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: “КОМПЛЕКСНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ”

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

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

Марія СТОЛЯР
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: Здобувачка вищої освіти гр. УБД 42
Марія СТОЛЯР

Керівник:
к.е.н., доцент Тетяна КАПЕЛЮШНА

Рецензент:
д.т.н., професор Галина ГАЙДУР

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 кафедрою УІКБ
_____Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Столяр Марії Ігорівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Комплексний підхід до управління інформаційною безпекою підприємств”

керівник кваліфікаційної роботи Тетяна КАПЕЛЮШНА, к.е.н, доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “25“ травня 2024 р. №195

2. Строк подання кваліфікаційної роботи “25” травня 2024 р

3. Вихідні дані до кваліфікаційної роботи: нормативно-правові акти, законодавство щодо інформаційної безпеки, аналітичні звіти компанії про репутаційні ризики та інформаційну безпеку підприємства, наукові статті та публікації українських та зарубіжних вчених, експертів щодо питань інформаційної безпеки та управління інформаційною безпекою.

4. Перелік питань, які потрібно розробити:

1. Уточнення понять "інформаційно безпека" та "безпека підприємства", визначення основниз загроз інформаційної безпеки для підприємства та розгляд особливостей управління інформаційною безпекою. Опис підходів до управління інформаційною безпеою.
2. Характеристика компанії, аналіз інформаційної безпеки та управління інформаційною безпекою на підприємстві.
3. Виявлення прогалин в наявному підходу до УІБ на підприємстві. Розробка комплексного підходу до УІБ на базі провдених досліджень. Порівняння розробленого комплексного підходу з наявних та визначення переваг.

5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “22” лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	13.03.2024	виконано
2.	Збір та аналіз літератури.	30.03.2024	виконано
3.	Ознайомлення та аналіз досліджуваного підприємства.	08.04.2024	виконано
4.	Аналіз інформаційної безпеки підприємства. Аніліз управління інформаційною безепекою підприємства.	22.04.2024	виконано
5.	Розробка комплексного підходу до управління інформаційною безпекою для підприємства.	09.05.2024	виконано
6.	Формулювання висновків на основі отриманих результатів дослідження.	15.05.2024	виконано
7.	Оформлення роботи.	17.05.2024	виконано
8.	Оформлення презентації.	19.05.2024	виконано
9.	Отримання рецензії на роботу.	03.06.2024	виконано
10.	Захист в ЕК.	13.06.2024	виконано

Здобувач вищої освіти _____ Марія СТОЛЯР
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(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 здобувачка Столяр М.І до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Комплексний підхід до управління інформаційною безпекою підприємств”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка **СТОЛЯР Марія** у кваліфікаційній роботі відповідно до обраної теми, визначила напрями та методи дослідження, опацювала достатній обсяг наукових текстів та матеріалів для розкриття, як теоретичних, так і практичних питань за темою. **СТОЛЯР Марія** продемонструвала розуміння проблематики дослідження та основних теоретичних та практичних напрямів щодо її вирішення, внесла пропозиції щодо розробки компелексного підходу до управління інформаційною безпекою підприємства на досліджуваному підприємстві, проявила себе як організова, відповідальна виконавиця.

Результати дослідження апробовані на конференції, що доводить практичну значимість отриманих результатів.

Вищевикладене дозволяє оцінити виконану кваліфікаційну роботу здобувачкою **СТОЛЯР Марією** на оцінку “відмінно” та присвоїти ій кваліфікацію “Бакалавр з кібербезпеки” за освітньою програмою “Управління інформаційною та кібернетичною безпекою”.

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“___“_____2024 року

Висновок кафедри про кваліфікаційну роботу

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти Столяр Марії
на тему: “Комплексний підхід до управління інформаційною безпекою підприємств”

Актуальність. Інформаційна безпека значиться на сьогодні важливою складовою безпеки, що пояснюється умовами воєнного стану, в яких функціонують підприємства, атаками на інформаційні бази даних та інформаційні ресурси підприємств. Питання захисту інформації та підходів до управління нею безперечно потребують перегляду з метою адаптації до умов сучасності, що актуалізує тематику дослідження кваліфікаційної бакалаврської роботи.

Позитивні сторони

1. У роботі досліджено підходи, які використовуються для управління інформаційною безпекою підприємства в умовах сучасності, вокремлено переваги використання комплексного підходу.
2. Проведено аналіз безпеки інформаційного середовища підприємства, надано його характеристику, проведено оцінку підходу, що використовується на підприємстві та розроблено комплексний підхід до управління інформаційною безпекою підприємства з наданням його переваг.
3. Результати дослідження апробовано на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», що вказує на можливість практичного використання результатів дослідження.

Недоліки

1. Варто було б розглянути питання, як саме покращиться управління інформаційною безпекою підприємства та розписати позитивні зміни щодо захисту інформації у разі його використання, проте, це не є вагомим упущенням та суттєво не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науковому рівні, заслуговує позитивної оцінки, а здобувачка Столяр Марія Ігорівна заслуговує присвоєння кваліфікації «Бакалавр кібербезпеки» за освітньою програмою Управління інформаційною та кібернетичною безпекою”

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра складається з 59 сторінок, включає 10 рисунків, 4 таблиці, 1 схему та базується на 30 джерелах.

Метою роботи дослідити наявну СУІБ на підприємстві та розробити комплексний підхід до УІБ.

Об'єктом дослідження є підходи до управління інформаційною безпекою підприємства

Предметом дослідження – переваги використання комплексного підходу управління інформаційною безпекою підприємства.

Застосовані методи дослідження включають аналіз, дедукцію, матрицю ризиків, порівняння, прогнозування.

Метою дослідження є розробка комплексного підходу до управління інформаційною безпекою підприємства.

Короткий зміст роботи. У роботі були розглянуті поняття «безпека підприємства» та «інформаційна безпека підприємства». У роботі були вивченні підходи до управління інформаційною безпекою. Був проведений аналіз інформаційної безпеки підприємства та управління нею.

У ході поведених досліджень та аналізу був розроблений індивідуальний підхід до управління інформаційною безпекою підприємства.

Галузь застосування. Розроблений комплексний підхід до управління інформаційною безпекою підприємства може бути використаний для покращення безпечності інформаційного поля підприємства та покращення наявної ситуації.

КЛЮЧОВІ СЛОВА: БЕЗПЕКА ПІДПРИЄМСТВА, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА, ПІДХОДИ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА, КОМПЛЕКСНИЙ ПІДХІД.

ABSTRACT

The textual part of the qualification work for the bachelor's degree consists of 62 pages, includes 10 figures, 4 tables, 1 diagram and is based on 30 sources.

The purpose of the work is to study the existing ISMS at the enterprise and develop an integrated approach to ISMS.

Object of research is approaches to enterprise information security management

Subject of research the benefits of using an integrated approach to enterprise information security management.

Research methods. The research methods used include analysis, deduction, risk matrix, comparison, forecasting.

The research methods used include analysis, deduction, risk matrix, comparison, forecasting.

Summary of the work. The paper considers the concepts of “enterprise security” and “enterprise information security”. Approaches to information security management were studied. An analysis of enterprise information security and its management was carried out.

In the course of the conducted research and analysis, an individual approach to the management of enterprise information security was developed**.**

Field of research. The developed integrated approach to enterprise information security management can be used to improve the security of the enterprise information field and improve the current situation.

KEYWORDS: ENTERPRISE SECURITY, ENTERPRISE INFORMATION SECURITY, ENTERPRISE INFORMATION SECURITY MANAGEMENT SYSTEM, APPROACHES TO ENTERPRISE INFORMATION SECURITY MANAGEMENT, INTEGRATED APPROACH.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – Інформаційна безпека

ІТ – Інформаційні технології

ПЗ – Програмне забезпечення

СУБД – Система управління базами даних

СУІБ – Система управління інформаційною безпекою

ЗПЗ – Захист програмного забезпечення

ШПЗ – Шкідливе програмне забезпечення

УІБ – Управління інформаційною безпекою

ІС – Інформаційне середовище

ВСТУП

Актуальність теми. Актуальність обраної теми ґрунтується на створенні економічно вигідного, низьковитратного підходу до управління інформаційною безпекою підприємства, який буде надійним та дієвим в умовах невизначеності функціонування підприємств та постійних інформаційних та кібернетичних атак. Поєднання дієвості та ефективності досяжне лише за системного, комбінованого або ж комбінованого підходів.

Комбінований підхід до УІБ є важливою частиною стратегії кібербезпеки будь-якої організації в наш час. Він може допомогти організаціям ефективніше протистояти кіберзагроз, захистити свої інформаційні активи та відповідати всім регуляторним вимогам. Сучасні кіберзагрози стають все більш складними та різноманітними. Це робить традиційні підходи до УІБ, засновані на одній технології або процесі, недостатньо ефективними. Комбінований підхід до УІБ використовує різні технології, процеси та практики, що дозволяє організаціям ефективніше протистояти цій складності.

Метою роботи є розробка комплексного підходу до управління інформаційною безпекою підприємства.

Об'єктом дослідження є інформаційна безпека підприємства та управління нею

Предметом дослідження – переваги комплексного підхіду управління інформаційною безпекою підприємства.

Застосовані методи дослідження включають аналіз, порівняння, дедукцію, матрицю ризиків, прогнозування.

Тобто робота націлена на вивчення особливостей управління інформаційною безпекою підприємства та розробка індивідуального комплексного підходу до управління інформаційною безпекою.

Аналіз існуючих практик управління інформаційною безпекою на

підприємстві є трудомістким процесом та потребує ретельного збору інформації щодо їх реалізації на підприємствах.

Апробація результатів. Результати кваліфікаційної роботи було апробовано та оприлюднено на ІІІ Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (тези: «Комплексний підхід до управління інформаційною безпекою підприємства»).

