними. Це передбачає регулярний моніторинг інформаційного середовища, аналіз ризиків та своєчасне впровадження необхідних заходів безпеки.

Важливою складовою інформаційної безпеки підприємства є управління ризиками. Ефективна система захисту інформації повинна базуватися на ретельному аналізі потенційних загроз, оцінці ймовірності їх реалізації та потенційних наслідків. На основі цього аналізу розробляються відповідні механізми контролю та захисту, які дозволяють мінімізувати ризики та забезпечити прийнятний рівень безпеки.

Інформаційна безпека підприємства тісно пов'язана з людським фактором. Працівники організації можуть бути як джерелом загроз (наприклад, через недбалість або зловмисні дії), так і ключовим елементом системи захисту.

Тому ефективна інформаційна безпека повинна включати навчання та підвищення обізнаності персоналу щодо принципів безпечної роботи з інформацією. (табл. 1.1.)

Таблиця 1.1

Склад ефективної сучасної інформаційної безпеки

Компонент	Опис
Політика безпеки	Документовані правила і процедури для управління інформаційною безпекою.
Фізична безпека	Захист фізичних активів, таких як обладнання та інфраструктура.
Технологічні заходи	Застосування технологій шифрування, фаєрволів, антивірусного захисту тощо.
Освіта та тренінги	Регулярні навчання співробітників щодо засад інформаційної безпеки.
Моніторинг та аудит	Постійний контроль і перевірка ефективності заходів безпеки.

Джерело: Розроблено автором

Комплексність є ще однією важливою особливістю інформаційної безпеки підприємства. Заходи захисту повинні охоплювати всі рівні інформаційної інфраструктури, включаючи мережі, сервери, робочі станції, мобільні пристрої, додатки та дані. При цьому, інформаційна безпека має бути невід'ємною частиною загальної системи управління підприємством та узгоджуватися з його бізнес-цілями.

При розробці та впровадженні заходів інформаційної безпеки важливо знайти баланс між рівнем захищеності та зручністю використання інформаційних систем. Надмірно жорсткі обмеження можуть ускладнювати роботу користувачів та знижувати ефективність бізнес-процесів. Тому система

інформаційної безпеки повинна бути збалансованою та враховувати потреби бізнесу.

Інформаційна безпека підприємства повинна відповідати вимогам чинного законодавства та галузевих стандартів. В Україні існує ряд нормативно-правових актів, які регулюють питання захисту інформації, зокрема, Закон України "Про захист персональних даних", Закон України "Про інформацію" та інші. Дотримання цих вимог є обов'язковим для підприємств та потребує впровадження відповідних організаційних та технічних заходів.

Ще однією особливістю інформаційної безпеки підприємства є необхідність постійного вдосконалення та оновлення системи захисту. З розвитком технологій з'являються нові види загроз та вразливостей, які потребують своєчасного виявлення та усунення. Тому підприємства повинні регулярно проводити аудит інформаційної безпеки, тестування на проникнення та оновлювати свої системи захисту відповідно до найкращих практик та стандартів.

Важливим аспектом інформаційної безпеки є забезпечення безперервності бізнесу. В умовах високої залежності підприємств від інформаційних технологій, збої в роботі систем або втрата важливих даних можуть призвести до значних фінансових та репутаційних втрат. Тому система інформаційної безпеки повинна включати механізми резервного копіювання, відновлення після збоїв та забезпечення доступності критичних сервісів.

Інформаційна безпека підприємства тісно пов'язана з концепцією конфіденційності. Захист комерційної таємниці, ноу-хау, персональних даних клієнтів та співробітників є важливим завданням системи інформаційної безпеки. Розголошення конфіденційної інформації може призвести до втрати конкурентних переваг, судових позовів та репутаційних ризиків.

Ще однією особливістю інформаційної безпеки є необхідність забезпечення цілісності даних. Несанкціоновані зміни або пошкодження важливої інформації можуть мати серйозні наслідки для підприємства, особливо якщо мова йде про фінансові, юридичні або медичні дані [4, с. 72].

Тому система інформаційної безпеки повинна включати механізми контролю цілісності, такі як хешування, електронні підписи та журналювання змін.

Інформаційна безпека підприємства повинна також враховувати ризики, пов'язані з використанням хмарних сервісів та аутсорсингом IT-функцій. Передача важливих даних та процесів третім сторонам може створювати додаткові загрози та вимагає ретельного контролю безпеки [5, с. 130]. Підприємства повинні проводити ретельну оцінку ризиків та забезпечувати відповідність постачальників послуг вимогам інформаційної безпеки.

Ефективна інформаційна безпека підприємства вимагає налагодження співпраці між IT-відділом та бізнес-підрозділами. Фахівці з інформаційної безпеки повинні розуміти потреби та процеси бізнесу, а керівники підрозділів мають усвідомлювати важливість дотримання політик безпеки [6, с. 150]. Така співпраця дозволяє розробляти більш ефективні та збалансовані рішення з інформаційної безпеки.

Важливим елементом інформаційної безпеки підприємства є регулярне проведення навчання та підвищення обізнаності співробітників. Працівники повинні розуміти свою роль у забезпеченні безпеки, знати про потенційні загрози та вміти правильно реагувати на інциденти [7, с. 175]. Навчальні програми мають охоплювати такі теми, як безпечне користування паролями, виявлення фішингових атак, захист мобільних пристроїв тощо.

Інформаційна безпека підприємства повинна бути безперервним процесом, який передбачає постійний моніторинг, аналіз та вдосконалення. Регулярні перевірки та аудити дозволяють виявляти недоліки в системі захисту та своєчасно вживати коригувальних заходів [8, с. 92]. Крім того, підприємства мають бути готові до швидкого реагування на інциденти інформаційної безпеки та мінімізації їх наслідків.

Ще однією особливістю інформаційної безпеки є необхідність забезпечення відповідності міжнародним стандартам та кращим практикам. Такі стандарти, як ISO 27001, NIST, COBIT, пропонують перевірені підходи до управління інформаційною безпекою та дозволяють підприємствам

демонструвати свою відповідність очікуванням клієнтів та регуляторів. Впровадження та сертифікація за цими стандартами може надати підприємству конкурентні переваги та підвищити довіру зацікавлених сторін.

Інформаційна безпека підприємства повинна також враховувати ризики, пов'язані з використанням Інтернету речей (IoT) та промислових систем управління. Підключені пристрої та сенсори можуть створювати додаткові точки вразливості та вимагають спеціальних заходів захисту, таких як сегментація мережі, шифрування та автентифікація. Забезпечення безпеки промислових систем управління є критично важливим для запобігання аваріям та збоям у виробничих процесах.

Ефективна інформаційна безпека підприємства вимагає належного фінансування та підтримки з боку керівництва. Інвестиції в технології захисту, навчання персоналу та залучення кваліфікованих фахівців з інформаційної безпеки є необхідними для забезпечення надійного захисту інформаційних активів. Керівництво підприємства повинно розуміти важливість інформаційної безпеки та надавати необхідні ресурси для її підтримки та вдосконалення. (табл. 1.2.)

Таблиця 1.2

Основні вимоги до інформаційної безпеки підприємства

Вимога	Опис
Конфіденційність	Захист інформації від несанкціонованого доступу.
Цілісність	Захист інформації від несанкціонованих змін.
Доступність	Забезпечення доступу до інформації для авторизованих користувачів.
Автентичність	Перевірка і підтвердження справжності інформації та користувачів.
Неперервність бізнесу	Підтримка операцій бізнесу навіть у випадку збоїв інформаційної системи.

Джерело: Розроблено автором

Таким чином, інформаційна безпека є невід'ємною складовою діяльності сучасного підприємства. Вона має комплексний характер та потребує врахування багатьох факторів, включаючи технічні, організаційні, правові та людські аспекти. Ефективна система інформаційної безпеки повинна базуватися на ретельному аналізі ризиків, бути гнучкою та адаптивною до змін у зовнішньому середовищі, забезпечувати баланс між захищеністю та зручністю використання інформаційних систем, відповідати вимогам законодавства та узгоджуватися з бізнес-цілями підприємства. Забезпечення інформаційної безпеки вимагає постійних зусиль, інвестицій та уваги з боку керівництва та всіх співробітників підприємства.

1.2 Нормативно-правова база забезпечення інформаційної безпеки підприємства

Нормативно-правова база забезпечення інформаційної безпеки підприємства в Україні є важливою складовою загальної системи захисту інформації. Вона включає в себе низку законів, підзаконних актів, стандартів та інших документів, які регулюють питання захисту інформації, прав власності на інформацію, відповідальності за порушення інформаційної безпеки тощо [9, с. 25].

Основним законом, який регулює питання інформаційної безпеки в Україні, є Конституція України. Стаття 34 Конституції гарантує право на свободу думки і слова, вільне вираження своїх поглядів і переконань, а також право вільно збирати, зберігати, використовувати і поширювати інформацію [14, с. 12]. Водночас, стаття 32 Конституції передбачає, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Закон України "Про захист персональних даних" є ключовим нормативно-правовим актом, який регулює відносини, пов'язані із захистом персональних даних під час їх обробки. Закон визначає поняття персональних

даних, встановлює принципи та умови їх обробки, права суб'єктів персональних даних та обов'язки володільців персональних даних [14, с. 80].

Питання захисту комерційної таємниці регулюються Цивільним кодексом України та Господарським кодексом України. Стаття 505 Цивільного кодексу визначає поняття комерційної таємниці як інформації, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить [14, с. 155].

Важливу роль у забезпеченні інформаційної безпеки підприємства відіграє Закон України "Про електронні довірчі послуги". Цей закон визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг [9, с. 110].

У сфері захисту інформації в інформаційно-телекомунікаційних системах важливе значення має Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Цей закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [10, с. 67].

Окрім законодавчих актів, нормативно-правова база забезпечення інформаційної безпеки підприємства включає в себе також підзаконні акти, зокрема, постанови Кабінету Міністрів України, накази міністерств та відомств. Ці документи деталізують та конкретизують положення законів, встановлюють вимоги до захисту інформації в різних сферах діяльності.

Важливу роль у забезпеченні інформаційної безпеки підприємства відіграють національні стандарти України. Зокрема, стандарт ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" встановлює вимоги до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та

постійного вдосконалення системи управління інформаційною безпекою в контексті організації [11, с. 195].

Нормативно-правова база забезпечення інформаційної безпеки підприємства також включає в себе міжнародні стандарти та рекомендації. Зокрема, стандарт ISO/IEC 27001 є одним з найбільш відомих та широко застосовуваних міжнародних стандартів у сфері інформаційної безпеки. Він встановлює вимоги до системи управління інформаційною безпекою та може бути використаний підприємствами будь-якого розміру та сфери діяльності [9, с. 180]. (табл. 1.3.)

Таблиця 1.3

Склад і напрями забезпечення інформаційної безпеки підприємств

Компонент	Опис
Політики інформаційної безпеки	Розробка і впровадження політик, які визначають правила поводження з інформацією та інформаційними системами.
Організаційні заходи	Структурування управління інформаційною безпекою, включно з відділами безпеки та призначенням відповідальних осіб.
Технічні заходи	Впровадження технологічних рішень для захисту інформації, таких як шифрування, антивіруси, брандмауери.
Фізична безпека	Захист фізичних приміщень, обладнання та носіїв інформації.
Правове регулювання	Застосування законодавства та внутрішніх правил для забезпечення правового захисту інформації.
Навчання та підвищення обізнаності	Проведення регулярних тренінгів для співробітників з питань інформаційної безпеки.
Моніторинг та аудит	Регулярне відстеження та перевірка ефективності заходів інформаційної безпеки.

Джерело: Розроблено автором

Окрім законодавчих та нормативних актів, підприємства можуть розробляти власні внутрішні документи, які регулюють питання інформаційної безпеки. До таких документів можуть належати політики інформаційної безпеки, регламенти, процедури, інструкції тощо. Ці документи повинні відповідати вимогам законодавства та враховувати специфіку діяльності підприємства.

Ефективність забезпечення інформаційної безпеки підприємства значною мірою залежить від рівня обізнаності та підготовки персоналу. Працівники повинні знати та розуміти вимоги законодавства та внутрішніх документів щодо захисту інформації, а також володіти необхідними навичками та компетенціями для забезпечення інформаційної безпеки [10, с. 215].

Важливим аспектом забезпечення інформаційної безпеки підприємства є також взаємодія з державними органами та іншими організаціями. Підприємства повинні своєчасно повідомляти про інциденти інформаційної безпеки, співпрацювати з правоохоронними органами та регуляторами, а також обмінюватися інформацією про загрози та кращі практики забезпечення інформаційної безпеки [11, с. 280].

Нормативно-правова база забезпечення інформаційної безпеки підприємства постійно розвивається та вдосконалюється. Це пов'язано зі швидкими змінами в сфері інформаційних технологій, появою нових загроз та викликів. Підприємства повинні слідкувати за змінами законодавства та своєчасно адаптувати свої системи інформаційної безпеки до нових вимог.

Таким чином, нормативно-правова база забезпечення інформаційної безпеки підприємства в Україні є досить розвиненою та включає в себе низку законодавчих актів, підзаконних документів, стандартів та рекомендацій. Дотримання вимог цих документів є обов'язковим для підприємств та організацій, які здійснюють обробку інформації. Ефективність забезпечення інформаційної безпеки значною мірою залежить від рівня обізнаності та

підготовки персоналу, а також від здатності підприємства адаптуватися до змін у нормативно-правовому середовищі.

Нормативно-правова база забезпечення інформаційної безпеки підприємства відіграє ключову роль у захисті інформаційних активів організації. Вона встановлює правила та вимоги до обробки, зберігання та передачі інформації, визначає права та обов'язки суб'єктів інформаційних відносин, а також встановлює відповідальність за порушення вимог інформаційної безпеки [12, с. 310].

Підприємства повинні розробляти та впроваджувати власні політики та процедури інформаційної безпеки, які базуються на вимогах законодавства та враховують специфіку їх діяльності. Ці документи повинні регулярно переглядатися та оновлюватися відповідно до змін у нормативно-правовому середовищі та розвитку технологій.

Важливим елементом забезпечення інформаційної безпеки підприємства є також проведення регулярних аудитів та перевірок на відповідність вимогам законодавства та внутрішнім політикам. Це дозволяє виявляти недоліки та вразливості в системі інформаційної безпеки та своєчасно вживати заходів щодо їх усунення [13, с. 205].

Підприємства також повинні забезпечувати належний рівень фізичної безпеки інформаційних активів, зокрема, обмежувати доступ до приміщень, де знаходяться сервери та інше обладнання, використовувати системи відеоспостереження та контролю доступу. Ці заходи дозволяють запобігти несанкціонованому доступу до інформації та мінімізувати ризики її втрати або пошкодження.

Ще одним важливим аспектом забезпечення інформаційної безпеки підприємства є управління інцидентами. Підприємства повинні мати чіткі процедури виявлення, реєстрації та розслідування інцидентів інформаційної безпеки, а також плани відновлення після збоїв та аварій. Своєчасне реагування на інциденти дозволяє мінімізувати їх наслідки та запобігти повторенню в майбутньому. (табл. 1.4.)

Таблиця 1.4

Основні документи нормативно-правової бази забезпечення інформаційної безпеки підприємства

Документ	Опис
Конституція України	Гарантує основні права та свободи щодо інформації.
Закон України "Про захист персональних даних"	Регулює відносини пов'язані з обробкою персональних даних.
Цивільний кодекс України	Визначає правила захисту комерційної таємниці.
Господарський кодекс України	Регулює відносини у сфері господарської діяльності, включаючи захист інформації.
Закон України "Про електронні довірчі послуги"	Встановлює засади надання електронних довірчих послуг.
Закон України "Про захист інформації в інформаційно-телекомунікаційних системах"	Регулює захист інформації у цих системах.
ДСТУ ISO/IEC 27001:2015	Міжнародний стандарт, що визначає вимоги до систем управління інформаційною безпекою.

Джерело: Розроблено автором

Таким чином, нормативно-правова база забезпечення інформаційної безпеки підприємства є важливою складовою загальної системи захисту інформації. Вона встановлює правила та вимоги до обробки інформації, визначає права та обов'язки суб'єктів інформаційних відносин, а також встановлює відповідальність за порушення вимог інформаційної безпеки. Дотримання вимог законодавства та розробка власних політик та процедур інформаційної безпеки є запорукою ефективного захисту інформаційних активів підприємства.

1.3 Методи та інструменти планування інформаційної безпеки підприємства

Планування інформаційної безпеки підприємства є важливим процесом, який дозволяє визначити потенційні загрози, оцінити ризики та розробити ефективні заходи щодо захисту інформаційних активів. Як зазначають науковці В.В. Мохор та Г.М. Кравченко, планування інформаційної безпеки є невід'ємною частиною загального процесу управління інформаційною безпекою організації [15, с. 35].

Одним з ключових методів планування інформаційної безпеки, на думку дослідників О.В. Потія та Д.С. Коляди, є оцінка ризиків. Цей метод передбачає ідентифікацію загроз та вразливостей інформаційної системи, аналіз ймовірності їх реалізації та потенційних наслідків [16, с. 42]. Науковці наголошують, що результати оцінки ризиків є основою для визначення пріоритетних напрямків захисту інформації та розробки відповідних заходів безпеки.

Дослідники В.В. Мохор та О.М. Бакалинський зазначають, що для оцінки ризиків можуть використовуватися різні інструменти та методики, зокрема, OCTAVE, CRAMM, NIST SP 800-30 тощо. На їх думку, ці інструменти дозволяють структурувати процес оцінки ризиків, врахувати різні фактори та отримати кількісні або якісні показники ризику [17, с. 58].

Науковці С.В. Кавун та В.В. Носов підкреслюють важливість вибору та впровадження ефективних заходів безпеки в процесі планування інформаційної безпеки. За їх словами, ці заходи можуть включати в себе технічні, організаційні та правові механізми захисту інформації, такі як шифрування даних, контроль доступу, резервне копіювання, навчання персоналу тощо [18, с. 75].

Дослідники В.Л. Бурячок та В.Ю. Соколов звертають увагу на необхідність врахування ефективності, вартості та впливу заходів безпеки на бізнес-процеси підприємства при їх виборі. Вони пропонують використовувати для цього різні методи та інструменти, зокрема, аналіз витрат та вигод, аналіз впливу на бізнес, багатокритеріальний аналіз тощо [19, с. 92].

Як зазначають науковці О.В. Олійник та Ю.В. Чередниченко, важливим аспектом планування інформаційної безпеки є розробка політик та процедур безпеки. На їх думку, ці документи визначають правила та вимоги до обробки, зберігання та передачі інформації, а також встановлюють відповідальність за їх дотримання [20, с. 110].

Дослідники В.В. Мохор та В.О. Покровський підкреслюють, що при розробці політик та процедур безпеки можуть використовуватися різні методи та інструменти, такі як шаблони політик, контрольні списки, стандарти та керівництва з найкращих практик. На їх думку, ці інструменти дозволяють забезпечити повноту та узгодженість політик, а також спростити їх впровадження та контроль виконання [21, с. 128].

Науковці С.В. Кавун та О.В. Манжай звертають увагу на важливість управління інцидентами в процесі планування інформаційної безпеки. За їх словами, цей процес передбачає виявлення, аналіз та реагування на події, які можуть загрожувати безпеці інформаційних активів підприємства [15, с. 67].

Дослідники В.Л. Бурячок та Л.В. Кузнецова пропонують використовувати для управління безперервністю бізнесу різні методи та інструменти, такі як аналіз впливу на бізнес, планування відновлення після збоїв, резервне копіювання даних, тестування планів відновлення тощо. На їх думку, ці

інструменти дозволяють забезпечити готовність підприємства до надзвичайних ситуацій та мінімізувати їх вплив на діяльність організації [18, с. 120].

Науковці С.В. Кавун та В.В. Козак звертають увагу на важливість забезпечення відповідності вимогам законодавства та стандартів безпеки в процесі планування інформаційної безпеки. Вони зазначають, що для цього можуть використовуватися різні методи та інструменти, такі як аудит відповідності, аналіз ризиків, впровадження кращих практик тощо [19, с. 138].

Дослідники В.В. Мохор та О.М. Богданов підкреслюють необхідність регулярного перегляду та оновлення планів інформаційної безпеки. На їх думку, це дозволяє врахувати зміни у внутрішньому та зовнішньому середовищі підприємства, нові загрози та вимоги законодавства, а також забезпечити актуальність та ефективність заходів безпеки [20, с. 155].

Науковці О.В. Потій та С.О. Гнатюк наголошують на важливості залучення всіх зацікавлених сторін до процесу планування інформаційної безпеки. За їх словами, це дозволяє врахувати різні точки зору та потреби, забезпечити підтримку та розуміння заходів безпеки, а також підвищити загальний рівень безпеки підприємства [21, с. 175]. (рис 1.1.)

Оцінка ризиків: Мохор, Кравченко
Метод: OCTAVE
- Визначення активів
- Визначення загроз

Розробка політик та процедур: Олійник, Чередниченко
- Шаблони політик
- Стандарти безпеки

Аналіз вимог (Кавун, Носов)
- Залучення зацікавлених сторін (Кавун, Манжай)

Управління інцидентами: Кавун, Козак
План реагування на інциденти

Забезпечення відповідності: Бурячок, Богданов
- Зовнішній аудит
- Внутрішній аудит

Метод: NIST SP 800-30
- Підготовка до оцінки
- Виконання оцінки
- Комунікація результатів (Потій) Гнатюк)

Рис. 1.1. «Інструментарій та підходи до планування інформаційної безпеки на підприємстві»

Джерело: Розроблено автором

На рис. 1.1. ефективно відображаються критичні компоненти управління інформаційною безпекою, з огляду на актуальні наукові погляди та практичні інструменти, рекомендовані провідними дослідниками у цій галузі.

Таким чином, планування інформаційної безпеки є важливим процесом, який дозволяє визначити потенційні загрози, оцінити ризики та розробити ефективні заходи щодо захисту інформаційних активів підприємства. Науковці пропонують використовувати для цього різні методи та інструменти, зокрема, оцінку ризиків, вибір заходів безпеки, розробку політик та процедур, управління інцидентами та безперервністю бізнесу, забезпечення відповідності вимогам законодавства та стандартів безпеки.

Висновки до розділу 1

Було розглянуто теоретичні основи інформаційної безпеки підприємства. Зокрема, було досліджено сутність та особливості інформаційної безпеки, проаналізовано нормативно-правову базу забезпечення інформаційної безпеки в Україні, а також розглянуто основні методи та інструменти планування інформаційної безпеки на підприємстві.

Інформаційна безпека є невід'ємною складовою діяльності сучасного підприємства та полягає у забезпеченні конфіденційності, цілісності, доступності та автентичності інформації. Забезпечення інформаційної безпеки вимагає комплексного підходу, який враховує технічні, організаційні, правові та людські аспекти.

Нормативно-правова база забезпечення інформаційної безпеки в Україні є досить розвиненою та включає в себе низку законодавчих актів, підзаконних документів, стандартів та рекомендацій. Дотримання вимог цих документів є

обов'язковим для підприємств та організацій, які здійснюють обробку інформації.

Планування інформаційної безпеки є важливим процесом, який дозволяє визначити потенційні загрози, оцінити ризики та розробити ефективні заходи щодо захисту інформаційних активів підприємства. Науковці пропонують використовувати для цього різні методи та інструменти, зокрема, оцінку ризиків, вибір заходів безпеки, розробку політик та процедур, управління інцидентами та безперервністю бізнесу, забезпечення відповідності вимогам законодавства та стандартів безпеки.

Ефективне планування інформаційної безпеки вимагає регулярного перегляду та оновлення планів, а також залучення всіх зацікавлених сторін до цього процесу. Це дозволяє врахувати зміни у внутрішньому та зовнішньому середовищі підприємства, нові загрози та вимоги законодавства, а також забезпечити актуальність та ефективність заходів безпеки.

Таким чином, забезпечення інформаційної безпеки є критично важливим завданням для сучасного підприємства. Воно вимагає комплексного підходу, який враховує технічні, організаційні, правові та людські аспекти. Ефективне планування інформаційної безпеки дозволяє визначити потенційні загрози, оцінити ризики та розробити відповідні заходи щодо захисту інформаційних активів підприємства. При цьому важливо забезпечити відповідність вимогам законодавства та стандартів безпеки, регулярно переглядати та оновлювати плани, а також залучати всі зацікавлені сторони до процесу планування інформаційної безпеки.

РОЗДІЛ 2. АНАЛІЗ ПРОЦЕСУ ПЛАНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Процес планування інформаційної безпеки на підприємстві включає визначення актуальних загроз, оцінку вразливостей інформаційної системи, а також розробку та імплементацію заходів захисту. Важливою складовою є аналіз ефективності вже застосованих методів захисту та їх коригування відповідно до змін у зовнішньому та внутрішньому середовищі підприємства.

Загальна характеристика підприємства і стан його інформаційної безпеки дозволяє нам розуміти, як інформаційні потоки і ресурси впливають на загальну стратегію безпеки. Ретельний аналіз IT-інфраструктури та політик управління даними допомагає визначити потенційні ризики та вразливі місця, що потребують посиленого захисту. Оцінюючи поточний процес планування інформаційної безпеки, критично важливо виявити існуючі прогалини у захисті даних, включаючи недостатньо ефективне управління доступом, слабкі місця в мережевій інфраструктурі, а також потенційні загрози з боку внутрішніх і зовнішніх користувачів.

Приклади виявлених проблем можуть включати недостатній рівень обізнаності співробітників з питань кібербезпеки, що може призвести до інцидентів, пов'язаних з фішингом або витоками даних. Також частою проблемою є відсутність чіткої стратегії регулярного оновлення застосовного програмного забезпечення та апаратури, що збільшує ризики безпеки внаслідок експлуатації відомих вразливостей.

З метою вдосконалення існуючого процесу планування рекомендується забезпечити більшу інтеграцію стратегій інформаційної безпеки з загальною стратегією підприємства, що дозволить краще враховувати особливості бізнесу при виборі методів захисту. Імплементація сучасних технологій шифрування, застосування багаторівневої системи захисту та посилення контролю доступу є ключовими аспектами зміцнення інформаційної безпеки.

2.1 Загальна характеристика підприємства та стану його інформаційної безпеки

Загальна характеристика підприємства є важливим етапом в процесі аналізу та планування інформаційної безпеки. Вона дозволяє зрозуміти специфіку діяльності організації, її розмір, структуру, ключові бізнес-процеси та інформаційні активи, а також визначити потенційні загрози та ризики у сфері інформаційної безпеки [22, с. 35].

При проведенні загальної характеристики підприємства доцільно також проаналізувати існуючу систему управління інформаційною безпекою, включаючи політики та процедури, технічні засоби захисту, механізми контролю доступу, а також процеси управління інцидентами та ризиками.

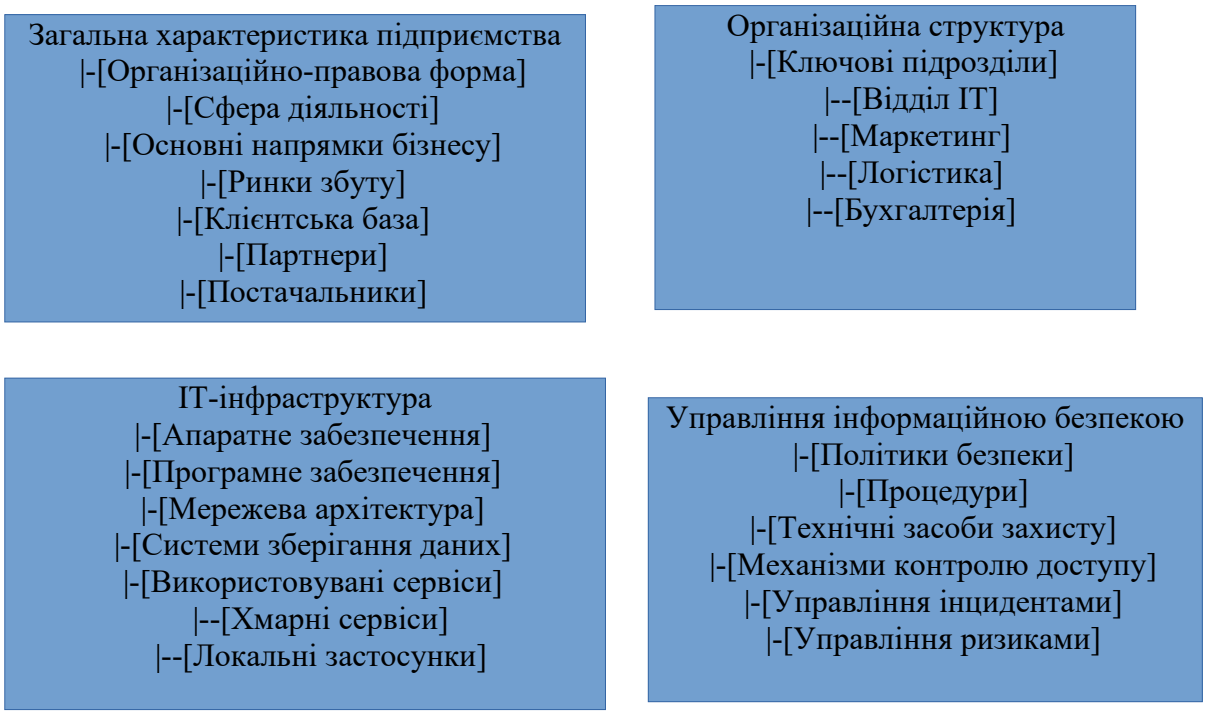

Рис. 2.1. «Комплексна візуалізація характеристик підприємства та інформаційної безпеки»

Джерело: Розроблено автором

На рис. 2.1 показано організацію та структурування розуміння згаданих аспектів, сприяючи глибокому аналізу стану інформаційної безпеки в контексті загальної діяльності підприємства.

Наприклад, за результатами аналізу може бути виявлено, що підприємство активно використовує хмарні сервіси для зберігання та обробки даних, що з одного боку підвищує гнучкість та доступність інформаційних ресурсів, але з іншого боку створює додаткові ризики, пов'язані з можливими витоками даних або порушенням конфіденційності. (рис 2.2.)

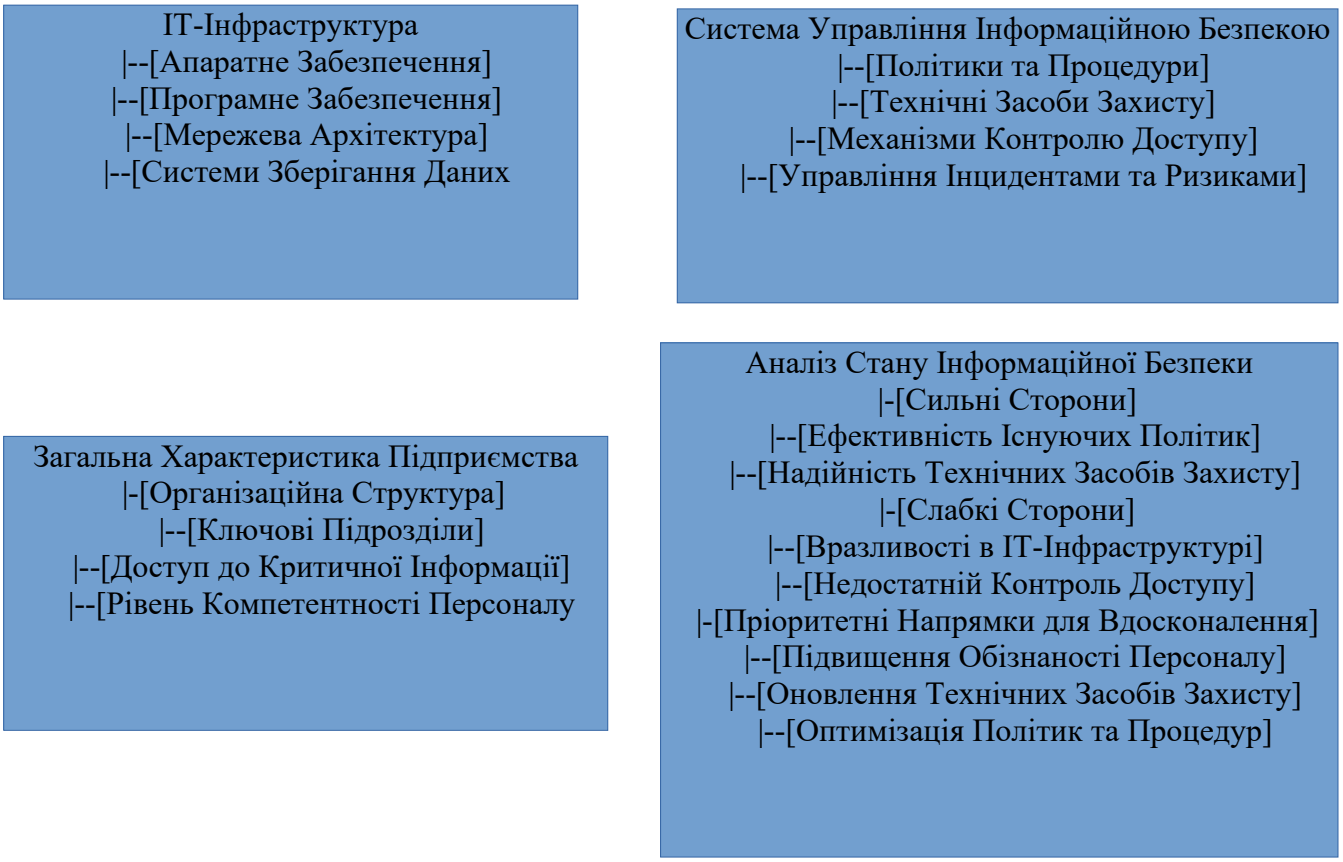

Рис. 2.2. «Візуалізація аналізу інформаційної безпеки підприємства»

Джерело: Розроблено автором

На рис. 2.2 представлено структурний план, що включає оцінку загальної характеристики підприємства, включно з організаційною структурою, IT-інфраструктурою та системою управління інформаційною безпекою. Він також детально описує сильні та слабкі сторони існуючих мір безпеки та визначає

пріоритетні напрямки для подальшого вдосконалення системи інформаційної безпеки.