РОЗДІЛ 1
КОМПЛЕКСНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

1.1 Безпека та інформаційна безпека підприємства

Безпека підприємства - це комплекс заходів, спрямованих на захист його життєво важливих інтересів від внутрішніх та зовнішніх загроз. Її мета - забезпечити стабільне функціонування та розвиток підприємства в мінливих умовах середовища.

Український науковець Кононов Віталій Владиславович дає визначення поняттю безпека підприємства так: безпека підприємства – це система заходів, спрямованих на захист його від усіх видів загроз, які можуть завдати шкоди його життєво важливим інтересам [28]. С.Ф. Покропивний надає визначення, що безпека підприємства – це система заходів, спрямованих на захист його життєво важливих інтересів в економічній, інформаційній, кадровій, екологічній та інших сферах [29].

Основними функціональними складовими економічної безпеки є: фінансова безпека, інтелектуальна безпека, техніко-технологічна безпека, політико-правова безпека, ресурсна безпека, екологічна безпека, соціальна безпека, інформаційна безпека, силова безпека та безпека праці.

В умовах сучасного світу безпека для підприємства стала критично важливою з огляду на різноманітні загрози. У останні десятиліття світовий процес діджиталізації суспільства призвів до нової актуальної проблеми - інформаційної безпеки. У сучасному світі багато ключових інтересів підприємств залежить від стану інформаційного середовища. Зовнішні або внутрішні впливи на інформаційну сферу можуть становити серйозну загрозу для діяльності підприємства та його інтересів і призводити до різноманітних ризиків і втрат.

Тому в сучасних умовах забезпечення інформаційної безпеки стає невід'ємною умовою для нормального функціонування підприємств. Стало очевидним, що

загальний рівень економічної безпеки підприємства в значній мірі залежить від інформаційної складової.

Інформаційна безпека підприємства- це сукупність заходів, спрямованих на захист інформаційних ресурсів підприємства від несанкціонованого доступу, використання, розголошення, знищення, зміни або порушення їх цілісності. Український науковець Кононов Віталій Владиславович дає визначення поняттю інформаційна безпека підприємства таким чином: інформаційна безпека підприємства – це система заходів, спрямованих на захист інформаційних активів підприємства від несанкціонованого доступу, зміни, знищення або розголошення [28].

На меті інформаційної безпеки - забезпечити конфіденційність, доступність та цілісність інформації, що використовується в діяльності підприємства.

До ключових аспектів інформаційної безпеки належить: підготовка персоналу, захист програмного забезпечення, захист даних, захист інформаційних систем рис. 1.1.

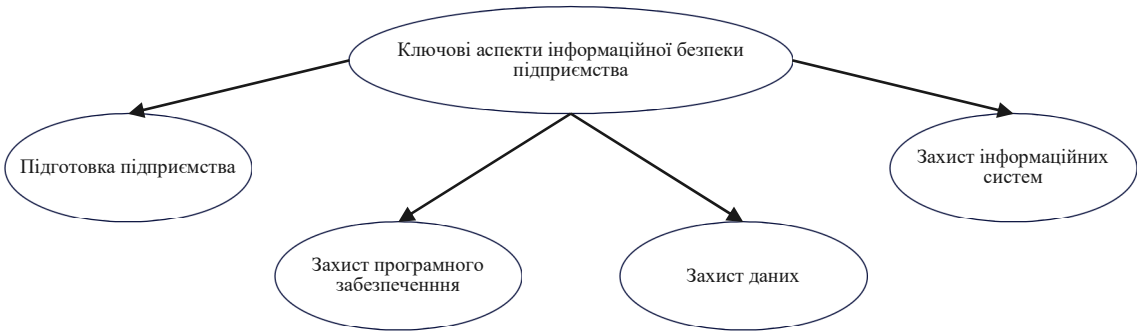

Рис. 1.1. Ключові аспекти забезпечення інформаційної безпеки підприємства

Джерело: складено на основі [28]

У сучасних умовах глобальної діджиталізації ЗПЗ підприємства є найважливішим аспектом інформаційної безпеки. Підприємства володіють великою

кількістю конфіденційних даних, таких як фінансова інформація, дані про клієнтів, комерційні таємниці та некодифікованою інформацією. Витік або втрата цих даних може завдати значної шкоди репутації підприємства, призвести до фінансових втрат та навіть до юридичних наслідків. ЗПЗ допомагає захистити конфіденційні дані від несанкціонованого доступу, використання, розголошення, модифікації, знищення або викрадення.

Кібератаки є однією з найбільш актуальних проблем сучасного світу. Зловмисники постійно вдосконалюють свої методи, використовуючи різноманітні типи кібератак для отримання доступу до чутливої інформації та завдавання шкоди комп'ютерним системам. Підприємство може піддаватися кібератакам. Кібератаки спрямовані на пошкодження важливих документів і систем у корпоративній або персональній комп’ютерній мережі, а також отримання доступу до них. Кібератаки здійснюють як окремі особи, так і цілі організації в політичних, кримінальних або особистих цілях для знищення засекреченої інформації чи отримання доступу до неї [8].

Різноманітність та різновиди кібератак вражають, їх кількість зростає в геометричній прогресії, але основними можна відзначити: шкідливе програмне забезпечення (ШПЗ), фішинг, розподілена атака "відмова в обслуговуванні" (DDoS-атака), міжсайтові сценарії (XSS), бот-мережі, зловмисні програми з вимогою викупу рис 1.2 [8].

Шкідливе програмне забезпечення (ШПЗ) - це програмне забезпечення, спеціально розроблене зловмисниками для завдавання шкоди комп'ютерним системам. Воно може бути замасковане під надійні джерела, такі як електронні листи, вкладення або файли, що робить його складним для виявлення, ШПЗ може потрапити до ОС підприємства через: електронну пошту, веб-сайти, піратське програмне забезпечення, USB-накопичувачі.

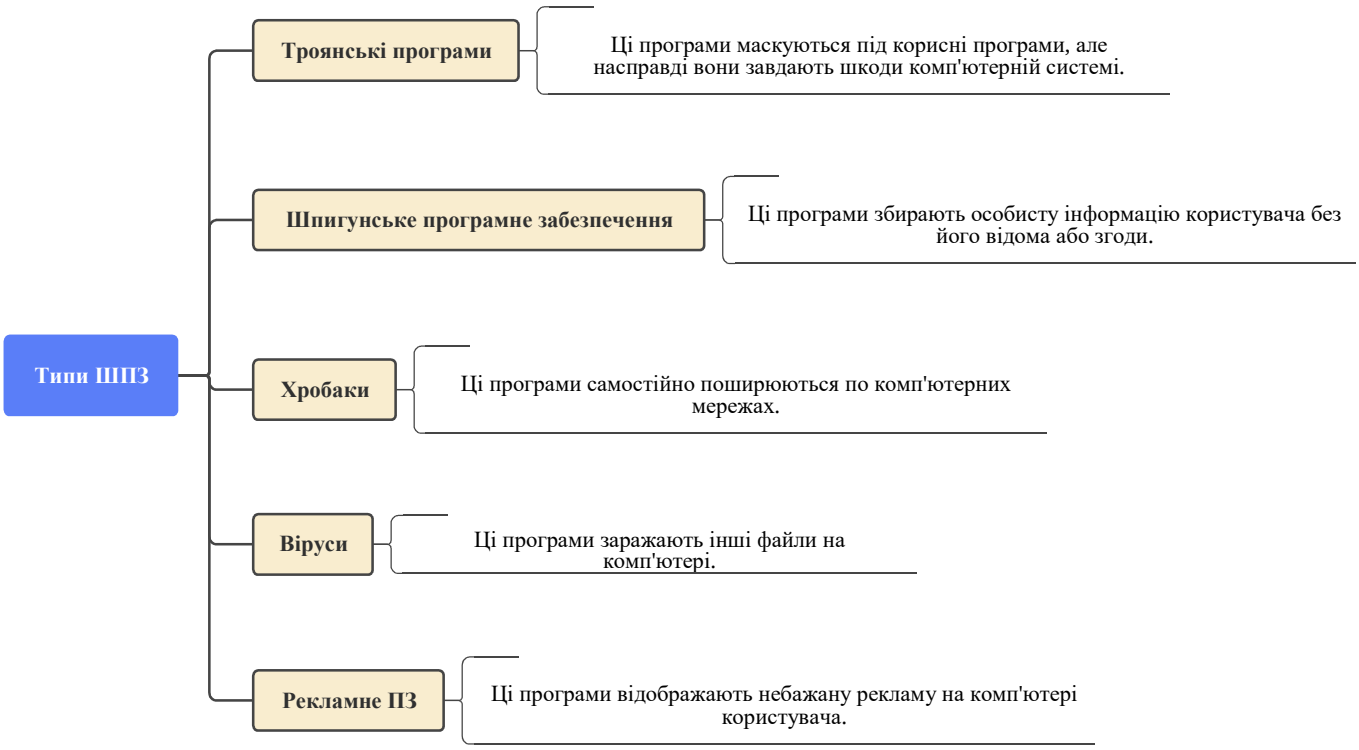

Рис. 1.2. Типи ШПЗ

Джерело: складено на основі [1, 6].

ШПЗ може завдати значної шкоди комп'ютерним системам та їхнім користувачам і підприємству в цілому. Шкідливе програмне забезпечення може збирати інформацію про кредитні картки, паролі та інші особисті дані. Віруси та інші типи шкідливі ПЗ можуть пошкодити або знищити файли на комп'ютері. Хробаки та можуть самостійно поширюватися по комп'ютерних мережах, заражаючи інші комп'ютери. ШПЗ може зробити комп'ютер непридатним до використання, сповільнити його роботу або зробити його нестабільним. Також ШПЗ може нанести величезні наслідки для ІТ-мережі підприємства, що призведе до значних фінансових втрат та втрати репутації тощо.