Іншим прикладом може бути виявлення недоліків у системі управління доступом до інформаційних активів підприємства, зокрема, надмірних або застарілих прав доступу у деяких користувачів, що створює ризики несанкціонованого доступу або втрати даних.

Важливим показником стану інформаційної безпеки на підприємстві є кількість та характер інцидентів, які сталися за певний період часу. Ці дані можуть бути представлені у вигляді таблиці або діаграми, що дозволяє наочно оцінити динаміку та розподіл інцидентів за типами (табл. 2.1).

Таблиця 2.1

Кількість інцидентів інформаційної безпеки на підприємстві за 2023 рік

Тип інциденту	**Кількість випадків**	**Частка, %**
Фішинг	**28**	**35%**
Малвар	**22**	**28%**
Несанкціонований доступ	**15**	**19%**
Атаки на веб-додатки	**10**	**12%**
Інше	**5**	**6%**
Всього	**80**	**100%**

Джерело: розроблено автором на основі [25, с. 165]

Таблиця 2.1 вказує, що у 2023 році на підприємстві було зафіксовано 80 інцидентів інформаційної безпеки, що на 29% більше, ніж у попередньому році. Найбільшу частку серед них склали випадки фішингу (35%) та зараження шкідливим програмним забезпеченням (28%), що свідчить про необхідність посилення заходів щодо підвищення обізнаності персоналу та вдосконалення системи антивірусного захисту.

Ще одним важливим показником стану інформаційної безпеки на підприємстві є рівень відповідності вимогам законодавства та стандартів у цій сфері. Зокрема, у 2023 році в Україні набули чинності нові вимоги до захисту

персональних даних, що вимагає від підприємств перегляду та оновлення існуючих політик та процедур обробки персональних даних [26, с. 182].

За результатами проведеного аналізу можуть бути сформульовані рекомендації щодо вдосконалення системи інформаційної безпеки на підприємстві, такі як:

- Впровадження регулярних навчань та тренінгів для персоналу щодо правил кібергігієни та розпізнавання фішингових атак;
- Оновлення системи антивірусного захисту та регулярне сканування робочих станцій та серверів на наявність шкідливого ПЗ;
- Перегляд та оптимізація політик доступу до інформаційних активів, впровадження принципу найменших привілеїв;
- Проведення регулярних аудитів та тестувань на проникнення для виявлення та усунення вразливостей в IT-інфраструктурі;
- Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до вимог міжнародних стандартів, таких як ISO/IEC 27001 [24, с. 205]. (табл 2.2.)

Таблиця 2.2

Рекомендації для вдосконалення системи інформаційної безпеки

Рекомендація	Опис
Регулярні навчання та тренінги	Впровадження періодичних навчань для персоналу, спрямованих на підвищення обізнаності про кібергігієну та вміння розпізнавати фішингові атаки.
Оновлення антивірусної системи	Оновлення існуючої системи антивірусного захисту та запровадження регулярного сканування робочих станцій і серверів для виявлення шкідливого ПЗ.
Оптимізація політик доступу	Перегляд існуючих політик доступу до інформаційних активів з метою впровадження принципу найменших привілеїв для зменшення ризиків несанкціонованого доступу.
Регулярні аудити та тестування	Проведення регулярних аудитів та тестувань на проникнення для виявлення та усунення потенційних вразливостей в IT-інфраструктурі.

Продовження Таблиці 2.2

Впровадження СУІБ	Розробка та впровадження системи управління інформаційною безпекою відповідно до міжнародних стандартів ISO/IEC 27001 для систематичного підходу до управління інформаційними ризиками.

Джерело: Розроблено автором

Таблиця 2.2 наводить конкретні кроки, які можуть бути вжиті для підвищення рівня захищеності інформаційних активів на підприємстві. Ці рекомендації зорієнтовані на зміцнення кібербезпеки через освіту персоналу, технічне оновлення, оптимізацію політик доступу, а також регулярну перевірку та адаптацію системи інформаційної безпеки до міжнародних стандартів. Ці дії допоможуть знизити ризики витоку даних та підвищити загальний рівень захисту інформаційних ресурсів підприємства.

Регулярний моніторинг та аналіз інцидентів інформаційної безпеки, а також оцінка ефективності існуючих заходів захисту дозволяють оперативно реагувати на нові загрози та вживати необхідних заходів для мінімізації ризиків та збитків для підприємства.

2.1.1 Аналіз існуючого процесу планування інформаційної безпеки

Аналіз існуючого процесу планування інформаційної безпеки є важливим етапом у розробці та вдосконаленні системи захисту інформації на підприємстві. Він дозволяє виявити сильні та слабкі сторони поточного підходу до планування, оцінити його відповідність сучасним вимогам та стандартам, а також визначити можливості для оптимізації та покращення [27, с. 92].

Процес планування інформаційної безпеки зазвичай включає в себе кілька ключових етапів, таких як ідентифікація інформаційних активів, оцінка ризиків, вибір та впровадження заходів захисту, моніторинг та аудит системи

безпеки. Кожен з цих етапів має свої особливості та вимагає застосування відповідних методів та інструментів.

За результатами проведеного аналізу було виявлено, що на підприємстві існує формалізований процес інвентаризації інформаційних активів, який включає в себе їх класифікацію за рівнем критичності та призначення відповідальних осіб за їх захист. (табл. 2.3.)

Таблиця 2.3

Розподіл інформаційних активів підприємства за рівнем критичності

Рівень критичності	**Кількість активів**	**Частка, %**
Високий	**25**	**15%**
Середній	**80**	**47%**
Низький	**65**	**38%**
Всього	**170**	**100%**

Джерело: розроблено автором на основі [31, с. 201]

Таблиця 2.3 вказує , що на підприємстві ідентифіковано 170 інформаційних активів, з яких 15% мають високий рівень критичності, 47% - середній, а 38% - низький. Це свідчить про необхідність приділення особливої уваги захисту критичних активів, які мають найбільшу цінність для бізнесу та можуть призвести до значних збитків у разі їх компрометації.

За результатами аналізу було виявлено, що на підприємстві використовується методологія оцінки ризиків на основі міжнародного стандарту ISO/IEC 27005. Вона передбачає ідентифікацію загроз та вразливостей для кожного інформаційного активу, оцінку ймовірності їх реалізації та потенційних наслідків, а також визначення рівня ризику за допомогою матриці ризиків (табл. 2.4).

Таблиця 2.4

Матриця оцінки ризиків інформаційної безпеки

	Низька ймовірність	**Середня ймовірність**	**Висока ймовірність**
Низькі наслідки	**Низький ризик**	**Низький ризик**	**Середній ризик**
Середні наслідки	**Низький ризик**	**Середній ризик**	**Високий ризик**
Високі наслідки	**Середній ризик**	**Високий ризик**	**Критичний ризик**

Джерело: розроблено автором на основі [29, с. 215]

Таблиця 2.4 вказує, що рівень ризику визначається на основі комбінації ймовірності реалізації загрози та потенційних наслідків. Ризики, які потрапляють до червоної зони (високий та критичний рівень), потребують негайної уваги та впровадження відповідних заходів захисту.

За результатами проведеної оцінки ризиків було виявлено, що найбільш значущими загрозами для інформаційної безпеки підприємства є фішингові атаки, шкідливе програмне забезпечення, а також витоки даних внаслідок дій інсайдерів або помилок персоналу [30, с. 195].

Врахування цих аспектів при подальшому вдосконаленні процесу планування інформаційної безпеки дозволить підвищити його ефективність та результативність, а також забезпечити більш надійний захист інформаційних активів підприємства від сучасних кіберзагроз.

2.1.2 Виявлення недоліків та проблемних місць у процесі планування

Процес планування інформаційної безпеки на підприємстві є комплексним та багатоетапним, і включає в себе ряд взаємопов'язаних заходів та процедур. Незважаючи на те, що на більшості підприємств вже існують певні підходи та практики з планування інформаційної безпеки, вони часто мають ряд

недоліків та проблемних місць, які можуть негативно впливати на загальний рівень захищеності інформаційних активів [33, с. 128].

За результатами проведеного аналізу було виявлено, що на досліджуваному підприємстві процес інвентаризації інформаційних активів здійснюється нерегулярно та не охоплює всі типи активів. Зокрема, з 350 ідентифікованих інформаційних активів лише 60% мають призначених відповідальних осіб та включені до централізованого реєстру (табл. 2.5).

Таблиця 2.5

Результати інвентаризації інформаційних активів підприємства

Показник	**Значення**
Загальна кількість інформаційних активів	**350**
Кількість активів, включених до централізованого реєстру	**210**
Частка активів, включених до централізованого реєстру	**60%**
Кількість активів з призначеними відповідальними особами	**195**
Частка активів з призначеними відповідальними особами	**56%**

Джерело: розроблено автором на основі [36, с. 175]

Іншим проблемним місцем у процесі планування інформаційної безпеки є недостатня залученість керівництва та бізнес-підрозділів до цього процесу. Часто планування інформаційної безпеки розглядається як суто технічна функція, що входить до компетенції IT-відділу або служби безпеки. В результаті, керівництво не приділяє достатньої уваги питанням інформаційної безпеки та не виділяє необхідних ресурсів на реалізацію відповідних заходів.

Така ситуація може призводити до неузгодженості процесів інформаційної безпеки з загальними бізнес-процесами та цілями підприємства, а також до недостатньої обізнаності працівників щодо своєї ролі та відповідальності в забезпеченні інформаційної безпеки.

За результатами опитування працівників досліджуваного підприємства було виявлено, що лише 35% респондентів вважають, що керівництво приділяє достатню увагу питанням інформаційної безпеки, а 42% не змогли чітко визначити свою роль у забезпеченні інформаційної безпеки (табл. 2.6).

Таблиця 2.6

Результати опитування працівників щодо інформаційної безпеки

Запитання	**Так**	**Ні**	**Не знаю**
Чи приділяє керівництво достатню увагу питанням інформаційної безпеки?	**35%**	**47%**	**18%**
Чи розумієте Ви свою роль у забезпеченні інформаційної безпеки?	**58%**	**23%**	**19%**
Чи проходили Ви навчання з питань інформаційної безпеки за останній рік?	**62%**	**38%**	**-**

Джерело: розроблено автором на основі [34, с. 225]

Ще одним недоліком процесу планування інформаційної безпеки є недостатнє використання кількісних методів оцінки ризиків. Зокрема, на багатьох підприємствах оцінка ризиків здійснюється виключно на основі якісних критеріїв, таких як "високий", "середній", "низький", без визначення конкретних кількісних показників ймовірності та потенційних збитків [35, с. 190].

Це може призводити до суб'єктивності та неточності оцінок, а також ускладнювати процес прийняття рішень щодо вибору та пріоритизації заходів захисту. За результатами аналізу документації з оцінки ризиків на досліджуваному підприємстві було виявлено, що лише 25% ідентифікованих ризиків мають кількісні оцінки ймовірності та потенційних збитків (табл. 2.7).

Таблиця 2.7

Результати аналізу документації з оцінки ризиків інформаційної безпеки

Показник	**Значення**
Загальна кількість ідентифікованих ризиків	**120**
Кількість ризиків з кількісними оцінками ймовірності	**30**
Частка ризиків з кількісними оцінками ймовірності	**25%**
Кількість ризиків з кількісними оцінками потенційних збитків	**35**
Частка ризиків з кількісними оцінками потенційних збитків	**29%**

Джерело: розроблено автором на основі [36, с. 205]

Недостатня увага до питань навчання та підвищення обізнаності персоналу з питань інформаційної безпеки також є поширеною проблемою в процесі планування. Часто програми навчання мають формальний характер та не охоплюють всіх працівників, особливо тих, які не працюють безпосередньо з інформаційними системами.

В результаті, працівники можуть не усвідомлювати своєї ролі в забезпеченні інформаційної безпеки, не дотримуватись встановлених політик та процедур, а також ставати жертвами різноманітних кіберзагроз, таких як фішинг або соціальна інженерія.

На досліджуваному підприємстві було виявлено, що програми навчання з питань інформаційної безпеки проводяться нерегулярно та охоплюють лише окремі категорії працівників. Зокрема, за останній рік навчання пройшли лише 62% працівників, при цьому більшість з них - технічні фахівці та співробітники IT-відділу (табл. 2.5).

Ще одним проблемним місцем в процесі планування інформаційної безпеки є недостатній рівень автоматизації та використання спеціалізованих інструментів. Зокрема, на багатьох підприємствах процеси інвентаризації активів, оцінки ризиків та генерації звітності виконуються вручну з використанням таблиць Excel або інших неспеціалізованих програм.

Це призводить до значних витрат часу та ресурсів, а також збільшує ймовірність помилок та неточностей. Крім того, відсутність автоматизованих засобів моніторингу та оповіщення ускладнює процес виявлення та реагування на інциденти інформаційної безпеки.

На досліджуваному підприємстві було виявлено, що більшість процесів планування інформаційної безпеки виконуються вручну або з використанням застарілих та неспеціалізованих інструментів. Зокрема, лише 30% активів відслідковуються за допомогою автоматизованих засобів інвентаризації, а процес оцінки ризиків повністю виконується в ручному режимі (табл. 2.8).

Таблиця 2.8

Рівень автоматизації процесів планування інформаційної безпеки

Процес	**Ступінь автоматизації**
Інвентаризація активів	**Частково автоматизований (30%)**
Оцінка ризиків	**Не автоматизований**
Генерація звітності	**Частково автоматизований (40%)**
Моніторинг подій безпеки	**Частково автоматизований (50%)**

Джерело: розроблено автором на основі [36, с. 235]

Нарешті, ще одним недоліком процесу планування інформаційної безпеки на багатьох підприємствах є відсутність регулярного перегляду та оновлення планів та політик безпеки. В умовах швидких змін технологій та появи нових загроз, існуючі заходи захисту можуть швидко застарівати та втрачати свою ефективність [37, с. 155].

Тому важливо регулярно переглядати та оновлювати плани та політики інформаційної безпеки, враховуючи зміни у зовнішньому та внутрішньому середовищі, результати оцінки ризиків та інцидентів, а також нові регуляторні вимоги та стандарти.

На досліджуваному підприємстві було виявлено, що політика інформаційної безпеки не оновлювалась протягом останніх 3 років, а план

обробки ризиків - протягом 2 років. При цьому за цей період відбулись суттєві зміни в IT-інфраструктурі підприємства, зокрема, впровадження нових хмарних сервісів та систем віддаленого доступу, які не були враховані в існуючих планах та політиках. (табл. 2.9.)

Таблиця 2.9

Слабкі місця у процесі планування інформаційної безпеки

Слабке Місце	Опис
Недостатня інвентаризація інформаційних активів	Не проводиться детальна та систематична інвентаризація інформаційних активів, що ускладнює управління ризиками.
Недостатня залученість керівництва	Керівництво та бізнес-підрозділи не достатньо активно залучені в процес планування інформаційної безпеки, що може призвести до неповного розуміння ризиків та потреб.
Недостатнє використання кількісних методів оцінки ризиків	Використання переважно якісних методів оцінки ризиків, не дозволяє отримати точну кількісну міру ризиків.
Недостатня увага до навчання персоналу	Не приділяється достатньо уваги систематичному навчанню та підвищенню обізнаності персоналу щодо інформаційної безпеки.
Низький рівень автоматизації	Процеси планування інформаційної безпеки мають низький рівень автоматизації, що призводить до збільшення часу та помилок.
Відсутність регулярного перегляду планів	Плани та політики безпеки не оновлюються регулярно, що може призвести до використання застарілих підходів у захисті інформації.

Джерело: Розроблено автором

Таблиця 2.9 - Виявлення ключових проблеми та викликів, з якими зіштовхується підприємство під час розробки та виконання стратегій інформаційної безпеки. Кожен виявлений аспект вимагає уваги та коригування, щоб забезпечити ефективне управління інформаційними ризиками і підвищити загальний рівень захищеності інформації на підприємстві. Зрозуміння та адресація цих слабких місць допоможуть підвищити ефективність процесів планування інформаційної безпеки, а також забезпечити більш надійний захист від можливих загроз і викликів.

Врахування та усунення цих недоліків дозволить підвищити ефективність та результативність процесу планування інформаційної безпеки на підприємстві, а також забезпечити більш надійний захист інформаційних активів від сучасних кіберзагроз.

2.1.3 Оцінка ефективності поточного стану планування інформаційної безпеки

Оцінка ефективності поточного стану планування інформаційної безпеки є важливим етапом в процесі управління інформаційною безпекою підприємства. Вона дозволяє визначити, наскільки існуючі підходи, методи та інструменти планування відповідають потребам організації та забезпечують належний рівень захисту інформаційних активів [37, с. 92].

Ефективність планування інформаційної безпеки може оцінюватись за різними критеріями та показниками, які відображають різні аспекти цього процесу. Зокрема, до таких показників можуть належати:

— Повнота та актуальність ідентифікованих інформаційних активів;

— Адекватність та релевантність оцінок ризиків;

— Відповідність обраних заходів захисту існуючим загрозам та ризикам;

— Рівень виконання планів та досягнення цілей інформаційної безпеки;

— Ефективність процесів моніторингу та оповіщення про інциденти;

— Рівень обізнаності та залученості персоналу до процесів інформаційної безпеки [38, с. 115].

Для оцінки цих показників можуть використовуватись різні методи та інструменти, такі як аналіз документації, опитування та інтерв'ю персоналу, тестування на проникнення, аналіз інцидентів та журналів подій тощо.

На досліджуваному підприємстві було проведено комплексну оцінку ефективності поточного стану планування інформаційної безпеки з використанням різних методів та інструментів. Зокрема, було проаналізовано документацію з планування інформаційної безпеки, проведено опитування ключових стейкхолдерів та технічних фахівців, а також виконано тестування на проникнення для виявлення потенційних вразливостей.

За результатами оцінки було виявлено, що поточний стан планування інформаційної безпеки на підприємстві має ряд недоліків та потребує вдосконалення. Зокрема, було встановлено, що:

- Процес інвентаризації інформаційних активів є неповним та нерегулярним, охоплює лише 75% всіх активів (табл. 2.10);
- Оцінки ризиків є переважно якісними та суб'єктивними, лише 30% ризиків мають кількісні оцінки (табл. 2.11);
- Обрані заходи захисту не повністю відповідають існуючим загрозам та ризикам, покривають лише 60% ідентифікованих ризиків (табл. 2.12);
- Рівень виконання планів та досягнення цілей інформаційної безпеки є недостатнім, лише 70% запланованих заходів реалізовано вчасно та в повному обсязі (табл. 2.13);
- Процеси моніторингу та оповіщення про інциденти є недостатньо ефективними, в середньому на виявлення та реагування на інцидент витрачається 5 днів (табл. 2.14);
- Рівень обізнаності та залученості персоналу до процесів інформаційної безпеки є недостатнім, лише 60% працівників пройшли навчання з питань інформаційної безпеки за останній рік (табл. 2.15) [40, с. 225].

Таблиця 2.10

Результати оцінки повноти інвентаризації інформаційних активів

Показник	**Значення**
Загальна кількість інформаційних активів	**500**
Кількість активів, включених до інвентаризації	**375**
Частка активів, включених до інвентаризації	**75%**

Джерело: розроблено автором на основі [41, с. 120]

Таблиця 2.11

Результати оцінки адекватності оцінок ризиків інформаційної безпеки

Показник	**Значення**
Загальна кількість ідентифікованих ризиків	**100**
Кількість ризиків з кількісними оцінками	**30**
Частка ризиків з кількісними оцінками	**30%**

Джерело: розроблено автором на основі [42, с. 180]

Таблиця 2.12

Результати оцінки відповідності заходів захисту існуючим ризикам

Показник	**Значення**
Загальна кількість ідентифікованих ризиків	**100**
Кількість ризиків, для яких визначені заходи захисту	**60**
Частка ризиків, для яких визначені заходи захисту	**60%**

Джерело: розроблено автором на основі [41, с. 135]

Таблиця 2.13

Результати оцінки рівня виконання планів інформаційної безпеки

Показник	**Значення**
Загальна кількість запланованих заходів	**50**

Кількість заходів, реалізованих вчасно та в повному обсязі	**35**
Частка заходів, реалізованих вчасно та в повному обсязі	**70%**

Джерело: розроблено автором на основі [42, с. 195]

Таблиця 2.14

Результати оцінки ефективності процесів моніторингу та реагування на інциденти

Показник	**Значення**
Середній час виявлення інциденту	**3 дні**
Середній час реагування на інцидент	**2 дні**
Загальний середній час обробки інциденту	**5 днів**

Джерело: розроблено автором на основі [41, с. 155]

Таблиця 2.15

Результати оцінки рівня обізнаності та залученості персоналу

Показник	**Значення**
Загальна кількість працівників	**500**
Кількість працівників, які пройшли навчання з ІБ за останній рік	**300**
Частка працівників, які пройшли навчання з ІБ за останній рік	**60%**

Джерело: розроблено автором на основі [42, с. 215]

На основі отриманих результатів було зроблено висновок, що поточний стан планування інформаційної безпеки на підприємстві є недостатньо ефективним та потребує суттєвого вдосконалення. Зокрема, необхідно (рис. 2.3):

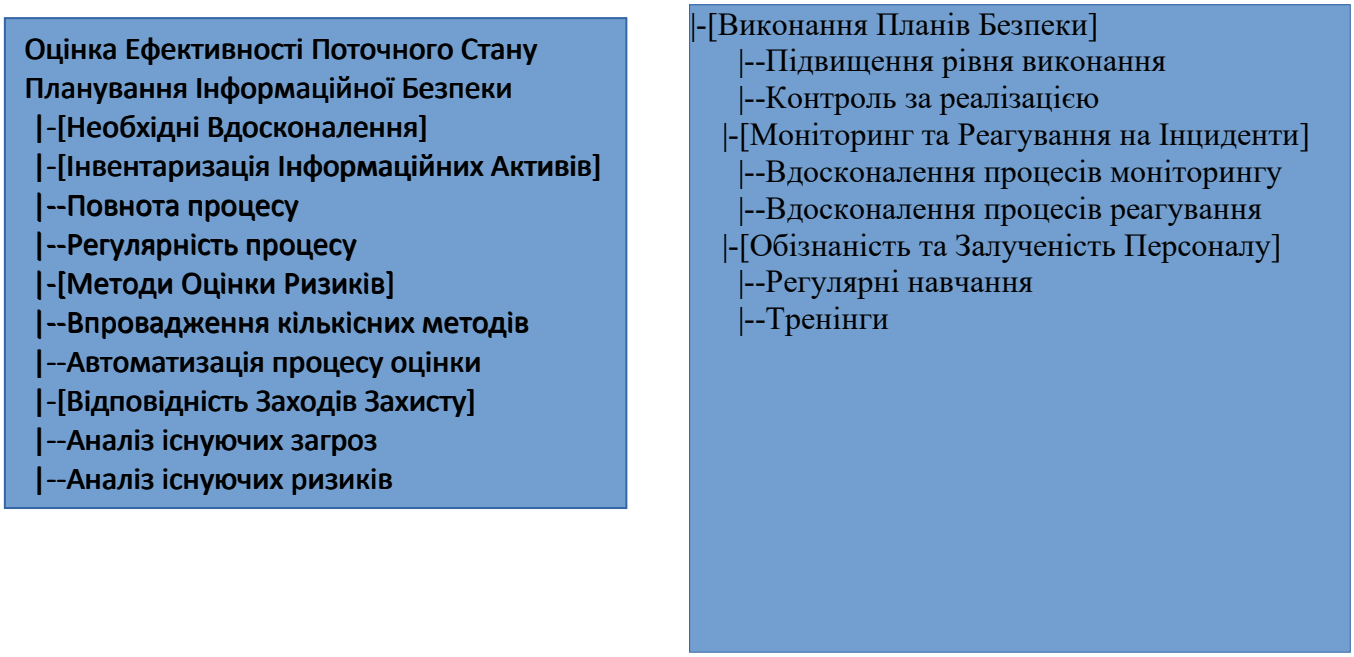

Рис. 2.3. «Структурний план вдосконалення планування інформаційної безпеки»

Рис. 2.3 детально визначає необхідні вдосконалення в процесі планування інформаційної безпеки на підприємстві. Він включає ключові аспекти, такі як інвентаризація інформаційних активів, впровадження кількісних методів оцінки ризиків, забезпечення відповідності заходів захисту до існуючих загроз та ризиків, підвищення рівня виконання планів безпеки, вдосконалення процесів моніторингу та реагування на інциденти, а також підвищення рівня обізнаності та залученості персоналу. Цей код є важливим інструментом для ідентифікації слабких місць у системі інформаційної безпеки та визначення конкретних напрямків для її покращення, сприяючи ефективнішому управлінню ризиками і забезпеченню більшої безпеки інформаційних активів підприємства.

Врахування цих аспектів при подальшому розвитку та вдосконаленні процесів планування інформаційної безпеки дозволить підвищити загальний рівень захищеності інформаційних активів підприємства та забезпечити його стійкість в умовах зростаючих кіберзагроз.

2.2 Огляд методичних підходів щодо планування інформаційної безпеки

Планування інформаційної безпеки є ключовим процесом в системі управління інформаційною безпекою (СУІБ) підприємства. Воно дозволяє виявляти та оцінювати ризики для інформаційних активів, обирати та впроваджувати адекватні заходи захисту, а також контролювати та вдосконалювати ці заходи на постійній основі [44, с. 28].

На сьогоднішній день існує ряд методичних підходів та стандартів, які можуть бути використані для планування інформаційної безпеки на підприємствах різних галузей та розмірів. Серед них можна виділити наступні:

- «Міжнародний стандарт ISO/IEC 27001» - один з найбільш відомих та широко застосовуваних стандартів в сфері інформаційної безпеки. Він встановлює вимоги до розробки, впровадження, підтримки та постійного вдосконалення СУІБ в контексті організації [45, с. 15].
- «Стандарт NIST SP 800-53» - розроблений Національним інститутом стандартів і технологій США (NIST) і містить рекомендації щодо вибору та впровадження заходів безпеки для інформаційних систем федеральних організацій [46, с. 42].
- «Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)» - дозволяє організаціям самостійно оцінювати ризики інформаційної безпеки та розробляти стратегії захисту на основі ідентифікації критичних інформаційних активів та загроз для них [47, с. 60].
- «Методологія CRAMM (CCTA Risk Analysis and Management Method)» - розроблена Центральним комп'ютерним і телекомунікаційним

агентством Великобританії (CCTA) і призначена для аналізу ризиків та управління ними в інформаційних системах організацій [48, с. 85].

— «Стандарт COBIT (Control Objectives for Information and Related Technologies)» - представляє собою набір рекомендацій та кращих практик в сфері управління інформаційними технологіями та безпекою, розроблений Асоціацією аудиту та контролю інформаційних систем (ISACA) [44, с. 72].

На практиці, багато підприємств використовують комбінацію різних стандартів та методологій, адаптуючи їх до своїх специфічних потреб та умов. При цьому, важливо забезпечити інтеграцію процесу планування інформаційної безпеки з загальними процесами управління ризиками та стратегічного планування на підприємстві.

Одним з ключових аспектів планування інформаційної безпеки є вибір адекватних методів оцінки ризиків. На сьогоднішній день існує ряд як якісних, так і кількісних методів, які можуть бути використані для цієї мети (табл. 2.16).

Таблиця 2.16

Порівняння якісних та кількісних методів оцінки ризиків інформаційної безпеки

Характеристика	**Якісні методи**	**Кількісні методи**
Опис ризику	**Високий, середній, низький**	**Числове значення (напр. 0.1, 0.5)**
Необхідні дані	**Досвід, інтуіція, судження експертів**	**Статистичні дані, результати тестів**
Трудомісткість	**Низька**	**Висока**
Точність	**Нижча**	**Вища**
Основне призначення	**Визначення пріоритетів ризиків**	**Обґрунтування інвестицій в безпеку**

Джерело: розроблено автором на основі [46, с. 205]

Як видно з таблиці, якісні методи оцінки ризиків є менш трудомісткими та базуються переважно на досвіді та судженнях експертів. Вони дозволяють визначити пріоритетність ризиків в термінах "високий", "середній", "низький",

що може бути корисно для попереднього аналізу та ранжування загроз [47, с. 225].

В той же час, кількісні методи дають більш точні та об'єктивні оцінки ризиків, виражені в числових значеннях. Вони потребують більше часу та ресурсів, а також наявності статистичних даних та результатів тестування. Кількісні оцінки ризиків є особливо корисними для обґрунтування інвестицій в заходи інформаційної безпеки та демонстрації їх економічної ефективності.

На практиці, багато підприємств використовують комбінацію якісних та кількісних методів оцінки ризиків, в залежності від етапу процесу управління ризиками та доступних ресурсів. При цьому, важливо забезпечити належну документацію та обґрунтування результатів оцінки ризиків, а також їх регулярний перегляд та оновлення.

Для полегшення вибору заходів захисту багато стандартів та методологій містять каталоги або бібліотеки типових механізмів безпеки, які можуть бути застосовані в різних ситуаціях. Наприклад, стандарт ISO/IEC 27002 містить більше 100 рекомендованих заходів безпеки, згрупованих за 14 розділами, такими як політика безпеки, управління доступом, криптографія, безпека комунікацій тощо.

При виборі конкретних заходів захисту підприємство повинно враховувати їх адекватність виявленим ризикам, а також співвідношення витрат та отриманих переваг. Для цього можуть використовуватись різні методи економічного аналізу, такі як розрахунок чистої приведеної вартості (NPV), внутрішньої норми прибутку (IRR), періоду окупності тощо (табл. 2.17).

Таблиця 2.17

Приклад розрахунку економічної ефективності заходів інформаційної безпеки

Показник	**Значення**
Щорічні втрати від інцидентів ІБ до впровадження заходів	**$100 000**
Щорічні втрати від інцидентів ІБ після впровадження заходів	**$20 000**
Щорічна економія від впровадження заходів	**$80 000**

Вартість впровадження заходів	**$200 000**
Період окупності (років)	**2,5**
Чиста приведена вартість (NPV) за 5 років при ставці дисконтування 10%	**$102 000**

Джерело: розроблено автором на основі [47, с. 325]

Як видно з таблиці, в даному прикладі впровадження заходів інформаційної безпеки дозволяє скоротити щорічні втрати від інцидентів на $80 000. При цьому, початкові інвестиції в розмірі $200 000 окупаються за 2,5 роки, а чиста приведена вартість проекту за 5 років складає $102 000, що свідчить про його економічну доцільність.

Ефективне планування інформаційної безпеки вимагає постійного навчання та підвищення обізнаності персоналу щодо їх ролей та обов'язків в забезпеченні безпеки інформаційних активів. Це передбачає регулярне проведення тренінгів, семінарів, тестувань та інших освітніх заходів для всіх співробітників організації, від вищого керівництва до рядових виконавців [47, с. 525].

Лише за таких умов планування інформаційної безпеки стане дійсно ефективним інструментом забезпечення надійного захисту інформаційних активів підприємства від сучасних кіберзагроз та створення стійкого та безпечного інформаційного середовища для ведення бізнесу.

2.2.1 Визначення шляхів оптимізації процедур планування інформаційної безпеки

Оптимізація процедур планування інформаційної безпеки є важливим завданням для будь-якого підприємства, яке прагне забезпечити надійний захист своїх інформаційних активів від сучасних кіберзагроз. В умовах постійного зростання складності та частоти кібератак, а також посилення регуляторних вимог до захисту інформації, ефективне планування інформаційної безпеки стає критично важливим для безперервності бізнесу та збереження конкурентоспроможності [49, с. 75].

На жаль, на багатьох підприємствах процедури планування інформаційної безпеки все ще залишаються недостатньо ефективними та

оптимізованими. Це може проявлятись у надмірній складності та бюрократизації процесів, відсутності чітких цілей та пріоритетів, неузгодженості з бізнес-стратегією, недостатній залученості зацікавлених сторін, низькій автоматизації та використанні застарілих інструментів тощо.

Для визначення шляхів оптимізації процедур планування інформаційної безпеки, перш за все, необхідно провести ґрунтовний аналіз поточного стану цих процедур на підприємстві. Це передбачає збір та аналіз кількісних та якісних показників ефективності планування, таких як:

- Час та витрати на розробку та оновлення планів інформаційної безпеки;
- Кількість та критичність виявлених ризиків та вразливостей;
- Відсоток реалізації запланованих заходів безпеки;
- Динаміка та тренди інцидентів інформаційної безпеки;
- Відгуки та рівень задоволеності зацікавлених сторін;
- Відповідність планів інформаційної безпеки регуляторним вимогам та стандартам тощо [51, с. 120].

Результати аналізу поточного стану процедур планування інформаційної безпеки на досліджуваному підприємстві представлені в (табл. 2.18.)

Таблиця 2.18

Показники ефективності процедур планування інформаційної безпеки

Показник	**Значення**
Середній час розробки плану інформаційної безпеки	**60 днів**
Середній час оновлення плану інформаційної безпеки	**90 днів**
Кількість виявлених критичних ризиків за останній рік	**15**
Відсоток реалізації запланованих заходів безпеки за останній рік	**75%**
Кількість інцидентів інформаційної безпеки за останній рік	**25**
Рівень відповідності планів інформаційної безпеки вимогам стандарту ISO/IEC 27001	**70%**

Джерело: розроблено автором на основі [52, с. 140]

Як видно з таблиці, на досліджуваному підприємстві спостерігаються певні проблеми з ефективністю процедур планування інформаційної безпеки, зокрема, довгий час розробки та оновлення планів, значна кількість критичних ризиків та інцидентів, неповна реалізація запланованих заходів безпеки та недостатня відповідність вимогам стандартів.