Фішинг також має велику актуальність в сучасних реаліях. Фішинг – це метод соціальної інженерії, який використовується для обману людей з метою розголошення конфіденційної інформації, такої як паролі або номери кредитних карток. Фішингові атаки можуть бути здійснені через електронну пошту, веб-сайти або текстові повідомлення. Необізнаність працівників підприємства - це одна з найпоширеніших

причин успішності фішингових атак. Працівники, які не знають про ризики фішингу, можуть легко бути обмануті зловмисниками та розголосити конфіденційну інформацію яка зберігається на підприємстві та подекуди може нести стратегічно важливе значення для об’єкту господарювання.

Атаки відмови в обслуговуванні (DoS) - це тип кібератаки, спрямований на те, щоб зробити комп'ютерну систему або веб-сайт недоступним для користувачів. Зловмисники надсилають велику кількість запитів на веб-сервер, що призводить до його перевантаження та відмови в обслуговуванні законних користувачів. Це може повести за собою великі фінансові втрати для підприємства, через простої та втрату продажів.

Міжсайтові сценарії (XSS) - це тип кібератаки, який використовує вразливості в веб-додатках для введення шкідливого коду JavaScript на веб-сторінку. Цей код може бути використаний для крадіжки конфіденційної інформації, перенаправлення користувачів на шкідливі веб-сайти або для інших зловмисних цілей. Дана кібератака може завдати сутєвих збитків для компанії, оскільки XSS-атаки можуть бути використані для крадіжки конфіденційної інформації, такої як паролі, номери кредитних карток або дані про клієнтів, здійснення шахрайства або крадіжки коштів, також завдати шкоди репутації підприємства та призвести до втрати клієнтів.

У сучасному цифровому світі інформація є одним із найцінніших активів підприємства.Вона може включати конфіденційні дані про клієнтів, фінансову інформацію, інтелектуальну власність та інші важливі бізнес-дані. Втрата або крадіжка цієї інформації може призвести до серйозних наслідків, таких як фінансові втрати, пошкодження репутації та навіть банкрутство.

Розробка моделі інформаційної безпеки (ІБ) може допомогти підприємствам захистити свої інформаційні активи від кіберзагроз. Модель інформаційної безпеки – це сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на інформаційну безпеку підприємства та на збереження матеріальних та інформаційних ресурсів. До цих об'єктивних чинників належать наступні: загрози інформаційній безпеці, які характеризуються вірогідністю

виникнення і реалізації загроз; вразливості інформаційної системи або системи контрзаходів, які впливають на вірогідність реалізації загроз для підприємства;

економічний ризик – чинник, що відображає можливі збитки підприємства в результаті реалізації загрози інформаційній безпеці: витік інформації та неправомірне її використання, і як наслідок, вірогідні прямі та непрямі фінансові збитки.

1.2. Особливості управління інформаційною безпекою підприємства

Управління інформаційною безпекою (УІБ) - це невід'ємна частина системи управління підприємством, яка ґрунтується на аналізі ризиків і має на меті проектувати, впроваджувати, контролювати, супроводжувати та вдосконалювати заходи з захисту інформації.

Як зазначають науковеці Іванченко Н.О. та Подскребко О.С. у своїй науковій статті «Особливості реалізації системи управлінн інформаційною безпекою», Управління інформаційною безпекою – це невід’ємна складова загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. До цієї системи входять організаційні структури, інформаційна політика, дії з планування, обов'язки, процедури, процеси і ресурси [9].

Управління інформаційною безпекою - є постійним процесом, що включає такі етапи: усвідомлення необхідності захисту інформації та постановка завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінка інформаційних ризиків; планування заходів щодо обробки ризиків; реалізація та впровадження відповідних механізмів контролю; розподіл ролей та відповідальності, навчання та мотивація персоналу; оперативна робота щодо здійснення захисних заходів; моніторинг

функціонування механізмів контролю та оцінка їх ефективності; відповідні коригувальні впливи на основі результатів моніторингу.

Історично управління інформаційною безпекою здебільшого покладалося на технічні заходи контролю; однак дослідження показали, що більшість збоїв інформаційної безпеки трапляються через порушення засобів контролю з боку персоналу, якому довіряють. Це свідчить про те, що управління інформаційною безпекою може бути адекватно забезпечене лише тоді, коли акцент виходить за межі технічного контролю і включає в себе бізнес-процеси та організаційні питання. Управління інформаційною безпекою в першу чергу стосується стратегічних, тактичних та оперативних питань, пов'язаних з плануванням, аналізом, розробкою, впровадженням та підтримкою програми інформаційної безпеки організації. Деякі з найбільш важливих питань включають оцінку активів, аудит, планування безперервності бізнесу, планування аварійного відновлення, етику, організаційну комунікацію, розробку політики, планування проектів, управління ризиками, освіту/тренінги з питань безпеки, а також різні юридичні питання, такі як відповідальність і дотримання нормативних вимог.

В ідеалі, діяльність з управління інформаційною безпекою повинна визначатися цілями організації, щоб жодні ресурси не витрачалися на безпеку без чіткого задокументованого розуміння того, як вона підтримує місію організації. Історично управління інформаційною безпекою полягало виключно у встановленні технічних та фізичних засобів контролю. Однак, зростаюче використання, цінність і залежність від комп'ютеризованих систем для підтримки реальних операцій підвищили важливість включення процесних і організаційних питань в управління ризиками безпеки. Управління ризиками інформаційної безпеки, процес, що використовується для визначення оптимальної стратегії захисту в умовах обмеженого бюджету на безпеку, перетворилося на необхідну функцію в організаціях, які стурбовані своєю здатністю пом'якшити наслідки порушення інформаційної безпеки. Такі порушення називаються «інцидентами». Аналіз ризиків, перший крок процесу

управління ризиками, вимагає ідентифікації та документування критично важливих організаційних ресурсів (наприклад, інформації, людей, процесів і технологій) серед величезної кількості загальних інформаційних ресурсів, які використовуються для підтримки місії організації. Визначення критичності не є тривіальним. Воно вимагає оцінки цінності, яку ресурс надає організації, виходячи з того, як він підтримує стратегічні цілі організації. Масштаб і складність організації, взаємозалежності між ресурсами та динамічний характер використання ресурсів значно ускладнюють визначення вартості. Однак точна оцінка ресурсів є необхідною, оскільки вона безпосередньо впливає на якість рішень, що приймаються під час управління. Оцінка, разом з оцінкою загроз, вразливостей та ймовірності (за одиницю часу) їх перетину, використовується для визначення потенційної шкоди ресурсу з огляду на стан організаційної спроможності забезпечення безпеки. У сукупності ця інформація дає можливість впорядкувати ризики і вирішувати їх шляхом уникнення (наприклад, процеси змін), передачі (наприклад, аутсорсинг), пом'якшення (наприклад, застосування заходів контролю) або прийняття (наприклад, змиритися з можливими втратами), співмірними з цінністю ресурсу.

Належне повсякденне та стратегічне управління операціями з інформаційної безпеки є одним з найважливіших факторів успіху в досягненні цілей організації. Науковець Дональд Піпкін визначає циклічний, п’ятифазний процес для концептуалізації процесу управління інформаційною безпекою: перевірка, захист, виявлення, реагування та рефлексія [19]. Етап перевірки вимагає ідентифікації, оцінки та розподілу прав власності на інформаційні активи, що є критично важливими для організації; етап захисту вимагає призначення заходів контролю для захисту критично важливих інформаційних активів, співмірних з їх цінністю; етап виявлення вимагає розробки надійних засобів виявлення для забезпечення своєчасного виявлення будь-яких порушень в організації; етап реагування вимагає, щоб організація розробила ресурси та можливості для швидкого реагування, локалізації, розслідування та

усунення порушень; а етап аналізу вимагає ефективного документування після інциденту, звітності та підзвітності для забезпечення інституційного навчання. Дональд Піпкін стверджує, що забезпечення організаційної безпеки вимагає врахування всіх п'яти фаз рис 1.2 [19].

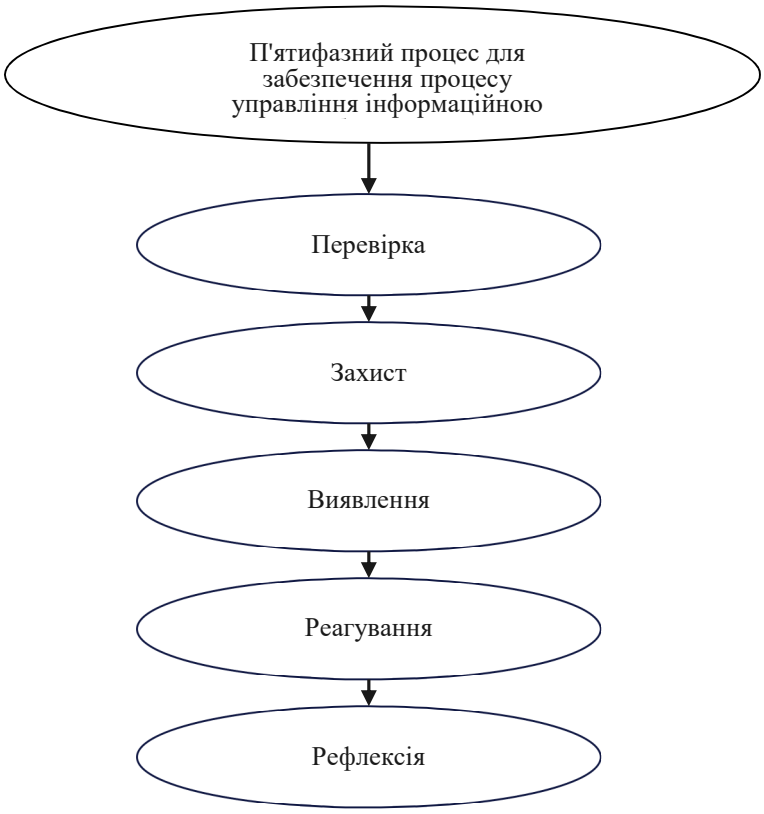

Рис.1.2 П'ятифазний процес для забезпечення процесу управління інформаційною безпекою

Джерело: складено на основі [19].