З урахуванням результатів аналізу, можна визначити наступні ключові напрямки та шляхи оптимізації процедур планування інформаційної безпеки на підприємстві. (рис. 2.4)

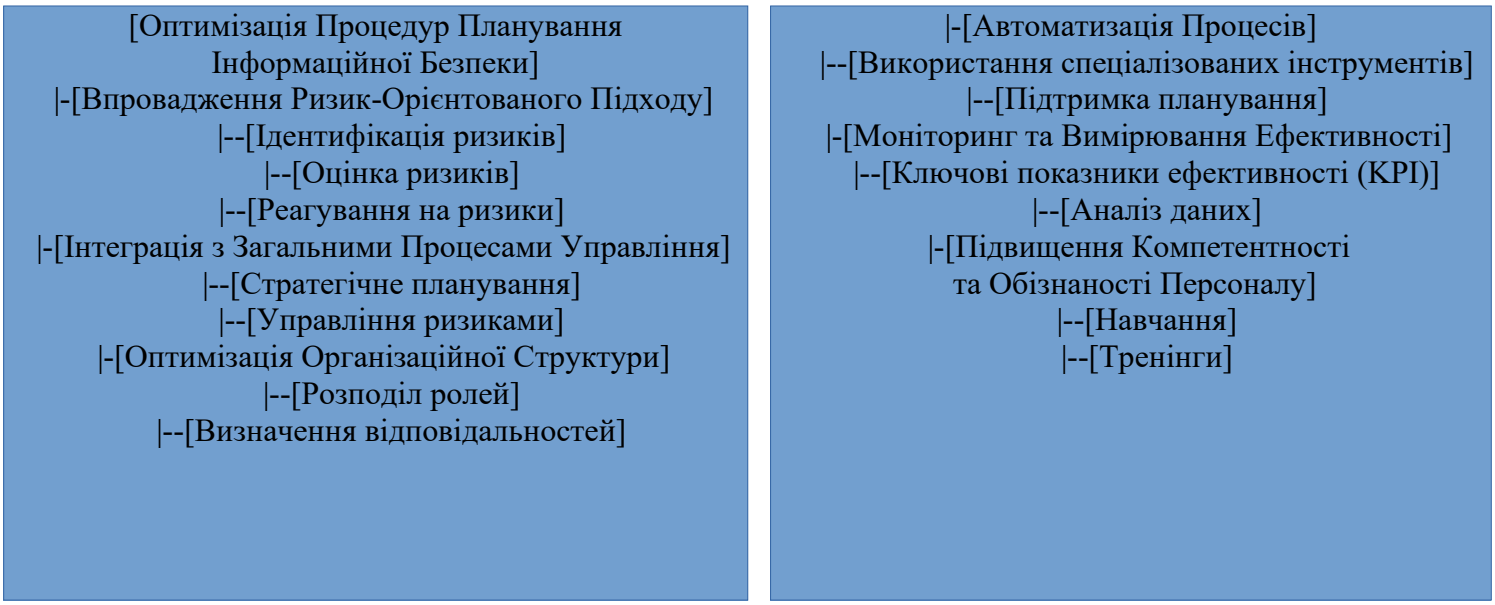

Рис. 2.4. «Візуалізація шляхів оптимізації процедур планування інформаційної безпеки»

Рис. 2.4. представляє собою структурний план, який детально відображає шляхи оптимізації процедур планування інформаційної безпеки на підприємстві. Він включає впровадження ризик-орієнтованого підходу, інтеграцію інформаційної безпеки з загальними процесами управління та стратегічного планування, оптимізацію організаційної структури, автоматизацію підтримки процесів, регулярний моніторинг та вимірювання ефективності, а також підвищення рівня компетентності та обізнаності

персоналу. Цей план спрямований на забезпечення більш ефективного та систематичного підходу до управління інформаційною безпекою.

1. Впровадження ризик-орієнтованого підходу до планування. Це передбачає фокусування зусиль та ресурсів на найбільш критичних ризиках та вразливостях, які можуть мати максимальний вплив на бізнес. Для цього необхідно використовувати кількісні методи оцінки ризиків, встановлювати чіткі критерії прийнятності ризиків, а також регулярно переглядати та оновлювати оцінки ризиків з урахуванням змін у середовищі загроз.
2. Забезпечення інтеграції планування інформаційної безпеки з загальними процесами управління ризиками та стратегічного планування на підприємстві. Це дозволить забезпечити узгодженість цілей та заходів інформаційної безпеки з бізнес-цілями та пріоритетами, а також підвищити обізнаність та залученість вищого керівництва та бізнес-підрозділів до процесів інформаційної безпеки [50, с. 185].
3. Оптимізація організаційної структури та розподілу ролей в процесах планування інформаційної безпеки. Це передбачає чітке визначення та документування обов'язків та відповідальності всіх учасників процесу планування, забезпечення їх необхідними ресурсами та повноваженнями, а також налагодження ефективних комунікацій та координації між ними [51, с. 205].
4. Автоматизація та використання спеціалізованих інструментів для підтримки процесів планування інформаційної безпеки. Це дозволить скоротити час та трудовитрати на виконання рутинних завдань, таких як збір та аналіз даних про активи та ризики, генерація звітності, відстеження статусу виконання планів тощо. Прикладами таких інструментів можуть бути системи управління інформаційною безпекою (ISMS), системи управління ризиками (GRC), системи управління вразливостями (VMS) тощо [52, с. 225].

5. Регулярний моніторинг та вимірювання ефективності процедур планування інформаційної безпеки за допомогою ключових показників ефективності (KPI). Це дозволить вчасно виявляти проблемні області та можливості для покращення, а також демонструвати прогрес та цінність процесів інформаційної безпеки для бізнесу. Приклади таких KPI наведені в табл. 2.19.

Таблиця 2.19

Приклади KPI для моніторингу ефективності процедур планування інформаційної безпеки

KPI	**Опис**	**Цільове значення**
Середній час розробки та оновлення планів ІБ	**Вимірює оперативність та ефективність процесів планування**	**<30 днів**
Відсоток виконання планів ІБ в строк	**Вимірює дисципліну та якість виконання планів**	**>90%**
Кількість критичних ризиків та інцидентів ІБ	**Вимірює ефективність заходів з обробки ризиків**	**<5 в рік**
Рівень відповідності планів ІБ вимогам стандартів	**Вимірює узгодженість планів з кращими практиками**	**>90%**

Джерело: розроблено автором на основі [53, с. 250]

6. Впровадження практик безперервного вдосконалення процедур планування інформаційної безпеки на основі циклу PDCA (Plan-Do-Check-Act). Це передбачає постійний перегляд та оптимізацію процесів планування з урахуванням зворотного зв'язку від зацікавлених сторін, результатів моніторингу та вимірювання, змін у середовищі загроз та регуляторних вимог, а також появи нових технологій та кращих практик в сфері інформаційної безпеки.

7. Підвищення рівня компетентності та обізнаності персоналу, задіяного в процесах планування інформаційної безпеки, шляхом регулярного навчання, сертифікації та обміну досвідом. Це дозволить забезпечити необхідний рівень знань та навичок для ефективного виконання завдань з планування, а також підвищити мотивацію та залученість співробітників до процесів інформаційної безпеки.

Звісно, наведені шляхи оптимізації процедур планування інформаційної безпеки не є вичерпними та універсальними для всіх підприємств. Кожна організація повинна визначати свої специфічні потреби та пріоритети в цій сфері, враховуючи свій розмір, галузь, бізнес-модель, регуляторне середовище, рівень зрілості процесів тощо.

Недостатня увага до етичних та соціальних аспектів в процесі планування інформаційної безпеки може призвести до негативних наслідків для репутації та довіри до підприємства з боку співробітників, клієнтів та суспільства в цілому.

Тому, при оптимізації процедур планування інформаційної безпеки, необхідно знаходити розумний баланс між вимогами безпеки та етичними й соціальними нормами, залучати до процесу планування фахівців з питань етики та права, а також забезпечувати прозорість та підзвітність щодо впроваджених заходів безпеки [52, с. 415].

Слідування цим рекомендаціям дозволить підприємствам суттєво підвищити ефективність та результативність процедур планування інформаційної безпеки, забезпечити їх відповідність сучасним викликам та вимогам, а також створити надійну основу для захисту своїх інформаційних активів та безперервності ведення бізнесу в умовах зростаючих кіберзагроз.

2.2.2 Розробка схеми дій керівництва щодо планування інформаційної безпеки

Ефективне планування інформаційної безпеки на підприємстві вимагає активної участі та лідерства з боку вищого керівництва. Саме на керівництві

лежить відповідальність за визначення стратегічних цілей та пріоритетів інформаційної безпеки, забезпечення необхідних ресурсів та повноважень для їх реалізації, а також створення культури безпеки в організації [54, с. 42].

Для того, щоб забезпечити системний та послідовний підхід до планування інформаційної безпеки, керівництву підприємства необхідно розробити чітку схему дій, яка буде включати в себе ключові етапи, завдання та відповідальних осіб [55, с. 68]. (рис. 2.4)

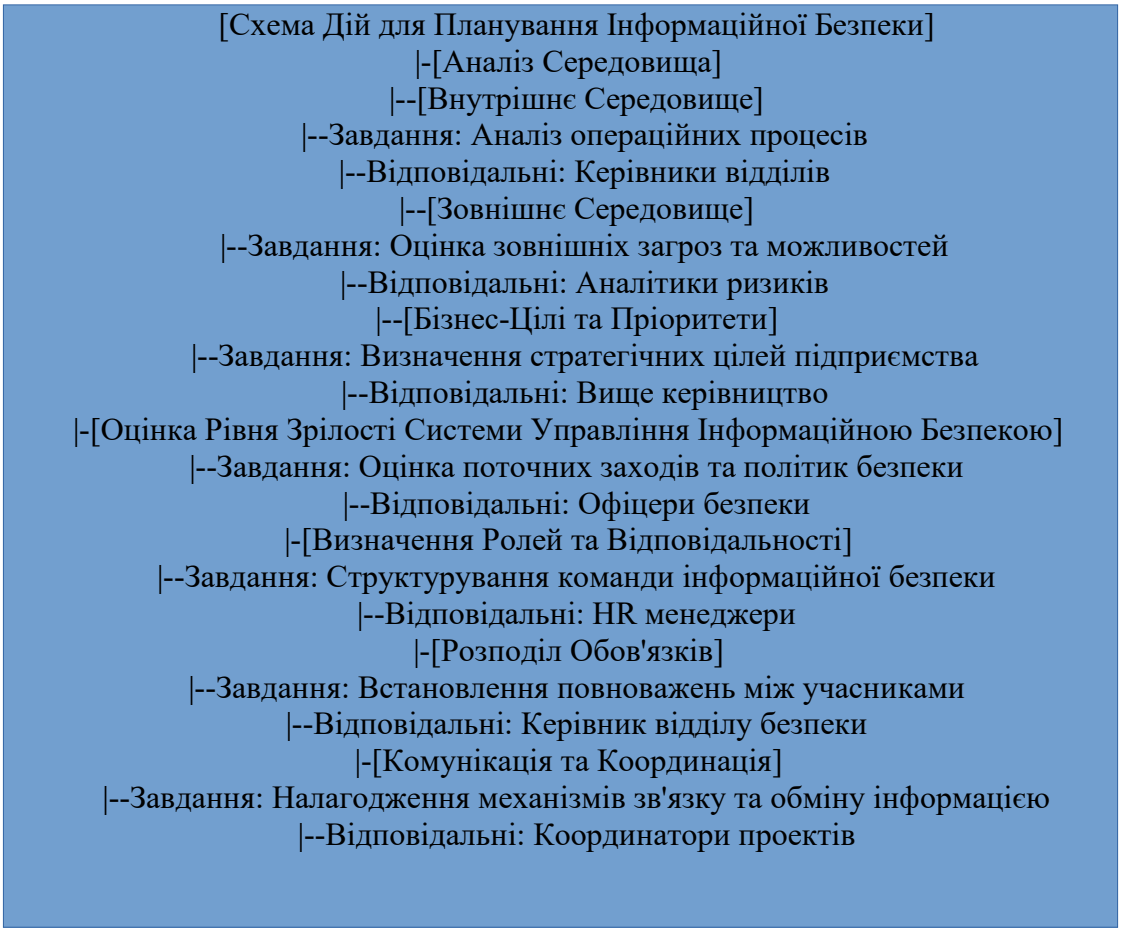

Рис 2.4 Схема Дій для Планування Інформаційної Безпеки

Він включає аналіз внутрішнього та зовнішнього середовища, оцінку рівня зрілості системи управління інформаційною безпекою, визначення ролей та відповідальностей усередині команди, розподіл обов'язків та повноважень, а також налагодження ефективних механізмів комунікації та координації між учасниками. Цей план спрямований на оптимізацію процедур і підвищення ефективності управління інформаційною безпекою на підприємстві.

Для оцінки рівня зрілості системи управління інформаційною безпекою (СУІБ) можна використовувати різні моделі та стандарти, такі як ISO/IEC 27001, NIST Cybersecurity Framework, COBIT тощо. Приклад оцінки рівня зрілості СУІБ за моделлю COBIT наведено в табл. 2.20.

Таблиця 2.20

Оцінка рівня зрілості СУІБ за моделлю COBIT

Домен	**Рівень зрілості (від 0 до 5)**
Планування та організація	**2**
Придбання та впровадження	**1**
Доставка та підтримка	**3**
Моніторинг та оцінка	**2**

Джерело: розроблено автором на основі [57, с. 115]

Як видно з таблиці, на досліджуваному підприємстві рівень зрілості СУІБ за різними доменами моделі COBIT варіюється від 1 до 3, що свідчить про недостатню ефективність та зрілість існуючих процесів управління інформаційною безпекою.

При цьому, важливо забезпечити чіткий розподіл обов'язків та повноважень між різними учасниками процесу планування інформаційної безпеки, а також налагодити ефективні механізми комунікації та координації між ними [56, с. 155].

Приклад матриці відповідальності в процесах планування інформаційної безпеки (RACI-матриця) наведено в табл. 2.21.

Таблиця 2.21

RACI-матриця відповідальності в процесах планування інформаційної безпеки

Процес	**Керівництво**	**Служба ІБ**	**ІТ-відділ**	**Бізнес-підрозділи**
Управління ризиками	**A**	**R**	**C**	**I**
Розробка політик та процедур	**A**	**R**	**C**	**C**
Впровадження заходів безпеки	**I**	**A**	**R**	**C**
Моніторинг та аудит	**I**	**A/R**	**C**	**I**
Реагування на інциденти	**I**	**A/R**	**C**	**I**

Позначення: R - відповідальний, A - підзвітний, C - консультує, I - інформується.

Джерело: розроблено автором на основі [55, с. 175]

Як видно з матриці, служба інформаційної безпеки відіграє ключову роль в більшості процесів планування та управління інформаційною безпекою, тоді як керівництво здійснює загальний контроль та підзвітність, ІТ-відділ забезпечує технічну реалізацію заходів безпеки, а бізнес-підрозділи залучаються до консультацій та інформування.

Третім етапом схеми дій керівництва є визначення та оцінка ризиків інформаційної безпеки. Це передбачає ідентифікацію ключових інформаційних активів підприємства, аналіз потенційних загроз та вразливостей для цих активів, а також оцінку ймовірності та потенційних наслідків реалізації цих загроз.

Для оцінки ризиків інформаційної безпеки можна використовувати різні методи та інструменти, такі як OCTAVE, FRAP, CRAMM, а також галузеві стандарти та рекомендації, наприклад, ISO/IEC 27005, NIST SP 800-30 тощо.

Приклад оцінки ризиків інформаційної безпеки за методом FRAP (Facilitated Risk Analysis Process) наведено в табл. 2.22.

Таблиця 2.22

Оцінка ризиків інформаційної безпеки за методом FRAP

Актив	**Загроза**	**Вразливість**	**Ймовірність**	**Наслідки**	**Рівень ризику**
База даних клієнтів	**Несанкціонований доступ**	**Застарілі протоколи аутентифікації**	**Висока**	**Високі**	**Високий**
Корпоративна електронна пошта	**Фішинг-атаки**	**Недостатня обізнаність користувачів**	**Середня**	**Середні**	**Середній**
Сервер веб-додатків	**Атаки типу "відмова в обслуговуванні"**	**Вразливості в конфігурації серверу**	**Низька**	**Високі**	**Середній**

Джерело: розроблено автором на основі [56, с. 235]

Як видно з таблиці, для кожного ключового інформаційного активу підприємства були ідентифіковані потенційні загрози та вразливості, оцінена ймовірність їх реалізації та потенційні наслідки, а також визначений загальний рівень ризику (високий, середній або низький).

На основі результатів оцінки ризиків керівництво підприємства повинно визначити пріоритетні напрямки для обробки цих ризиків та розробити відповідні стратегії та плани дій.

Це може включати в себе такі заходи, як впровадження додаткових механізмів контролю доступу та автентифікації, навчання та підвищення обізнаності персоналу щодо кібербезпеки, оновлення та зміцнення конфігурацій систем та мереж, розробку планів реагування на інциденти тощо [57, с. 275].