Нехтування будь-якою з п’яти фаз може наразити організацію на надмірні втрати, коли вона неминуче зіткнеться з інформаційним інцидентом.

1.3 Підходи до управління інформаційною безпекою підприємства

Інформаційні небезпеки для бізнесу формуються інформаційними загрозами, які поширюються через інформаційний простір та комунікації. Тому інформаційна безпека визначає економічну безпеку підприємства.

Зрештою, інформаційний ризик, які інші види ризику, є потенційною загрозою збитковості підприємств.

Підхід до управління ІБ підприємства повинен бути комплексним, ґрунтуватися на системному аналізі та охоплювати всі аспекти захисту інформаційних активів [28].

Комплексний підхід до управління ІБ передбачає поєднання організаційних, технічних та програмно-технічних заходів, спрямованих на захист інформаційних ресурсів підприємства [29].

Використання підходів до управління ІБ є вкрай важливим для підприємств з наступних причин:

1. Захист інформаційних активів:
    - Підприємства володіють цінними інформаційними активами, такими як дані про клієнтів, фінансова інформація, інтелектуальна власність.
    - Використання підходів до ІБ допомагає захистити ці активи від несанкціонованого доступу, зміни, знищення або розголошення.
2. Зниження ризиків
    - Інформаційні загрози, такі як кібератаки, можуть завдати значної шкоди підприємству, призвести до фінансових втрат, втрати репутації, перебоїв у роботі.
    - Використання підходів до ІБ допомагає виявити, оцінити та управляти цими ризиками, знижуючи ймовірність їх виникнення та пом'якшуючи їх наслідки.
3. Підвищення конкурентоспроможності:
    - Захист інформаційних активів та дотримання норм ІБ сприяє довірі з боку клієнтів та партнерів, що може позитивно вплинути на конкурентоспроможність.

Створення комплексної системи управління інформаційною безпекою повинно базуватися саме на підходах до управління інформаційною безпекою підприємства. Підходів до УІБ підприємства налічується безліч, в даній

роботі розглядатимуться основні: проактивний підхід, реактивний підхід, комбінований підхід, функціональний підхід, ансамблевий підхід.

Проактивний підхід до управління інформаційною безпекою (ІБ) підприємства ґрунтується на превентивних заходах, спрямованих на попередження виникнення інцидентів ІБ. Він передбачає виявлення та оцінку потенційних загроз, вразливостей та ризиків для інформаційних ресурсів підприємства до того, як вони можуть завдати шкоди.

Концептуальними засади проактивного підходу до управління інформаційною безпекою підприємства є: прогнозування, превенція, неперервність. В розрізі проактивного підходу до УІБ прогнозування має на увазі виявлення та аналіз потенційних загроз ІБ, які можуть виникнути в майбутньому. Що забезпечить завчасне виявлення та розуміння потенційних загроз дозволить вжити заходів для їх запобігання або мінімізації їхніх наслідків, допомагає вибудувати розуміння про пріоритетні загрози підприємству в майбутньому, та допоможе оптимізувати витрати на ІБ а також зосередити ресурси на найважливіших напрямках захисту. Прогнозування ймовірних сценаріїв інцидентів ІБ дає змогу розробити плани та процедури реагування, що дозволить мінімізувати час простою та збитки.

Превентивний захід ІБ є одним із концептуальних засад проактивного підходу до управління інформаційною безпекою. Метою проактивного заходу є запобігання виникненню інцидентів ІБ, мінімізація наслідків інцидентів, забезпечення відповідності нормативним вимогам. Впровадження заходів захисту, спрямованих на усунення причин та факторів, що можуть призвести до інцидентів ІБ. Якщо інцидент все ж таки стався, превентивні заходи допоможуть мінімізувати його негативні наслідки, такі як втрата інформації, порушення роботи систем, фінансові збитки тощо. Багато галузей мають нормативні вимоги до ІБ, які підприємства зобов'язані дотримуватися. Превентивні заходи допомагають підприємствам відповідати цим вимогам. Проактивний підхід до управління ІБ є найефективнішим способом захисту інформаційних ресурсів підприємства. Він дозволяє попередити виникнення

інцидентів ІБ та мінімізувати їхні наслідки, що, в свою чергу, сприяє стабільному розвитку та успіху підприємства.

Реактивний підхід до управління інформаційною безпекою (ІБ) підприємства ґрунтується на реагуванні на інциденти ІБ після їх виникнення. Цей підхід передбачає: розпізнання та фіксація факту порушення ІБ; визначення причини, масштабів та наслідків інциденту; відновлення пошкоджених даних та систем, а також мінімізація збитків, завданих інцидентом; внесення змін до системи ІБ для усунення причин, які призвели до інциденту. Концептуальними засадами реактивного підходу є: виявлення інциденту, розслідування інциденту, ліквідація наслідків інциденту, запобігання повторенню інциденту. Головними перевагами реактивного підходу в управлінні інформаційною безпекою підприємства є простота та легкість впровадження, оскільки реактивний підхід не потребує значних початкових інвестицій та ресурсів. Це може бути особливо актуально для малих та середніх підприємств, які мають обмежений бюджет на ІБ. Реактивний підхід дозволяє зосередитися на конкретних інцидентах ІБ та їх наслідках. Це може бути корисно для вивчення причин інциденту та вдосконалення системи ІБ. Реактивний підхід дає можливість вивчити причини інцидентів ІБ та вжити заходів для їх запобігання в майбутньому. Це може допомогти підприємству підвищити стійкість до кібератак. Реактивний підхід до управління ІБ має як свої переваги, так і недоліки. Він може бути простим та легким у впровадженні, але не гарантує попередження інцидентів ІБ та може призвести до значних збитків. Тому реактивний підхід рекомендується використовувати лише у поєднанні з проактивними заходами, такими як аналіз ризиків, впровадження заходів захисту та моніторинг системи ІБ.

Комплексний підхід до управління інформаційною безпекою (ІБ) підприємства поєднує в собі елементи проактивного та реактивного та функціонального підходів. Він ґрунтується на наступних принципах: проактивне запобігання інцидентам ІБ та реактивне реагування на інциденти

ІБ. Це має на увазі використання заходів, спрямованих на попередження виникнення інцидентів ІБ, таких як аналіз ризиків, впровадження заходів захисту та моніторинг системи ІБ та вжиття заходів для мінімізації наслідків інцидентів ІБ, які все ж таки виникли, таких як розслідування інциденту, ліквідація його наслідків та запобігання повторенню. Перевагами комплексного підходу управління інформаційною безпекою є: ефективне запобігання та реагування на інциденти ІБ, мінімізація збитків, підвищення стійкості до кібератак. Комплексний підхід дозволяє як попередити інциденти ІБ, так і ефективно реагувати на них, якщо вони все ж таки виникнуть. Завдяки проактивним заходам та швидкому реагуванню на інциденти ІБ комбінований підхід може допомогти мінімізувати збитки, які можуть бути завдані підприємству. Комплексний підхід робить підприємство більш стійким до кібератак, адже воно має як засоби для їх запобігання, так і для реагування на них. Комплексний підхід до управління ІБ є найефективнішим способом захисту інформаційних ресурсів підприємства. Він дозволяє як попередити інциденти ІБ, так і мінімізувати їхні наслідки, що, в свою чергу, сприяє стійкості та розвитку підприємства.

Функціональний підхід до управління інформаційною безпекою (ІБ) підприємства ґрунтується на розподілі відповідальності за ІБ між різними підрозділами та посадовими особами. Кожен підрозділ та посадова особа мають чітко визначені функції з ІБ, які вони повинні виконувати. Елементами функціонального підходу є: визначення відповідальності, розподіл функцій та координація і співпраця. На увазі мається визначення того, хто відповідає за різні аспекти ІБ, такі як розробка політик та процедур, впровадження заходів захисту, моніторинг системи ІБ та реагування на інциденти ІБ, розподіл функцій з ІБ між різними підрозділами та посадовими особами, забезпечення координації та співпраці між різними підрозділами та посадовими особами з питань ІБ. Перевагами функціонального підходу управління інформаційною безпекою є: чіткий розподіл відповідальності, підвищення ефективності, поліпшення координації. Функціональний підхід гарантує, що кожен знає свої

обов'язки з ІБ, що може допомогти уникнути дублювання роботи та пропусків. Розподіл функцій з ІБ між різними підрозділами та посадовими особами може підвищити ефективність ІБ, адже кожен підрозділ може зосередитися на своїх сильних сторонах. Розподіл функцій з ІБ між різними підрозділами та посадовими особами може підвищити ефективність ІБ, адже кожен підрозділ може зосередитися на своїх сильних сторонах. Функціональний підхід до управління ІБ може бути ефективним способом захисту інформаційних ресурсів підприємства, якщо він правильно впроваджений. Він може допомогти чітко розподілити відповідальність за ІБ, підвищити ефективність роботи та покращити координацію між різними підрозділами.