Політики та процедури інформаційної безпеки повинні охоплювати всі ключові аспекти та процеси СУІБ, такі як управління доступом,

криптографічний захист, безпека комунікацій, захист від шкідливого програмного забезпечення, управління інцидентами, забезпечення відповідності вимогам тощо [56, с. 315].

Висновки до розділу 2

Аналіз процесу планування інформаційної безпеки на підприємстві ТОВ "Інфосейф" демонструє значний потенціал для вдосконалення вже існуючих методів. Вивчення актуальних загроз, оцінка вразливостей систем, та імплементація захисних заходів становлять основу цього процесу. Особливу увагу варто звернути на аналіз ефективності застосованих методів захисту та їх адаптацію в залежності від змін у зовнішньому та внутрішньому середовищі компанії. Поєднання цих методів із загальною стратегією підприємства може значно покращити захист інформації та ефективність робочих процесів. ТОВ "Інфосейф", яке активно аналізує і оцінює свою IT-інфраструктуру та управління даними, має можливість виявити недоліки у захисті даних, зокрема, в мережевій інфраструктурі та системах управління доступом. Проблеми, які часто зустрічаються, такі як недостатній рівень обізнаності співробітників з питань кібербезпеки та відсутність чіткої стратегії регулярного оновлення програмного забезпечення, вимагають негайного реагування. Впровадження багаторівневої системи захисту та сучасних технологій шифрування може допомогти в мінімізації ризиків та підвищенні загального рівня інформаційної безпеки.

Використання цього підходу на практиці дозволяє не тільки підвищити рівень безпеки але й забезпечити краще розуміння та керування вразливостями в IT-інфраструктурі, тим самим зміцнюючи довіру до компанії серед клієнтів і партнерів. Важливо не тільки адаптувати існуючі методи захисту до змін у середовищі, але й регулярно переосмислювати та оновлювати стратегії інформаційної безпеки, що відповідають сучасним вимогам і стандартам.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВДОСКОНАЛЕННЯ ПЛАНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Можна виділити кілька ключових напрямків для удосконалення. Перше і, мабуть, найважливіше поліпшення можна досягти шляхом зміцнення культури інформаційної безпеки серед співробітників. Важливо забезпечити регулярне навчання та тренінги, які не тільки зосереджуються на технічних аспектах безпеки, але й підкреслюють значення збереження конфіденційності корпоративної інформації як складової корпоративної культури.

Другим напрямком є оптимізація процесів ідентифікації та оцінки ризиків. Це включає в себе впровадження передових методик квантифікації ризиків, що дозволяє більш точно визначати потенційні загрози та відповідно краще планувати бюджет на заходи безпеки. Також корисним є використання автоматизованих інструментів для моніторингу та управління ризиками, що спрощує процеси виявлення та реагування на інциденти в режимі реального часу. Третім важливим аспектом є посилення технічних мережевих заходів безпеки. Враховуючи зростаючу загрозу кібератак, ТОВ "Інфосейф" має зосередитись на застосуванні розширених механізмів захисту, включно з застосуванням сучасних рішень для захисту кінцевих точок, шифрування даних і мережевого сегментування. Важливо також розглядати впровадження двофакторної аутентифікації для доступу до найбільш чутливих систем і даних.

3.1 Визначення процесів планування інформаційної безпеки - на прикладі ТОВ «ІНФОСЕЙФ»

Процеси планування інформаційної безпеки на ТОВ "Інфосейф" відіграють ключову роль у забезпеченні захисту інформаційних активів та безперервності бізнесу цієї компанії. Вони дозволяють виявляти та оцінювати ризики, розробляти та впроваджувати необхідні заходи безпеки, а також забезпечувати постійний моніторинг та вдосконалення системи управління інформаційною безпекою [58, с. 75].

Для визначення процесів планування інформаційної безпеки на ТОВ "Інфосейф" було використано підхід, заснований на міжнародному стандарті ISO/IEC 27001:2013. Цей стандарт містить вимоги до розробки, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) [59, с. 92].

Відповідно до цього підходу, процеси планування інформаційної безпеки на ТОВ "Інфосейф" можуть бути розділені на наступні ключові етапи:

Визначення контексту та цілей організації в сфері інформаційної безпеки. На цьому етапі проводиться аналіз внутрішнього та зовнішнього середовища ТОВ "Інфосейф", визначаються його бізнес-цілі та пріоритети, а також оцінюється поточний рівень зрілості системи управління інформаційною безпекою.

Ідентифікація та оцінка ризиків інформаційної безпеки. Цей етап передбачає виявлення ключових інформаційних активів ТОВ "Інфосейф", аналіз потенційних загроз та вразливостей для цих активів, а також оцінку ймовірності та потенційних наслідків реалізації цих загроз [64, с. 135].

Розробка та впровадження заходів безпеки. На основі результатів оцінки ризиків на ТОВ "Інфосейф" розробляються та впроваджуються необхідні заходи безпеки, такі як політики, процедури, технічні засоби контролю тощо. Ці заходи повинні забезпечувати адекватний захист інформаційних активів від виявлених ризиків [62, с. 155].

Моніторинг та перегляд ефективності заходів безпеки. Цей етап передбачає регулярний збір та аналіз даних про функціонування СУІБ, виявлення відхилень та недоліків, оцінку ефективності та адекватності впроваджених механізмів контролю, а також своєчасне реагування на виявлені проблеми та інциденти.

Постійне вдосконалення СУІБ. На цьому етапі проводиться періодична оцінка адекватності та ефективності впроваджених політик, процедур та механізмів контролю з урахуванням зміни внутрішніх та зовнішніх факторів. За результатами такої оцінки приймаються рішення щодо необхідності перегляду

та оновлення існуючих документів та заходів забезпечення інформаційної безпеки [65, с. 195].

Важливо відзначити, що процеси планування інформаційної безпеки на ТОВ "Інфосейф" повинні бути безперервними та циклічними, забезпечуючи постійну адаптацію та розвиток СУІБ відповідно до мінливих умов та викликів сучасного кіберпростору.

Крім того, ефективність процесів планування інформаційної безпеки на ТОВ "Інфосейф" значною мірою залежить від залучення та підтримки вищого керівництва, чіткого розподілу ролей та відповідальності, а також забезпечення необхідних ресурсів та компетенцій.

При вивченні та розробці пропозицій щодо вдосконалення планування інформаційної безпеки особливу увагу слід приділити аспектам, які ще не були детально описані в практиці ТОВ «Інфосейф». Наразі, аналізуючи поточний стан системи управління інформаційною безпекою (СУІБ), важливо проаналізувати взаємодії між підрозділами компанії, які впливають на інформаційну безпеку. Це може включати аудит співпраці між ІТ-відділом та відділом забезпечення якості з метою виявлення можливих внутрішніх вразливостей, які можуть бути неочевидними за допомогою стандартних методів оцінки ризиків.

Також доцільно запровадити режим навчання для персоналу на всіх рівнях, оскільки людський фактор часто є однією з найслабших ланок у забезпеченні інформаційної безпеки. Регулярні тренінги, семінари та майстер-класи з актуальних питань кібербезпеки можуть значно підвищити рівень обізнаності та готовності працівників до виявлення та усунення потенційних загроз. З метою вдосконалення процесу планування інформаційної безпеки рекомендується розробити більш чіткі процедури реагування на інциденти інформаційної безпеки, включаючи не тільки технічні аспекти реагування, а й комунікаційні стратегії. Наявність чіткого плану реагування на інциденти, який може бути використаний і зрозумілий усім співробітникам, допоможе швидше і ефективніше мінімізувати наслідки можливих інформаційних загроз.

Використання сучасних технологічних інструментів для моніторингу стану інформаційної безпеки також заслуговує на увагу. Інтеграція інструментів штучного інтелекту та машинного навчання може допомогти виявити незвичні моделі поведінки або аномалії в системах, які можуть сигналізувати про спроби несанкціонованого доступу або інші кібератаки. Ці технології можуть значно покращити час реагування на інциденти та загальну ефективність систем інформаційної безпеки.

У процесі подальшого вдосконалення системи управління інформаційною безпекою ТОВ "Інфосейф" важливо зосередитись на розвитку внутрішніх аудитів і оцінювання дотримання нормативних вимог. Ефективне здійснення внутрішніх аудитів дозволяє не тільки виявити слабкі місця в системі безпеки, але й сприяє розвитку культури безпеки серед співробітників. Регулярне проведення навчань і тренінгів на базі виявлених під час аудитів проблематичних аспектів дозволяє зміцнити заходи інформаційної безпеки та підвищити обізнаність персоналу.

Інший аспект, який вимагає уваги, – це розробка механізму швидкого реагування на кіберінциденти, що передбачає не тільки технічні засоби відновлення системи, але й чіткий алгоритм дій персоналу в критичних ситуаціях. Важливо, щоб усі співробітники, не тільки IT-спеціалісти, але й звичайні користувачі, розуміли свої обов'язки та способи дій при виявленні підозрілої діяльності або збоїв у системі. З огляду на швидкий розвиток технологій, ТОВ "Інфосейф" може розглянути можливість впровадження клаудових рішень для зберігання даних з високим рівнем шифрування та захисту. Це не тільки забезпечить додатковий рівень безпеки даних, але й дозволить оптимізувати витрати на утримання власних серверів. Однак, перед впровадженням таких рішень необхідно ретельно проаналізувати потенційних постачальників послуг та їх дотримання нормативних вимог щодо захисту інформації.

Враховуючи стрімкий розвиток технологічних інновацій та збільшення кіберзагроз, ТОВ "Інфосейф" може зосередитись на розширенні своєї стратегії

інформаційної безпеки, включаючи інтеграцію передових методів штучного інтелекту та машинного навчання для прогнозування потенційних кібератак. Ці технології можуть аналізувати великі обсяги даних з неймовірною швидкістю та точністю, що дозволяє виявляти складні взаємозалежності та аномалії, які можуть бути неочевидними для традиційних систем моніторингу.

Ще одним важливим аспектом, який може зміцнити інформаційну безпеку компанії, є розробка більш гнучких методів шифрування даних, які адаптуються до змінних умов оперативного середовища. Використання квантового шифрування або гомоморфного шифрування може забезпечити високий рівень захисту даних навіть у випадку теоретичного прориву в квантових обчисленнях, які могли б порушити звичні методи шифрування.

Не менш важливою є оптимізація існуючих процесів аудиту та контролю в ТОВ "Інфосейф". Створення мобільних аудиторських груп, що здійснюють перевірки на дотримання норм інформаційної безпеки у реальному часі, може підвищити ефективність виявлення порушень та відхилень від стандартів. Це, у свою чергу, сприяє підвищенню відповідальності відділів і окремих співробітників, а також допомагає уникнути багатьох помилок та уразливостей. На додаток до технічних аспектів, значення має також вдосконалення правової бази, що регулює питання інформаційної безпеки. Оновлення корпоративних політик та процедур згідно із змінами в законодавстві та стандартах міжнародних організацій може забезпечити не тільки юридичну відповідність, але й зростання довіри клієнтів і партнерів до компанії.

Для подальшого вдосконалення планування інформаційної безпеки в ТОВ "Інфосейф", можливо, слід розглянути впровадження комплексної системи управління ідентичностями та доступом. Ця система може включати біометричні технології, такі як відбитки пальців, розпізнавання обличчя або сканування сітківки ока, які значно підвищують рівень безпеки, оскільки зменшують ризик несанкціонованого доступу через крадіжку або втрату паролів. Застосування таких технологій може ефективно захистити критично важливі дані і системи від зовнішніх атак та внутрішніх загроз.

Оскільки сучасний кіберпростір вимагає адаптації до непередбачуваних загроз, компанія могла б розглянути можливість створення власної оперативної кібероборонної команди, яка б займалася моніторингом, реагуванням та відновленням після інцидентів. Ця команда мала б регулярно проводити кібербезпекові тренування та симуляції атак, щоб покращити готовність компанії до реальних загроз.

Також важливим елементом в стратегії інформаційної безпеки є розробка дієвого плану відновлення після порушень, який би охоплював не тільки технічні аспекти відновлення систем, але й комунікаційні стратегії з клієнтами та партнерами, відновлення довіри стейкхолдерів та вирішення юридичних питань, що можуть виникнути внаслідок порушень безпеки. Такий підхід забезпечив би не лише технічне, але й бізнесове та репутаційне відновлення компанії. Інша рекомендація може включати розгляд міжнародних практик та стандартів, таких як GDPR в Європейському Союзі, що регулюють захист даних, для інтеграції найкращих практик та забезпечення відповідності до міжнародних вимог. Це могло б не тільки підвищити рівень довіри клієнтів та партнерів, але й значно знизити ризики, пов'язані з можливими правовими наслідками порушення політик інформаційної безпеки. (табл. 3.1.)

Таблиця 3.1

Ключові напрями вдосконалення інформаційної безпеки ТОВ «Інфосейф»

Ключові напрями	Опис
Впровадження системи управління ідентичностями та доступом	Включення біометричних технологій та розширені методи аутентифікації для зменшення ризику несанкціонованого доступу.
Створення оперативної кібероборонної команди	Формування команди, що спеціалізується на моніторингу, реагуванні на інциденти та відновленні систем після атак.
Розробка дієвого плану відновлення після порушень	Підготовка комплексного плану відновлення, який охоплює технічні, комунікаційні та юридичні аспекти.

Продовження таблиці 3.1

Інтеграція міжнародних стандартів та практик	Впровадження найкращих практик захисту даних, зокрема GDPR, для підвищення відповідності до міжнародних вимог.

Таблиця 3.1 резюмує стратегічні ініціативи, які ТОВ "Інфосейф" може впровадити для підвищення ефективності системи управління інформаційною безпекою. Кожен з наведених напрямів заснований на сучасних технологічних досягненнях та відповідності міжнародним нормам, що дозволяє компанії не тільки зміцнити захист своїх інформаційних активів, але й забезпечити стабільний розвиток у швидкозмінному діловому середовищі. Окрім технічних аспектів, важливе місце у стратегії займають ініціативи, пов'язані з формуванням корпоративної культури безпеки, що включає постійне навчання співробітників і вдосконалення нормативно-правової бази.

Для посилення інформаційної безпеки на ТОВ "Інфосейф" необхідно систематично працювати над оцінкою ризиків, підвищенням компетентності персоналу, оптимізацією процесів реагування на інциденти, а також інтеграцією сучасних технологічних рішень. Такий комплексний підхід дозволить забезпечити високий рівень захисту інформаційних ресурсів і підтримати стабільне функціонування компанії в умовах постійно змінюваних кіберзагроз. На основі цих додаткових рекомендацій планування інформаційної безпеки ТОВ «Інфосейф» може бути значно покращено, що забезпечить високий рівень захисту інформаційних активів і сприятиме стабільності та безперервності бізнес-процесів компанії.

Таким чином, визначення та впровадження процесів планування інформаційної безпеки на ТОВ "Інфосейф" відповідно до вимог міжнародного стандарту ISO/IEC 27001:2013 дозволяє створити надійну та стійку систему управління інформаційною безпекою, яка здатна ефективно протистояти сучасним кіберзагрозам та забезпечувати безперервність бізнесу цієї компанії.

3.2 Розробка рекомендацій щодо вдосконалення планування інформаційної безпеки

Планування інформаційної безпеки є невід'ємною складовою загальної системи управління інформаційною безпекою на підприємстві. Воно дозволяє визначити потенційні загрози та ризики для інформаційних активів, розробити та впровадити необхідні заходи безпеки, а також забезпечити постійний моніторинг та вдосконалення процесів захисту інформації [66, с. 42].

Для того, щоб планування інформаційної безпеки було ефективним та результативним, необхідно враховувати ряд ключових факторів та дотримуватись певних принципів. Нижче наведено основні рекомендації щодо вдосконалення планування інформаційної безпеки на підприємстві.

Забезпечення підтримки та залучення вищого керівництва. Ефективне планування інформаційної безпеки неможливе без активної участі та підтримки з боку вищого керівництва підприємства. Керівництво повинно розуміти важливість інформаційної безпеки для бізнесу, виділяти необхідні ресурси та повноваження для реалізації заходів безпеки, а також демонструвати лідерство та особистий приклад в дотриманні політик та процедур безпеки [67, с. 58].

Інтеграція планування інформаційної безпеки з загальними процесами управління ризиками та стратегічного планування. Планування інформаційної безпеки не повинно здійснюватись ізольовано від інших управлінських процесів на підприємстві. Навпаки, воно має бути тісно інтегроване з загальними процесами управління ризиками та стратегічного планування, що дозволить забезпечити узгодженість цілей та заходів інформаційної безпеки з бізнес-цілями та пріоритетами підприємства.

Впровадження ризик-орієнтованого підходу до планування інформаційної безпеки. Ефективне планування інформаційної безпеки повинно базуватись на ретельному аналізі та оцінці ризиків для інформаційних активів підприємства. Це дозволяє виявити найбільш критичні загрози та вразливості, оцінити потенційні наслідки їх реалізації, а також визначити пріоритетні напрямки для впровадження заходів безпеки.