Таблиця 1.1

Підхід	Сутність	Переваги/недоліки
Реактивний підхід	Реактивний підхід до забезпечення управління інформаційною безпекою (ІБ) ґрунтується на реагуванні на інциденти ІБ після їх виникнення. Цей підхід передбачає, що організація зосереджується на виявленні та реагуванні на кібератаки, порушення даних та інші інциденти ІБ, коли вони вже сталися.	Реактивний підхід може бути ефективним для вирішення відомих проблем ІБ, оскільки організація може зосередити свої ресурси на конкретних загрозах, з якими вона вже стикалася. Реактивний підхід може бути неефективним для вирішення нових проблем ІБ, оскільки організація може не мати необхідних знань або ресурсів для швидкого реагування.
Проактивний підхід	Проактивний підхід до забезпечення управління інформаційною безпекою (ІБ) ґрунтується на запобіганні інцидентам ІБ, перш ніж вони виникнуть. Цей підхід передбачає, що організація вживає заходів для виявлення та усунення потенційних загроз ІБ, перш ніж вони зможуть завдати шкоди.	Проактивний підхід може допомогти організації значно знизити ризик інцидентів ІБ, що може призвести до економії коштів та запобігти шкоди репутації. Проактивний підхід може допомогти організації більш ефективно використовувати свої ресурси з питань ІБ, оскільки вона може зосередитися на запобіганні проблемам, а не на їх вирішенні після виникнення.

Продовження таблиці 1.1.

Функціональний підхід	Функціональний підхід до забезпечення управління інформаційною безпекою (ІБ) ґрунтується на розподілі відповідальності за ІБ між різними підрозділами організації. Цей підхід передбачає, що кожен підрозділ має чітко визначені обов'язки та відповідальність у сфері ІБ.	Функціональний підхід забезпечує чіткий розподіл відповідальності за ІБ, що може допомогти уникнути дублювання зусиль та пропусків. Функціональний підхід може допомогти підвищити підзвітність за ІБ, оскільки кожен підрозділ несе відповідальність за свої дії. Функціональний підхід може бути складним для впровадження, оскільки він вимагає чіткого визначення та документування ролей та відповідальності. Функціональний підхід може призвести до виникнення конфліктів між різними підрозділами, якщо їхні обов'язки та відповідальність не чітко визначені.
Комплексний підхід	Комплексний підхід до забезпечення управління інформаційною безпекою (ІБ) ґрунтується на поєднанні превентивних, реактивних та функціональних заходів для забезпечення всебічного захисту організації від кіберзагроз. Цей підхід передбачає, що організація використовує різні методи та інструменти для виявлення, запобігання та реагування на інциденти ІБ, а також для забезпечення чіткого розподілу відповідальності та ефективного використання ресурсів.	Комплексний підхід забезпечує всебічний захист організації від кіберзагроз, оскільки він поєднує в собі превентивні, реактивні та функціональні заходи. Комплексний підхід може допомогти підвищити стійкість організації до кіберзагроз, оскільки вона має широкий спектр інструментів для реагування на інциденти ІБ. Комплексний підхід може бути складним для впровадження, оскільки він вимагає значних інвестицій у ресурси та час. Комплексний підхід потребує постійного вдосконалення, оскільки загрози ІБ постійно змінюються.

Кожен з наведених підходів є широко використованим в управлінні інформаційною безпекою підприємств.

Висновки до першого розділу

У першому розділі даної кваліфікаційної роботи розглядалися важливі аспекти управління інформаційною безпекою підприємства, а саме були розглянуті особливості та підходи до управління інформаційною безпекою

підприємства. Розглядаються основні поняття “безпека підприємства” та “інформаційна безпека підприємства”. Досліджується система управління інформаційною безпекою підприємства та основними підходами до управління інформаційною безпекою. Був досліджений вплив різноманітних чинників на діяльність ІТ-системи підприємства. Розглянуті можливі наслідки для діяльності підприємства.

Важливим аспектом є розгляд особливостей управління інформаційною безпекою. Визначається, що функції інформаційної безпеки підприємства полягають у ефективному управлінні системою забезпечення інформаційної безпеки, використанні ефективних механізмів управління. Дані функції забезпечують якісне та активне функціювання об’єкта господарювання на ринку відповідної сфери діяльності. У сучасному світі, де інформація стає все більш цінною, інформаційна безпека (ІБ) набуває виняткового значення для будь-якої організації. Підібрати правильний підхід до управління ІБ є життєво важливою для будь-якої організації з наступних причин: ефективінсть, відповідальність, оптимізація витрат, зниження ризиків, підвищення конкурентоспроможності, поліпшення корпоративної культури, підвищення стійкості.

РОЗДІЛ 2
АНАЛІЗ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

2.1 Характеристика та особливості функціонування компанії

В даній кваліфікіційні роботі розглядається українська компанія «Парус», першочергово варто звернути увагу на історію створення даної компанії. Група компаній «Парус» — українська компанія, розробник програмного забезпечення для підприємств малого та середнього бізнесу, великих корпорацій і холдингів, а також установ та організацій державного сектору економіки. Головний офіс організації «Парус» розташований в Києві. Регіональна мережа налічує близько 45 дочірніх компаній, філій та дилерів у всіх областях України [10].

Група компаній «Парус» заснувалась у 1990 році. День народження компанії — 5 квітня. Перший продажі та встановлення програм відбулися в грудні 1991 року (системи автоматизації розрахунку та нарахування заробітної плати «Парус-Заробітна плата»). Згодом були розроблені й представлені програми для автоматизації бухгалтерського, кадрового, складського обліку та інші. Усі ці програмні продукти об'єднані у двох комплексних системах: «Парус-Підприємство 4.XX» (для комерційних організацій) та «Парус-Бюджет 4.XX» (для бюджетних установ). У 1998 році на ринку з’явилися комплексні системи управління «Парус-Підприємство 8» і «Парус-Бюджет 8» (на базі СКБД Oracle) для великих підприємств і організацій. У 1999 році випустили системи «Парус-Підприємство 7» та «Парус-Бюджет 7» (на базі Visual FoxPro) для автоматизації управління та обліку на підприємствах малого і середнього бізнесу та у низькобюджетних установах [10].

Група компаній «Парус» є лауреатом і переможцем різних конкурсів у сфері IT, таких як: «Soft Regatta», «ITC — Award», «ТОП-профі комп'ютерної

України», «IT для управління підприємством: нові рішення», «Best CIO 2012» та інших. Наразы, компанія займає топові позиції в різноманітних рейтингах [10].

Будучи системним інтегратором тв маючи кваліфікований персонал, група компаній "Парус" є: розробником програмного забезпечення для управління підприємством та бюджетними установами і організаціями (Парус-Планування і Фінансування, Парус-Управління автотранспортом, Парус-Менеджмент і Маркетинг, Парус-Консолідація, Парус-Страхування, Парус-Ресторан, Парус-Готель, Парус-Бухгалтерія, Парус-Заробітна плата, Парус-Персонал, Парус-Управління виробництвом, Парус-Управління діловими процесами, Парус-Магазин, Парус-Краса-Здоров'я-Спорт, Парус-Аквапарк, Парус-Розважальний заклад, Парус-Управління Логістикою, Парус-Управління конкурсними закупівлями, Парус-Канцелярія, Парус-Управління майном, Парус-Реклама, Парус-Туристичне агентство, Парус-Молочне виробництво, Парус-Контакт-центр, Парус-Пропускний режим, Парус-Торгівля і склад і т.д.), постачальником супутнього програмного забезпечення (ORACLE, MICROSOFT), різного торгового обладнання (ЕККР ІКС, MIHI, Datecs, Samsung та ін), POS-обладнання (Posiflex, Flytech, JIVA, IBM, Aura, EPSON, TYSSO та ін), обладнання систем контролю доступу (CARD SYSTEMS), відеоспостереження та надає своїм клієнтам широкий спектр послуг, перелік яких може задовольнити найвимогливіших з них [11].

Дана компанія займається обробкою великою кількості даних, які належать для самого підприємства та даних які несуть критичну важливість для всіх клієнтів організації. В компанії обробляється важлива інформація її клієнтів така як: контактна інформація користувачів, демографічні дані користувачів, фінансова інформація клієнтів також дані про використання це може включати інформацію про те, як клієнт використовує ПЗ, наприклад, які функції він використовує, як часто він його використовує та які дані він вводить. Також компанією обробляються: файли cookie та інші ідентифікатори, операційні системи, IP-адреси.

Вся інформація якою володіє компанія можна класифікувати за видами:

виробнича, фінансова, маркетингова, кадрова, юридична, технічна, науково-дослідницька рис 2.1.

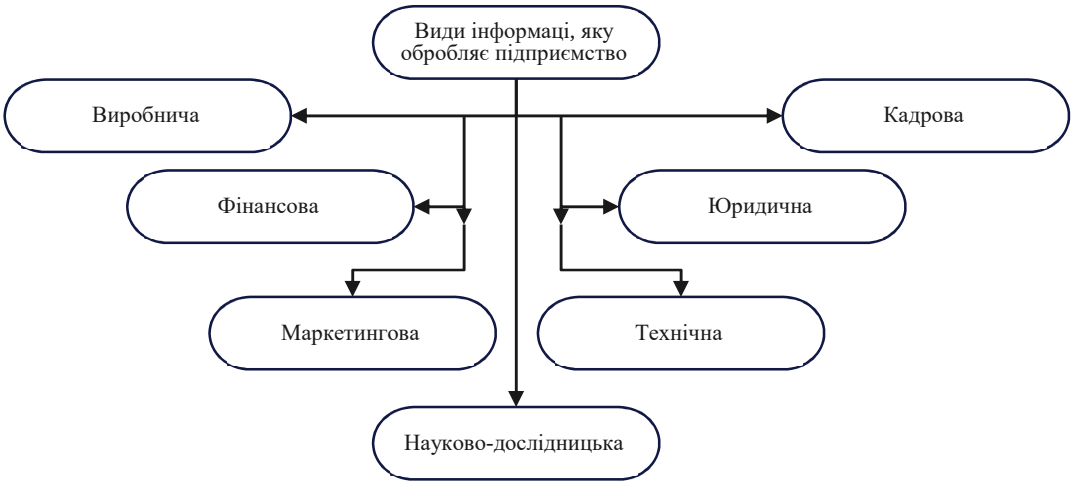

Рис. 2.1. Види інформації в компанії «Парус».

Джерело: складено на основі [1, 6].

Інформація на підприємстві переноситься на паперових та електронних носіях інформації. Паперові носії інформації в даному випадку це є: ділові документи, кадрові документи, юридичні документи, технічні документи, фінансові документи. А саме: рахунки-фактури, договори, листи, звіти, протоколи зустрічей, рахунки-фактури, договори, листи, звіти, протоколи зустрічей, резюме, трудові договори, накази про призначення, накази про звільнення, особові картки працівників, свідоцтва про державну реєстрацію, ліцензії, дозволи, договори оренди, договори купівлі-продажу, креслення, специфікації, інструкції з експлуатації, гарантійні талони, касові ордери, платіжні квитанції, банківські виписки, податкові декларації рис 2.2.

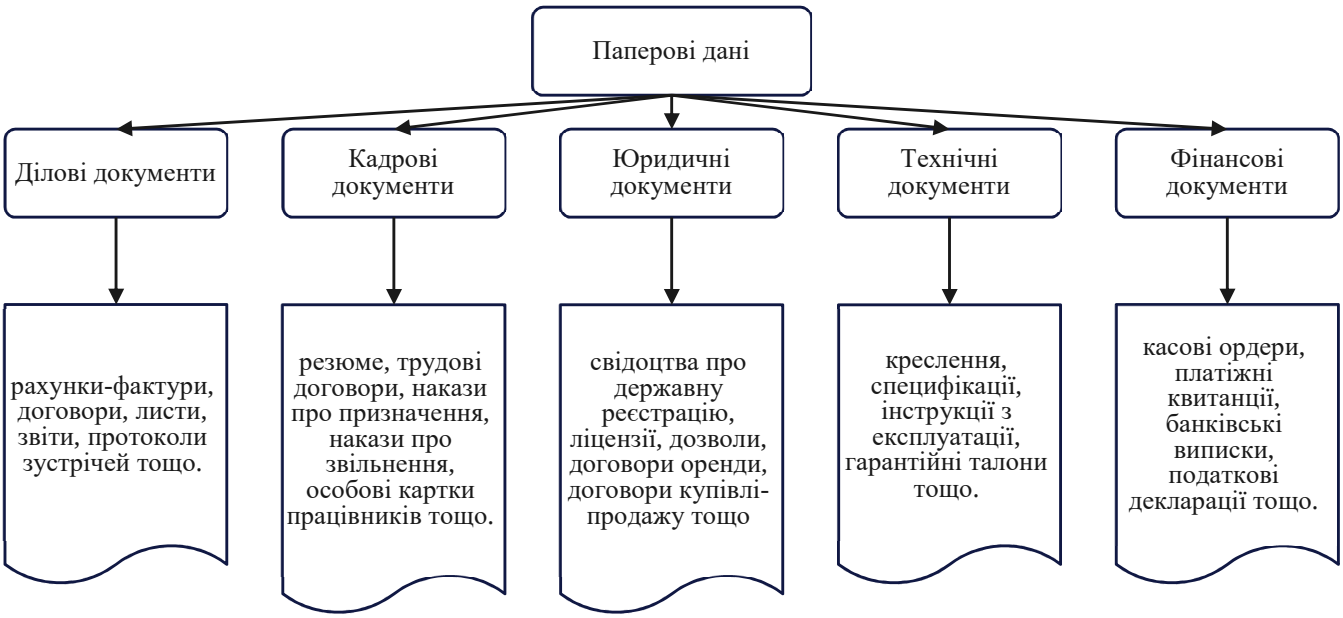

Рис. 2.2. Класифікація паперових даних на підприємстві «Парус»

Джерело: авторська розробка

Електронні дані - це будь-яка інформація, яка представлена в цифровій формі та зберігається на електронних носіях. Це може включати: текстові дані, табличні дані, мультимедійні дані, програмне забезпечення. На підприємстві електронні дані зберігаються на локальних комп’ютерах, серверах та хмарних сховищах рис 2.3. Дані зберігаються на жорстких дисках комп'ютерів, зберігаються на серверах, які розміщені на підприємстві та зберігаються в хмарних сховищах, таких як Dropbox, Google Drive, OneDrive.

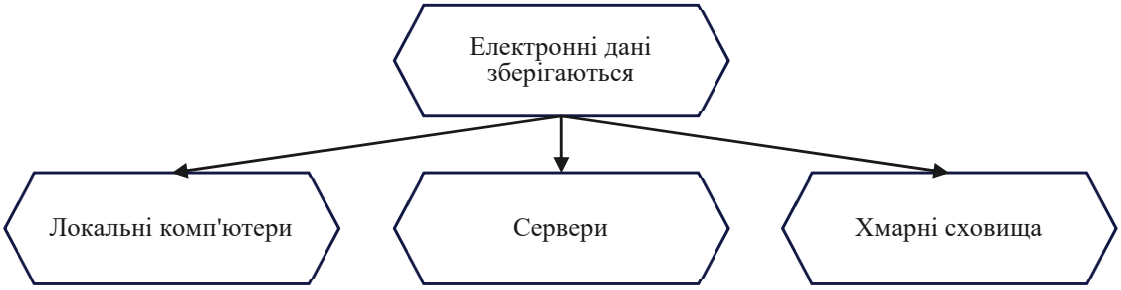

Рис.2.3. Місця збережання електронних даних на підприємстві «Парус»

Джерело: авторська розробка

За ступенем конфеденційності інформації на даному об’єкті господарювання інформація класифікується як загальноступна, а саме дані, які доступні для всіх, наприклад, інформація про продукти та послуги, контактні дані. Конфіденційна - дані, які доступні обмеженому колу осіб, наприклад, комерційна таємниця, персональні дані працівників. Секретна – дані, які доступні лише уповноваженими особами, наприклад, державна таємниця.

На підприємстві використовується різноманітна інформація для прийняття управлінських рішень, планування діяльності, контролю за роботою персоналу, оцінки ризиків, розвитку нових продуктів та послуг тощо.

2.2 Аналіз безпечності інформаційого середовища підприємства

Аналіз безпечності інформаційного середовища (ІС) підприємства – це комплексний процес, який дозволяє виявити, оцінити та нейтралізувати загрози, вразливості та ризики для інформаційних активів.

Аналіз інформаційної безпеки середовища підприємства - це систематизований процес збору, обробки та аналізу інформації про стан

інформаційної безпеки підприємства з метою виявлення потенційних загроз, оцінки їх ймовірності та наслідків реалізації, а також розробки заходів щодо їх нейтралізації – дане визначення надають науковці Савченко О.В., Олійник О.М. у своїй роботу «Аналіз інформаційної безпеки середовища підприємства на основі моделі COBIT».

Аналіз безпечності діяльності підприємства доцільно проводити експертним шляхом. При проведенні даного аналізу можна виявити недоліки в системі заходів захисту інформації. Метою проведення аналізу є оцінка стану інформаційної системи та розробка рекомендацій із застосування комплекстного підходу до управління інформаційною безпекою і програмно-технічних засобів, які спрямовані на захист інформаційної системи підприємства. Аналіз безпечності інформаційного серидовища підприємства допомагає прийняти обґрунтовані рішення, які підсилюються за допомогою засобів захисту інформації, які є найрелевантнішими щодо їх вартості й можливосте застереження загроз безпеці інформаційної сфери та діяльності підриємства загалом.

Аналіз безпечності інформаційного середовища включає кілька етапів, таких як збір інформації про системи, перевірка на вразливості, оцінка ризиків та соціальна інженерія. Кожен з наведених етапів відіграє ключову роль у виявленні проблем та наданні рекомендацій для покращення безпеки [15].

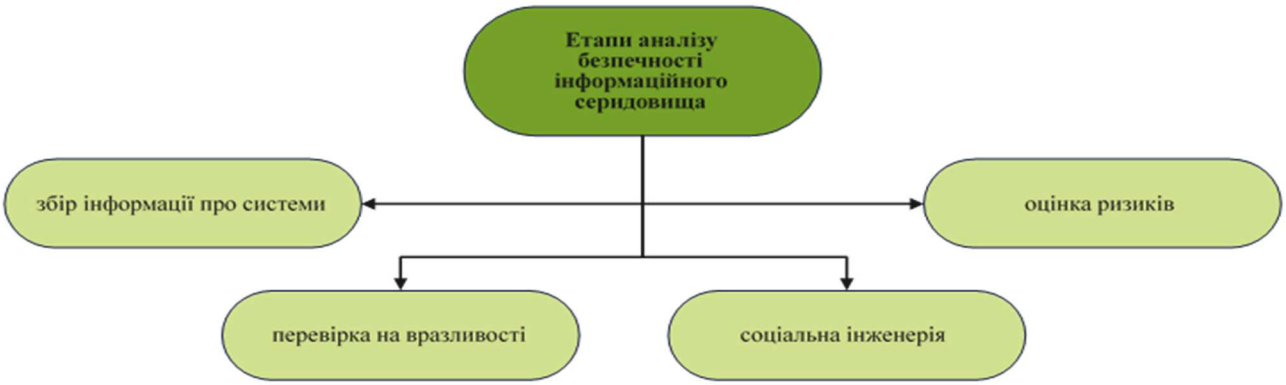

Рис. 2.4 Етапи аналізу безпечності інформаційного серидовища

Джерело: авторська розробка

При проведені аналізу безпечності інформаційного середовища підприємства можна визначити загальний стан безпечності інформаційного підприємства. Це допоможе – виявити слабкі місця та вразливості в середині інформаційного серидовища підприємства, оцінити потенційні ризики для об’єкта господарювання та бізнес-процесів компанії. Результати аналізу допомагають виявити та удосконалити прогалини в інформаційній безпеці підприємства, удосконалити заходи безпеки для більш успішної протидії загрозам, запобігати інцидентам та захистити репутацію.