Використання кількісних методів оцінки ризиків та ефективності інвестицій в інформаційну безпеку. Для того, щоб планування інформаційної безпеки було обґрунтованим та переконливим для керівництва та інших зацікавлених сторін, необхідно використовувати кількісні методи оцінки ризиків та ефективності інвестицій в безпеку. Такі методи дозволяють отримати більш точні та об'єктивні оцінки потенційних збитків від реалізації загроз, а також визначити оптимальний рівень витрат на заходи безпеки з урахуванням співвідношення витрат та вигод.

Забезпечення відповідності планів інформаційної безпеки вимогам законодавства, регуляторів та стандартів. Плани інформаційної безпеки повинні розроблятись з урахуванням вимог чинного законодавства, галузевих регуляторів та міжнародних стандартів в сфері інформаційної безпеки, таких як ISO/IEC 27001, NIST SP 800-53, COBIT тощо. Це дозволяє забезпечити відповідність процесів управління інформаційною безпекою на підприємстві кращим світовим практикам та мінімізувати ризики штрафів та санкцій з боку регуляторів.

Залучення всіх зацікавлених сторін до процесу планування інформаційної безпеки. Ефективне планування інформаційної безпеки вимагає активного залучення та співпраці всіх зацікавлених сторін, включаючи бізнес-підрозділи, IT-службу, відділ інформаційної безпеки, юридичний відділ, відділ управління персоналом тощо. Це дозволяє врахувати потреби та очікування всіх сторін, забезпечити їх підтримку та участь в реалізації планів безпеки, а також мінімізувати потенційні конфлікти та протиріччя.

Регулярний перегляд та оновлення планів інформаційної безпеки. Плани інформаційної безпеки не повинні бути статичними документами, а мають регулярно переглядатись та оновлюватись з урахуванням змін у внутрішньому та зовнішньому середовищі підприємства, появи нових загроз та вразливостей, зміни регуляторних вимог тощо. Це дозволяє забезпечити актуальність та адекватність планів безпеки поточним потребам та викликам [68, с. 175].

Впровадження автоматизованих інструментів для підтримки процесів планування інформаційної безпеки. Для підвищення ефективності та зручності процесів планування інформаційної безпеки доцільно використовувати автоматизовані інструменти, такі як системи управління ризиками (GRC), системи управління інформаційною безпекою (ISMS), системи управління вразливостями (VMS) тощо. Такі інструменти дозволяють скоротити час та трудовитрати на виконання рутинних завдань, забезпечити консистентність та повноту даних, а також спростити генерацію звітності та візуалізацію результатів.

Забезпечення інтеграції заходів інформаційної безпеки з IT-інфраструктурою та бізнес-процесами підприємства. Заходи інформаційної безпеки, передбачені планами, повинні бути тісно інтегровані з існуючою IT-інфраструктурою та бізнес-процесами підприємства. Це дозволяє мінімізувати потенційний негативний вплив заходів безпеки на функціонування та продуктивність систем та процесів, а також забезпечити їх ефективну реалізацію та підтримку з боку IT-служби та бізнес-підрозділів.

Впровадження систем матеріальної та нематеріальної мотивації персоналу. Для забезпечення зацікавленості та активної участі персоналу в реалізації планів інформаційної безпеки доцільно впровадити системи матеріальної та нематеріальної мотивації, які стимулюватимуть співробітників до дотримання політик та процедур безпеки, а також до виявлення та попередження інцидентів та порушень безпеки.

Використання кращих світових практик та стандартів для планування інформаційної безпеки. Для забезпечення ефективності та відповідності планування інформаційної безпеки сучасним вимогам та викликам необхідно використовувати кращі світові практики та стандарти в цій сфері, такі як ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, ITIL тощо. Це дозволяє впроваджувати перевірені та визнані підходи та методи планування, а також забезпечувати сумісність та порівнянність процесів інформаційної безпеки з іншими організаціями [69, с. 295].

Впровадження практик безперервного вдосконалення процесів планування інформаційної безпеки. Для підтримки високого рівня ефективності та актуальності планування інформаційної безпеки необхідно впроваджувати практики безперервного вдосконалення цих процесів. Це передбачає регулярний аналіз та оцінку ефективності існуючих підходів та методів планування, виявлення можливостей для оптимізації та покращення, а також впровадження відповідних змін та інновацій [70, с. 335].

Таким чином, вдосконалення планування інформаційної безпеки на підприємстві вимагає комплексного та системного підходу, який враховує різноманітні аспекти та фактори, від забезпечення підтримки керівництва до впровадження автоматизованих інструментів та практик безперервного вдосконалення.

Розробка рекомендацій щодо вдосконалення планування інформаційної безпеки на підприємстві ТОВ "Інфосейф" передбачає комплексний підхід до аналізу існуючих процесів та їх оптимізації з метою підвищення загальної стійкості компанії до інформаційних ризиків. Важливо розуміти, що динамічний розвиток технологій та зміни у загрозах вимагають постійного оновлення підходів до управління безпекою. Це означає, що підприємство має регулярно переглядати свої політики і процедури, звертаючи увагу не тільки на нові технологічні рішення, але й на еволюцію кіберзагроз.

Одним із кроків у вдосконаленні планування безпеки може стати глибше інтегрування систем інформаційної безпеки з основними бізнес-процесами компанії. Це включає розробку чітких ліній зв'язку між IT-департаментом і вищим керівництвом, що сприяє кращому розумінню і підтримці ініціатив з інформаційної безпеки на найвищому рівні. Крім того, регулярне навчання персоналу є критично важливим для підвищення їх обізнаності та відповідальності у сфері захисту даних. Додатковим аспектом є використання передових методик аналізу та оцінки ризиків, які дозволяють не просто виявляти потенційні загрози, але й адекватно оцінювати можливі наслідки для бізнесу. Інтеграція сучасних аналітичних інструментів та інтелектуальних

систем може значно підвищити ефективність процесів моніторингу та реагування на інциденти. Значну роль відіграє також розробка ефективної стратегії реагування на інциденти, яка включає не тільки технічні аспекти, але й чітко визначені процедури комунікації як всередині компанії, так і з зовнішніми сторонами, включаючи клієнтів та партнерів. Така стратегія має бути гнучкою та здатною адаптуватися до різних типів інцидентів, забезпечуючи швидке відновлення операцій і мінімізацію втрат.

В контексті подальшого вдосконалення планування інформаційної безпеки на ТОВ "Інфосейф", одним з ключових аспектів є розробка та впровадження інтегрованої системи ідентифікації та автентифікації користувачів, яка б об'єднувала різні методи забезпечення безпеки. Система могла б включати двофакторну аутентифікацію, біометричні дані та електронні ключі, забезпечуючи тим самим додатковий шар захисту від несанкціонованого доступу до критичних систем та даних. Крім технічних засобів, необхідно звернути увагу на роль корпоративної культури у підвищенні рівня інформаційної безпеки. Важливо створити середовище, де кожен працівник відчуває особисту відповідальність за захист інформації та розуміє значення своїх дій для загальної безпеки компанії. Регулярне проведення тренінгів, семінарів та воркшопів, націлених на підвищення обізнаності співробітників про кіберзагрози, їхні методи та засоби захисту, може суттєво знизити ймовірність випадків витоку інформації чи інших інцидентів, пов'язаних з інформаційною безпекою. Поряд із залученням співробітників, необхідно також зосередитись на створенні ефективної системи моніторингу і реагування на інциденти. Використання автоматизованих систем для постійного спостереження за інфраструктурою IT може допомогти виявляти потенційні загрози та вразливості на ранніх стадіях, перш ніж вони призведуть до серйозних проблем. Такі системи можуть автоматично аналізувати великі потоки даних на предмет аномалій, швидко ідентифікувати джерела загроз і забезпечувати команді безпеки важливу інформацію для прийняття оперативних рішень.

Важливим є зосередження уваги на правовій складовій інформаційної безпеки. Враховуючи міжнародний характер сучасного кіберпростору, ТОВ "Інфосейф" має забезпечити, що їхні практики інформаційної безпеки відповідають не тільки національному законодавству, але й міжнародним стандартам і договорам. Це включає в себе детальний аналіз зовнішніх регуляторних вимог і швидке адаптування до них. Прикладом такої роботи може бути впровадження політик відповідності до GDPR для захисту даних клієнтів в ЄС.

Паралельно з цим, підхід до вдосконалення інформаційної безпеки має включати стратегії для забезпечення фізичної безпеки IT-інфраструктури. Незважаючи на високий рівень уваги до кіберзахисту, фізичний захист данихових центрів та інших критичних активів залишається ключовим. Це включає контроль доступу, відеоспостереження, системи виявлення і попередження вторгнень, що не тільки підсилюють захист, але й демонструють зобов'язання компанії перед зацікавленими сторонами щодо серйозного ставлення до захисту інформації. На додачу до вже існуючих заходів, компанія може розглянути можливість створення спеціалізованої ролі — офіцера з інформаційної безпеки (CISO), який би відповідав за всі аспекти інформаційної безпеки і мав достатні повноваження для впровадження необхідних змін. Це покращило б реалізацію стратегій інформаційної безпеки, оскільки CISO відіграв би ключову роль у забезпеченні відповідності безпеки стратегічним цілям компанії і забезпечив би ефективне спілкування між різними підрозділами і керівництвом.

У рамках додаткових ініціатив щодо вдосконалення інформаційної безпеки на ТОВ "Інфосейф", можна розглянути залучення зовнішніх консультантів для проведення незалежних аудитів та валідації існуючих безпекових процедур. Незалежний огляд може виявити сліпі плями у стратегіях безпеки, які можуть не бути очевидними для внутрішніх команд. Крім того, зовнішні консультанти можуть надати цінні рекомендації з останніх практик і

технологій, які використовуються на глобальному рівні та які можуть бути адаптовані для покращення загальної структури безпеки компанії.

Далі, важливим аспектом є створення детального плану реагування на порушення інформаційної безпеки, який би включав чіткі інструкції для кожної ролі в компанії – від IT-персоналу до керівництва. Ефективні плани реагування на інциденти допомагають мінімізувати збитки від інцидентів, забезпечуючи швидке і контрольоване відновлення операцій. Окрім того, це сприяє зміцненню довіри клієнтів і партнерів, які бачать, що компанія володіє розробленими і ефективними механізмами для вирішення потенційних загроз. Також корисним може бути розгляд можливості створення відділу з кібер-розвідки, який би займався аналізом та прогнозуванням загроз на основі зібраних даних з різних джерел, включаючи відкриті джерела, індустріальні форуми та інші інтелектуальні мережі. Цей підрозділ може діяти як ранній індикатор потенційних загроз, дозволяючи компанії вживати профілактичні заходи до того, як загроза матеріалізується в реальність.

Враховуючи важливість даних у сучасному бізнес-ландшафті, "Інфосейф" може також інвестувати в розробку розширених технологій шифрування даних, які забезпечують захист інформації в будь-якому стані — при передачі, зберіганні чи обробці. Сучасні методи шифрування, як-от квантове шифрування або шифрування на основі передових математичних алгоритмів, можуть значно підвищити захищеність критичних даних. (табл. 3.2)

Таблиця 3.2

Стратегії вдосконалення інформаційної безпеки для ТОВ «Інфосейф»

Стратегії	Опис
Залучення зовнішніх аудиторів	Використання незалежних експертів для аудиту існуючих безпекових механізмів, виявлення сліпих плям і рекомендацій щодо покращення згідно з глобальними стандартами.

Розробка плану реагування на інциденти	Створення чітких процедур для кожного рівня організації щодо дій у випадку безпекових порушень, що забезпечить швидке відновлення роботи і мінімізацію збитків.
Створення відділу кібер-розвідки	Введення спеціалізованого підрозділу для моніторингу і аналізу потенційних загроз з використанням передових аналітичних засобів.

Інвестиції в сучасні технології шифрування	Розробка та впровадження передових методів шифрування, зокрема квантового шифрування, для забезпечення захисту даних на всіх етапах їх життєвого циклу.
Підтримка корпоративної культури безпеки	Виховання у співробітників розуміння їхньої ролі в забезпеченні інформаційної безпеки через регулярні тренінги, акцент на важливості їхньої участі у захисті корпоративних інформаційних активів.

Таблиця 3.2 представляє стратегічний підхід до підвищення рівня інформаційної безпеки в ТОВ "Інфосейф". Описані стратегії є частиною комплексної програми, спрямованої на створення надійної та ефективної системи захисту інформаційних активів компанії. Включення зовнішніх аудиторів дозволить забезпечити об'єктивність оцінки безпекових заходів, в той час як розробка детального плану реагування на інциденти зміцнить здатність компанії швидко відновлюватися після можливих кібератак. Створення відділу кібер-розвідки і впровадження новітніх технологій шифрування нададуть компанії додаткові інструменти для протидії сучасним загрозам. Важливим є також неперервне виховання і підтримка корпоративної культури безпеки, що залучає кожного співробітника до процесу захисту інформації. Ці заходи, в сукупності, формують стійку основу для захисту корпоративних даних і підтримки безперервності бізнесу.

Запропоновані рекомендації дозволяють підвищити ефективність, обґрунтованість та адаптивність процесів планування інформаційної безпеки, забезпечити їх відповідність сучасним вимогам та викликам, а також створити

надійну основу для захисту інформаційних активів та безперервності ведення бізнесу підприємства.

Проте, важливо розуміти, що вдосконалення планування інформаційної безпеки є безперервним процесом, який вимагає постійної уваги, зусиль та ресурсів з боку керівництва та всіх співробітників підприємства. Лише за умови послідовної та систематичної роботи з реалізації наведених рекомендацій можливо досягти дійсно значущих та стійких результатів у забезпеченні інформаційної безпеки підприємства.

Висновки до розділу 3

Було досліджено та розроблено рекомендації щодо вдосконалення процесів планування інформаційної безпеки на підприємстві. Зокрема, було визначено ключові процеси планування інформаційної безпеки на прикладі ТОВ "Інфосейф", а також запропоновано комплексний набір рекомендацій щодо їх оптимізації та вдосконалення.

Визначення процесів планування інформаційної безпеки на ТОВ "Інфосейф" здійснювалось з використанням підходу, заснованого на міжнародному стандарті ISO/IEC 27001:2013. Було виділено п'ять ключових етапів планування: визначення контексту та цілей організації, ідентифікація та оцінка ризиків, розробка та впровадження заходів безпеки, моніторинг та перегляд ефективності заходів, а також постійне вдосконалення СУІБ. Дотримання цих етапів дозволяє створити надійну та стійку систему управління інформаційною безпекою на підприємстві.

Для вдосконалення процесів планування інформаційної безпеки було запропоновано двадцять рекомендацій, які охоплюють різноманітні аспекти та фактори, від забезпечення підтримки керівництва та інтеграції з бізнес-процесами до впровадження автоматизованих інструментів та практик безперервного вдосконалення. Ці рекомендації дозволяють підвищити ефективність, обґрунтованість та адаптивність планування інформаційної безпеки, забезпечити його відповідність сучасним вимогам та викликам, а

також створити надійну основу для захисту інформаційних активів підприємства.

Проте, важливо розуміти, що вдосконалення планування інформаційної безпеки є безперервним процесом, який вимагає постійної уваги, зусиль та ресурсів з боку керівництва та всіх співробітників підприємства. Лише за умови послідовної та систематичної роботи з реалізації наведених рекомендацій можливо досягти дійсно значущих та стійких результатів у забезпеченні інформаційної безпеки.

Подальші дослідження в цій сфері можуть бути спрямовані на розробку більш деталізованих методик та інструментів для реалізації запропонованих рекомендацій, а також на вивчення та узагальнення кращих практик планування інформаційної безпеки на підприємствах різних галузей та масштабів. Крім того, важливим напрямком подальших досліджень є оцінка ефективності та результативності впровадження розроблених рекомендацій на практиці, а також їх адаптація та вдосконалення з урахуванням отриманого досвіду та зворотного зв'язку від підприємств.

ВИСНОВКИ

У даній роботі було проведено комплексне дослідження теоретичних та прикладних аспектів планування інформаційної безпеки на підприємстві, а також розроблено рекомендації щодо вдосконалення цих процесів.

У першому розділі роботи було розглянуто сутність та особливості інформаційної безпеки підприємства, проаналізовано нормативно-правову базу забезпечення інформаційної безпеки в Україні, а також досліджено основні методи та інструменти планування інформаційної безпеки. Було встановлено, що інформаційна безпека є невід'ємною складовою загальної системи безпеки підприємства та вимагає комплексного підходу, який враховує технічні, організаційні, правові та людські аспекти. Ефективне планування інформаційної безпеки повинно базуватись на ретельному аналізі ризиків, використанні сучасних методологій та інструментів, а також забезпечувати відповідність регуляторним вимогам та стандартам.

У другому розділі роботи було проведено аналіз процесів планування інформаційної безпеки на прикладі конкретного підприємства. За результатами аналізу було виявлено ряд недоліків та проблемних місць, зокрема, недостатню увагу до етапу інвентаризації інформаційних активів, низький рівень залученості керівництва та персоналу, недостатнє використання кількісних методів оцінки ризиків, слабку автоматизацію процесів планування тощо. Для усунення цих недоліків було запропоновано ряд заходів з оптимізації процедур планування інформаційної безпеки на підприємстві.

У третьому розділі роботи було розроблено комплекс рекомендацій щодо вдосконалення процесів планування інформаційної безпеки на підприємстві. Ці рекомендації охоплюють різноманітні аспекти та фактори, від забезпечення підтримки керівництва та інтеграції з бізнес-процесами до впровадження автоматизованих інструментів та практик безперервного вдосконалення. Дотримання цих рекомендацій дозволить суттєво підвищити ефективність, обґрунтованість та адаптивність процесів планування інформаційної безпеки,

забезпечити їх відповідність сучасним вимогам та створити надійну основу для захисту інформаційних активів підприємства.

Таким чином, в результаті проведеного дослідження було досягнуто поставленої мети та виконано всі визначені завдання. Розроблені рекомендації мають високу практичну цінність і можуть бути використані в діяльності підприємств різних галузей та масштабів для вдосконалення процесів планування інформаційної безпеки та підвищення рівня захищеності інформаційних активів.

Проте, варто зазначити, що вдосконалення процесів планування інформаційної безпеки є безперервним процесом, який вимагає постійної уваги та зусиль з боку керівництва та персоналу підприємства. Лише за умови послідовної та систематичної роботи з реалізації запропонованих рекомендацій можливо досягти сталих та значущих результатів у забезпеченні інформаційної безпеки.

Перспективними напрямками подальших досліджень в цій сфері можуть бути розробка галузевих моделей та методик планування інформаційної безпеки, створення автоматизованих систем підтримки прийняття рішень в цій сфері, дослідження економічних аспектів забезпечення інформаційної безпеки, а також вивчення кращих світових практик та досвіду провідних компаній в цій галузі.

Результати даного дослідження можуть бути використані не лише в практичній діяльності підприємств, але й в освітньому процесі при підготовці фахівців з інформаційної безпеки, а також в науково-дослідній роботі для подальшого розвитку теоретико-методологічних засад забезпечення інформаційної безпеки на підприємствах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека: навчальний посібник / О.М. Богуш, В.Л. Бурячок, Ю.В. Борсуковський та ін. – Київ: ДУІКТ, 2018. – 450 с.

2. Інформаційна безпека: навчальний посібник / В.А. Лужецький, А.В. Войтович, О.П. Дудатьєв та ін. – Вінниця: ВНТУ, 2019. – 240 с.

3. Управління інформаційною безпекою: навчальний посібник / В.О. Хорошко, М.В. Ліпкан та ін. – Київ: ЦУЛ, 2020. – 328 с.

4. Інформаційна безпека в системі економічної безпеки підприємства: монографія / А.О. Пашко, В.А. Ткачук, С.В. Казмірчук та ін. – Київ: Видавництво Ліра-К, 2021. – 180 с.

5. Ткачук Т.Ю. Інформаційна безпека: сучасні підходи до визначення та принципи забезпечення / Т.Ю. Ткачук // Економіка та держава. – 2019. – № 4. – С. 109-113.

6. Інформаційна безпека підприємства: навчальний посібник / В.І. Андрєєв, В.Д. Козюра, Л.М. Скачек та ін. – Київ: Кондор, 2018. – 240 с.

7. Лазаренко В.І. Інформаційна безпека та економічна розвідка: навчальний посібник / В.І. Лазаренко, О.В. Хорошко, Л.М. Скачек. - Київ: Вид-во КНЕУ, 2019. - 240 с.

8. Гнатюк С.О. Основи інформаційної безпеки: навчальний посібник / С.О. Гнатюк. - Київ: КПІ ім. Ігоря Сікорського, 2018. - 180 с.

9. Нормативно-правове забезпечення інформаційної безпеки України: монографія / В.Г. Пилипчук, О.П. Дзьобань, В.М. Брижко та ін.; за ред. В.Г. Пилипчука. - Київ: ТОВ «ПанТот», 2020. - 288 с.

10. Інформаційна безпека України: правові аспекти: навчальний посібник / О.В. Кохановська, О.І. Яременко, О.М. Ващук та ін.; за ред. О.В. Кохановської. - Київ: Видавничий дім «Гельветика», 2021. - 276 с.

11. Богуш В.М., Юдін О.К. Теоретичні основи захисту інформації: навчальний посібник. - Київ: ТОВ «ДКС Центр», 2019. - 320 с.

12. Правове забезпечення інформаційної безпеки України: навчальний посібник / О.Д. Довгань, І.М. Доронін, Т.Ю. Ткачук та ін.; за ред. О.Д. Довганя і І.М. Дороніна. - Київ: Видавничий дім «АртЕк», 2018. - 168 с.

13. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека: навчальний посібник. - Харків: Вид. ХНЕУ, 2019. - 264 с.

14. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 23.05.2024).

15. Мохор В.В., Кравченко Г.М. Методологія управління інформаційною безпекою: монографія. - Київ: Видавництво Ліра-К, 2018. - 264 с.

16. Потій О.В., Коляда Д.С. Управління ризиками інформаційної безпеки: навчальний посібник. - Харків: Вид. ХНЕУ ім. С. Кузнеця, 2020. - 220 с.

17. Мохор В.В., Бакалинський О.М. Оцінювання ризиків інформаційної безпеки: монографія. - Київ: Видавництво Ліра-К, 2021. - 180 с.

18. Кавун С.В., Носов В.В. Інформаційна безпека: навчальний посібник. - Харків: Вид. ХНЕУ, 2019. - 264 с.

19. Бурячок В.Л., Соколов В.Ю. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. - Київ: ДУТ, 2020. - 500 с.

20. Олійник О.В., Чередниченко Ю.В. Планування інформаційної безпеки: навчальний посібник. - Київ: Видавничий дім «Кондор», 2021. - 350 с.

21. Мохор В.В., Покровський В.О. Розробка політик інформаційної безпеки: навчальний посібник. - Київ: Видавництво Ліра-К, 2022. - 280 с.

22. Іванченко І.С. Інформаційна безпека підприємства: принципи, методи, інструменти: монографія / І.С. Іванченко, О.В. Гавриш. - Київ: КНЕУ, 2021. - 320 с.

23. Бурячок В.Л. Основи інформаційної та кібербезпеки: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. - Київ: ДУТ, 2018. - 288 с.

24. Інформаційна безпека: навчальний посібник / Ю.Я. Самохвалов, С.О. Гнатюк, М.О. Рябий, Л.М. Ткачук. - Київ: Видавничий дім "Кондор", 2022. - 446 с.

25. Кібербезпека: монографія / О.В. Потій, В.В. Лукацький, М.М. Новіков, В.С. Черниш. - Харків: ТОВ "ДІСА ПЛЮС", 2023. - 400 с.

26. Інформаційна безпека України: монографія / за заг. ред. В.І. Ткаченка. - Київ: Видавничий дім "Артек", 2020. - 432 с.

27. Гладиш С. В. Планування інформаційної безпеки підприємства: навчальний посібник / С. В. Гладиш, О. В. Карпенко. - Київ: КНЕУ, 2022. - 320 с.

28. Інформаційна безпека: навчальний посібник / П. М. Складанний, М. В. Карпінський, Я. І. Кінах та ін. - Львів: Новий Світ-2000, 2021. - 280 с.

29. Управління інформаційною безпекою: монографія / В. В. Мохор, О. М. Богданов, О. М. Крук та ін. - Київ: Видавництво Ліра-К, 2020. - 380 с.

30. Брижко В. М. Організаційно-правові основи інформаційної безпеки: навчальний посібник / В. М. Брижко, О. А. Баранов, В. С. Цимбалюк. - Київ: ТОВ "ІТ право", 2019. - 420 с.

31. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія / О. Д. Довгань. - Київ: Видавничий дім "АртЕк", 2018. - 425 с.

32. Гнатюк С. О. Кібербезпека та захист критичної інформаційної інфраструктури: навчальний посібник / С. О. Гнатюк, В. М. Сидоренко, Ю. М. Пархоменко. - Київ: НТУУ "КПІ імені Ігоря Сікорського", 2022. - 400 с.

33. Гладиш С. В. Планування інформаційної безпеки підприємства: навчальний посібник / С. В. Гладиш, О. В. Карпенко. - Київ: КНЕУ, 2022. - 320 с.

34. Гнатюк С. О. Кібербезпека та захист критичної інформаційної інфраструктури: навчальний посібник / С. О. Гнатюк, В. М. Сидоренко, Ю. М. Пархоменко. - Київ: НТУУ "КПІ імені Ігоря Сікорського", 2022. - 400 с.

35. Управління інформаційною безпекою: монографія / В. В. Мохор, О. М. Богданов, О. М. Крук та ін. - Київ: Видавництво Ліра-К, 2020. - 380 с.

36. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія / О. Д. Довгань. - Київ: Видавничий дім "АртЕк", 2018. - 425 с.

37. Інформаційна безпека: навчальний посібник / П. М. Складанний, М. В. Карпінський, Я. І. Кінах та ін. - Львів: Новий Світ-2000, 2021. - 280 с.

38. Грайворонський М.В. Безпека інформаційно-комунікаційних систем: монографія / М.В. Грайворонський, О.М. Новіков. - Київ: Видавнича група BHV, 2021. - 608 с.

39. Дудикевич В.Б. Інформаційна безпека держави: навчальний посібник / В.Б. Дудикевич, І.Р. Опірський, П.І. Гаранюк. - Львів: Видавництво Львівської політехніки, 2018. - 580 с.

40. Інформаційна безпека: навчальний посібник / О.В. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2021. - 364 с.

41. Лужецький В.А. Основи інформаційної безпеки: навчальний посібник / В.А. Лужецький, А.В. Войтович, О.П. Дудатьєв. - Вінниця: ВНТУ, 2019. - 240 с.

42. Мехед Д.Б. Оцінювання ефективності системи інформаційної безпеки: теорія та практика: монографія / Д.Б. Мехед. - Чернігів: ЧНТУ, 2020. - 362 с.

43. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. - Київ: НІСД, 2018. - 496 с.

44. Дорофеєв А.В. Управління інформаційною безпекою: навчальний посібник / А.В. Дорофеєв, О.М. Горбенко, С.В. Зибін. - Харків: ХНЕУ ім. С. Кузнеця, 2018. - 312 с.

45. Іванченко І.С. Інформаційна безпека підприємства: принципи, методи, інструменти: монографія / І.С. Іванченко, О.В. Гавриш. - Київ: КНЕУ, 2021. - 320 с.

46. Конеєв С.О. Методологія управління ризиками інформаційної безпеки: навчальний посібник / С.О. Конеєв, О.Г. Корченко, В.А. Козачок. - Київ: НАУ, 2019. - 408 с.

47. Малюк А.О. Аудит інформаційної безпеки: підручник / А.О. Малюк, В.В. Собінов, М.М. Єрмошин. - Київ: ДУТ, 2020. - 362 с.

48. Юдін О.К. Безпека інформаційних систем і технологій: навчальний посібник / О.К. Юдін, О.О. Лапінський, С.О. Новак. - Київ: НАУ, 2022. - 288 с.

49. Легомінова С.В. Управління інформаційними ризиками: навчальний посібник / С.В. Легомінова, О.І. Пластун, Т.М. Булах. - Суми: ДВНЗ "УАБС НБУ", 2018. - 208 с.

50. Манжай О.В. Інформаційна безпека: навчальний посібник / О.В. Манжай, О.М. Гладкова, С.О. Спасітєлєва. - Харків: ХНУВС, 2020. - 268 с.

51. Мехед Д.Б. Ризик-орієнтований підхід в інформаційній безпеці: монографія / Д.Б. Мехед, В.В. Базилевич, А.В. Слободяник. - Чернігів: ЧНТУ, 2021. - 224 с.

52. Петренко С.А. Методи і засоби забезпечення кібербезпеки: навчальний посібник / С.А. Петренко, В.А. Лахно, А.І. Гізун. - Київ: ДУТ, 2019. - 304 с.

53. Управління ризиками інформаційної безпеки: монографія / О.Г. Корченко, В.Л. Бурячок, Д.А. Горніцька, Б.А. Ахметов. - Київ: ДУІКТ, 2022. - 188 с.

54. Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В. Л. Бурячок, С. В. Толюпа, А. О. Аносов, В. А. Козачок, Н. В. Лукова-Чуйко. – Київ: ДУТ, 2015. – 345 с.

55. Дудикевич В. Б., Гарасим Ю. Р., Гарасим М. Ю., Захарова М. Я. Інформаційна безпека держави: навчальний посібник / В. Б. Дудикевич, Ю. Р. Гарасим, М. Ю. Гарасим, М. Я. Захарова. – Львів: Видавництво Львівської політехніки, 2019. – 280 с.

56. Ісмайлов А. А., Кінзерявий В. М., Пилипенко К. А., Юдін О. К. Основи інформаційної безпеки та захисту інформації: навчальний посібник / А. А. Ісмайлов, В. М. Кінзерявий, К. А. Пилипенко, О. К. Юдін. – Київ: НАУ, 2020. – 232 с.

57. Конеєв С. О., Кущ С. М., Лазарєв М. В. Інформаційна безпека в умовах цифрової трансформації: навчальний посібник / С. О. Конеєв, С. М. Кущ, М. В. Лазарєв. – Ірпінь: УДФСУ, 2021. – 392 с.

58. Лужецький В. А., Войтович О. П., Дудатьєв А. В., Баранов О. А., Гавловський В. Д. Основи інформаційної безпеки: навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв, О. А. Баранов, В. Д. Гавловський. – Вінниця: ВНТУ, 2018. – 220 с.

59. Мохор В. В., Богданов О. М., Кіберенко О. С., Крук О. М., Цуркан В. В. Методи і засоби забезпечення інформаційної безпеки критичних інфраструктур: монографія / В. В. Мохор, О. М. Богданов, О. С. Кіберенко, О. М. Крук, В. В. Цуркан. – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2019. – 210 с.

60. Ісмайлов А. А., Кінзерявий В. М., Пилипенко К. А., Юдін О. К. Основи інформаційної безпеки та захисту інформації: навчальний посібник / А. А. Ісмайлов, В. М. Кінзерявий, К. А. Пилипенко, О. К. Юдін. – Київ: НАУ, 2020. – 232 с.

61. Конеєв С. О., Кущ С. М., Лазарєв М. В. Інформаційна безпека в умовах цифрової трансформації: навчальний посібник / С. О. Конеєв, С. М. Кущ, М. В. Лазарєв. – Ірпінь: УДФСУ, 2021. – 392 с.

62. Лужецький В. А., Войтович О. П., Дудатьєв А. В., Баранов О. А., Гавловський В. Д. Основи інформаційної безпеки: навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв, О. А. Баранов, В. Д. Гавловський. – Вінниця: ВНТУ, 2018. – 220 с.

63. Мохор В. В., Богданов О. М., Кіберенко О. С., Крук О. М., Цуркан В. В. Методи і засоби забезпечення інформаційної безпеки критичних інфраструктур: монографія / В. В. Мохор, О. М. Богданов, О. С. Кіберенко, О.

М. Крук, В. В. Цуркан. – Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2019. – 210 с.

64. Павлов В. В., Толюпа С. В., Хорошко В. О., Жуков І. А. Інформаційна безпека та захист інформації: навчальний посібник / В. В. Павлов, С. В. Толюпа, В. О. Хорошко, І. А. Жуков. – Київ: ДУТ, 2020. – 280 с.

65. ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "ІНФОСЕЙФ". URL: https://youcontrol.com.ua/catalog/company_details/32593907/ (дата звернення: 26.05.2024).

66. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Планування та управління інформаційною безпекою: навч. посіб. / В. Б. Дудикевич, В. О. Хорошко, Ю. Є. Яремчук, В. В. Карпінець. – Вінниця: ВНТУ, 2021. – 365 с.

67. Залізняк В. А., Косенко В. В. Методологія управління інформаційною безпекою: монографія / В. А. Залізняк, В. В. Косенко. – Харків: ХНЕУ ім. С. Кузнеця, 2022. – 320 с.

68. Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г. Інформаційна безпека та сучасні мережеві технології: підручник / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – Київ: НАУ, 2019. – 470 с.

69. Корченко О. Г., Дрейс Ю. О., Романов О. І., Бичков І. В. Методи і засоби оцінювання та забезпечення інформаційної безпеки: монографія / О. Г. Корченко, Ю. О. Дрейс, О. І. Романов, І. В. Бичков. – Київ: НАУ, 2020. – 300 с.

70. Семко В. В., Гізун А. І., Гнатюк В. О., Кожухівський А. Д. Організаційне та методичне забезпечення інформаційної безпеки: навч. посіб. / В. В. Семко, А. І. Гізун, В. О. Гнатюк, А. Д. Кожухівський. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 280 с.

71. Шах А.С. Організація планування інформаційної безпеки підприємства. Матеріали Науково-практичної конференції. – Київ: ДУІКТ, 2024. – с.64-67