Компанія «Парус» надає широкий спект послуг технічної підтримки для своїх клієнтів. Тех. підтримка включає в себе:

1. становка та обслуговування систем "Парус";
2. встановлення, технічне обслуговування та ремонт оргтехніки;
3. антивірусний захист;
4. обслуговування мережі;
5. підтримка та налаштування роботи ОС;
6. підтримка доступів до мережі Інтернет;
7. розробка та підтримка електронної пошти;
8. розробка та підтримка контрольно-пропускної системи;
9. створення системи відеоспостереження;
10. забезпечення оргтехніки витратними матеріалами;
11. постачання та супроводження ліцензійного ПЗ (Windows, MS Office, Adobe, Oracle та ін).

Надання такого широкого спектру послуг вимагає якісного забезпечення інформаційної безпеки на підприємстві. Підприємство має доступ до конфеденційної інформації своїх клієнтів, що потребує якісного забезпечення та управління інформаційною безпекою. Сучасні підприємства сильно залежать від своїх IT-систем для ведення бізнесу, перебої в роботі цих систем можуть призвести до серйозних збитків.

IT-інфраструктуру підприємства включає в себе програмне та апаратне забезпечення, мережеві ресурси та системи зберігання даних . Для забезпечення

локальної мережі підприємство використовує сервери баз даних Oracle (Oracle Database Server Enterprise Edition) також сервер для зберігання баз даних про користуваців та конфігурації (MySQL).

Мережевими пристроями даного підприємства є маршрутизатори, комутатори та брандмауери. ПК для розробників, ПК для тестування та ПК для служби підтримки – основні робочі станції.

Для забезпечення безпечності інформаційного простору дане підприємство використовує антивірусне програмне забезпечення (Zillya, Eset).

Оцінка ризиків інформаційної безпеки також є невід'ємною частиною аналізу інформаційної безпеки підприємства. Ризик, у більш широкому розумінні, - це ймовірність настання події, яка тягне за собою певні втрати (наприклад, фізичну травму, втрату майна, шкоду для організації тощо).

Ризик інформаційної безпеки - це потенційна ймовірність використання вразливостей активу або групи активів як конкретної загрози для завдання шкоди організації [16].

Інформаційні ризики мають свою класифікацію та їх можна розбити на п'ять груп: за природою (внутрішні, зовнішні), за джерелом (навмисне, ненавмисне), за способом впливу (прямий, не прямий), за результатом (порушення достовірності інформації, порушення актуальності інформації), за механізмом дії (стихійні лиха, аварії, людські помилки тощо)

Класифікація інформаційних ризиків наведена на рис. 2.5

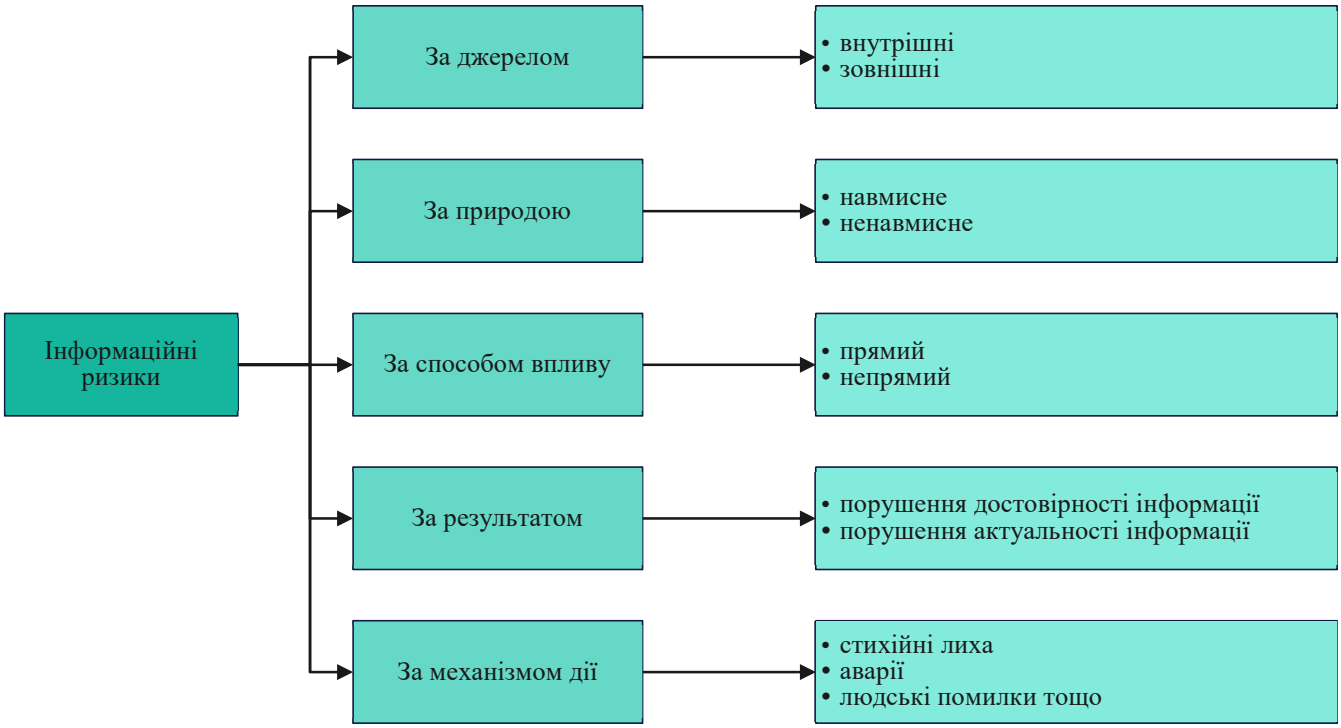

Рис. 2.5 Класифікація інформаційних ризиків

Джерело: складено на основі [17].

Аналіз ризиків включає в себе процес оцінки ризиків і потенційних методів зниження ризиків або зменшення пов'язаних з ними негативних наслідків. В контексті інформаційної безпеки вплив являє собою ймовірну шкоду, заподіяну організації в результаті порушення інформаційної безпеки, з урахуванням можливих наслідків втрати конфіденційності, цілісності або доступності інформації чи інших активів. Ймовірність оцінює ймовірність такого порушення з урахуванням наявних загроз і вразливостей, а також впроваджених заходів управління інформаційною безпекою. Рівень збитку є грошовим параметром та еквівалентом вартості, а вартість може бути розрахована за методиками, які впровадженні на підприємстві.

Аналіз ризиків інформаційної безпеки можна розділити на два типи: якісний та кількісний. Якісний аналіз визначає фактори, сфери та типи ризиків, і зазвичай використовує людську взаємодію, наприклад, шляхом проведення

семінарів або інтерв'ю, для отримання вхідних даних. Після збору даних ризик-менеджер застосовує якісний, а не кількісний аналіз. Хоча цей процес може не відповідати числовій моделі, його часто застосовують через його здатність відображати складність досліджуваних ризиків і встановлювати взаємозв'язки між, здавалося б, несуттєвими фрагментами інформації [17].

Можна проводити різні види якісного аналізу. Трудомістким, але зручним підходом є застосування тематичного аналізу до стенограм проведених інтерв'ю або тем, що обговорювалися під час семінарів. Він може, наприклад, ґрунтуватися на аналізі використаного дискурсу, оскільки людська мова може висвітлювати конкретні деталі про середовище та контекст ризиків. Враховуючи ці дані, якісна оцінка ризиків є ефективним способом розглянути взаємозв'язки у сферах бізнесу, а отже, мати можливість оцінити не лише технічні аспекти, але й проблеми, що виникають через людей та процеси.

При якісній оцінці ризиків основна увага приділяється ймовірності події, а не її статистичній ймовірності. Ці ймовірності виводяться з аналізу загроз і вразливостей, а потім генеруються якісні або кількісні значення для активу або активів, які можуть зазнати впливу (наслідків):

$$Ризик = Загроза \times Вразливість \times Вплив \qquad (2.1)$$

Соціальна інженерія - це метод маніпулювання людьми з метою отримання доступу до інформації, систем або ресурсів, на які вони не мають дозволу.

Науковці визначають соціальну інженерію як один з найпростіших методів збору інформації про об'єкт за допомогою використання людських слабкостей, які притаманні кожній організації. По суті, соціальна інженерія - це розробка та застосування обманних методів для навмисного маніпулювання людьми. У контексті кібербезпеки вона в першу чергу використовується для того, щоб спонукати жертв до розкриття конфіденційних даних або до виконання дій, які порушують протоколи безпеки, несвідомого зараження систем або

витоку секретної інформації. В основі атаки соціальної інженерії лежить спроба обійти системи кібербезпеки шляхом обману, використовуючи найслабшу ланку - людей. Протягом всієї взаємодії жертви не усвідомлюють деструктивного характеру своїх дій. Соціальний інженер експлуатує невинні інстинкти, а не злочинні. Відкриті методи, такі як погрози або підкуп, не підпадають під соціальну інженерію. Талановитий практик цієї дисципліни розуміє і сприймає моделі соціальної взаємодії для маніпулювання психологічними аспектами людської свідомості. Маючи таке розуміння, зловмисник здатен здійснити ефективний і дешевий компроміс безпеки, без необхідності інвестувати в порушення технічних заходів безпеки. Тим не менш, освічений соціальний інженер з комп'ютерних наук може також доповнити атаку технологічними засобами, щоб досягти зловмисних намірів.

На даному підприємстві було визначено, що більшість працівників організації не є ознайомленими з поняттям соціальна інженерія. Неодноразово працівники підприємства стикалися з фішингом, що в наслідок завдало матеріальної та технічої шкоди для організації.

2.3 Аналіз управління інформаційною безпекою підприємства

Аналіз управління інформаційною безпекою (УІБ) - це комплексне дослідження, яке дозволяє оцінити стан інформаційної безпеки підприємства, виявити потенційні загрози та вразливості, а також розробити план дій щодо їх усунення.

Управління інформаційної безпеки підприємства потребує системності, тому з’являється поняття системи управління інформаційною безпекою підприємства. Система управління інформаційною безпекою СУІБ (англ. information security management system, ISMS) — частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної

безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки [20].

Управління інформаційною безпекою на даному підприємстві відбувається на двох рівнях: – адміністративне управління інформаційною безпекою підприємства; – технологічне управління інформаційною безпекою підприємства. Забезпечення даних двох рівнів управління інформаційної безпеки підприємства забезпечує аутсорсингова компанія, яка надає послуги для організації з забезпечення та управління інформаційною безпекою. Це не є доцільним в наявній ситуації на підприємстві, оскільки велика кількість послуг, які надає підприємство вимагає якісного та структурованого забезпечення інформаційною безпекою, яке повинно контролюватися та мати швидке реагування на ризики та інциденти на підприємстві.

Оцінка ризиків є вирішальним і тривалим кроком у розробці СУІБ компанії, оскільки вона передбачає пошук, аналіз і класифікацію всіх можливих небезпек, які можуть вплинути на діяльність компанії. Хоча ризики можуть відрізнятися від інших компаній, мета полягає в тому, щоб гарантувати безпеку інформації та знайти найкраще рішення, яке задовольняє вимоги компанії. У компанії було багато процедур. Тим не менш, більшість із них не документувалися часто або взагалі. По суті, численні небезпеки були пропущені та, отже, не враховані.

Нами був проведений аніліз ризиків інформаційної безпеки підприємства, для аналізу були залучині працівники різних відділів. Після проведення інтерв’ю був визначений перелік інформаційних ризиків підприємства.

Ризики інформаційної безпеки на підприємстві «Парус»:

1. кібератаки;
2. людська помилка;
3. внутрішні збої;
4. технічні збої;
5. стихіні лиха.

Задопомогою визначених ризиків інформаційниї безпеки була розроблена матриця ризиків інформаційної безпеки підприємства «Парус».

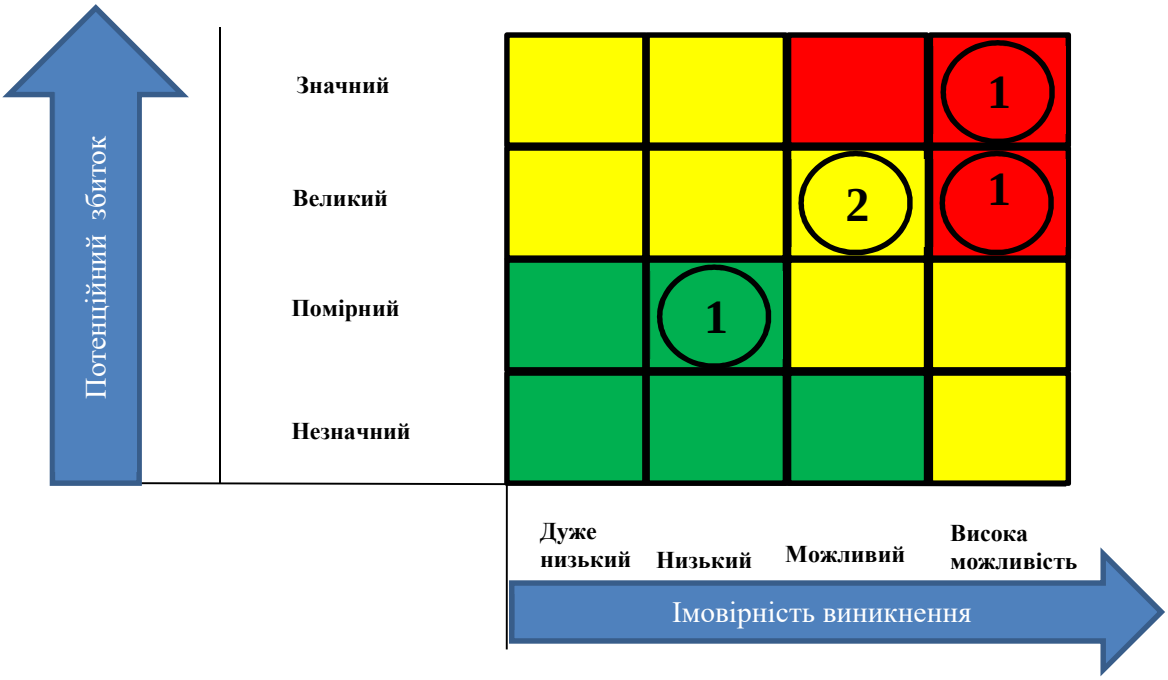

Рис. 2.6. Матриця ризиків інформаційної безпеки для досліджуваного підприємства «Парус»

Джерело: власна пропозиція

Управління виявленими ризиками є необхідним для безпеки підприємства оскільки неналежне реагування на них може завдати для організації великих збитків та втрати репутації, що є не реливантним на ринку послуг даної галузі. Оскільки підприємство має велику кількіст крупних конкурентів будь-які можливі недоліки у системі забезпечення інформаційної безпеки можуть бути критичними. В теперішній ситуації на підприємстві немає можливості самотужки реагувати на виникнуті ризики, оскільки забезпечення відбувається через аутсорсингові компанії. Кожна з компаній яка надає послугу виконує різні опції в забезпечені інформаційної безпеки, через відсутність загального комплексного підходу до управлінню інформаційною безпекою, неповномірно розуміє сутність наявних ризиків через брак інформації у різних сферах.

Висновки до другого розділу

У другому розділі даної кваліфікаційної роботи були розглянуті загальні характеристики підприємства, яке аналізується. Був проведений аналіз безпечності інформаційного середовища підприємства «Парус». Проаналізували наявну систему управління інформаційною безпекою підприємства, етапи реалізації СУІБ.

Існуюча система управління інформаційною безпекою не є відповідною для підприємства такої величини з великою кількістю послуг. Підприємство організовує свою роботу завдяки аутсорсингових компаній. Це не є доцільним у теперішній час, оскільки немає завіреної структури для захисту інформаційної безпеки. Кожна з аутсорсингових компаній має свою зону відповідальності, що в майбутньому може завдати проблем для організації.

Загальний стуктурований комплексний підхід допоможе для організації організувати процеси таким чином, щоб вони могли працювати як єдиний механізм.

РОЗДІЛ 3
КОМПЛЕКСНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ

3.1 Оцінка підходу до управління інформаційною безпекою підприємства та вияв прогалин

Оцінка підходу до управління інформаційною безпекою (УІБ) та виявлення вразливостей є критично важливим аспектом захисту інформаційних активів підприємства. Цей процес допомагає визначити сильні та слабкі сторони поточної системи УІБ, а також виявити потенційні загрози та вразливості, які можуть бути використані зловмисниками.

Проаналізувавши підприємство «Парус», а саме конкретно його робочі процеси, систему забезпечення інформаційної безпеки та управлінна інформаційною безпекою, можемо надати оцінку наявим використовуваним підприємством підходам.

Забезпечення управління інформаційною безпекою підприємства ґрунтується на реактивному підході. Застосування реактивного підходу на підприємстві ґрунтується на його економічності та відносній ефективності. Спеціалісти підпримства виявили що даний підхід є найоптимальнішим і може краще працювати ніж проактивний. За думкою організації, , жодна атака не є катастрофічною, тобто підприємство може пережити декілька атак незначних атак. По-друге, бюджет підприємства є ліквідним, це означає, що організація може перерозподіляти ресурси без штрафних санкцій. Реактивний підхід для підприємства «Парус» забезпечує декілька аутсорсингових організацій, кожна з яких має свою суворо окреслену зону відповідальності.

Таблиця 3.1

АНАЛІЗ НАЯВНОГО ПІДХОДУ УІБ НА ПІДПРИЄМСТВІ

Назва	Проблеми	Наслідки
Наявний реактивний підхід до УІБ на підприємстві «Парус»	Високий ризик інцидентів ІБ	Це може призвести до значних збитків, оскільки організація може втратити важливі дані, зазнати фінансових збитків або пошкодити свою репутацію.
	Неефективність при вирішенні нових проблем	Інциденти ІБ можуть призвести до переривання роботи організації, що може призвести до втрати продуктивності та доходу. Якщо організація не може ефективно вирішувати нові проблеми ІБ, вона може стикатися з повторними перебоями в роботі, що може серйозно вплинути на її діяльність.
	Недостатня підготовка	Реактивний підхід може призвести до того, що організація буде непідготовленою до інцидентів ІБ, що може призвести до хаосу та плутанини.
	Відсутність проактивності	Реактивний підхід до УІБ передбачає реагування на проблеми лише після їх виникнення. Це означає, що організація не вживає заходів для запобігання проблемам, що робить її більш схильною до кібератак, витоків даних та інших інцидентів ІБ. Зловмисники можуть використовувати нові вразливості та методи атак, перш ніж організація зможе вжити заходів для захисту.
	Недостатній контроль	Реактивний підхід може призвести до того, що організація не матиме достатнього контролю над своїми ризиками ІБ, що може зробити її більш вразливою до кібератак.

Аналізуючи підхід до управління інформаційною безпекою на підприємства ми виявили прогалини в даній системі. Основними прогалинами є відсутність превентивних дій щоб забезпечити підприємство від майбутніх кібератак. Організація задля збереження бюджету не вводить практики по прогнозуванню можливих загроз. Планування та прогнозування допоможе визначити потенційні загрози та вразливості та розробити план дій щодо їх запобігання, це є життєво важливим для будь-якого підприємства, яке хоче захистити свою інформацію. Зловмисники постійно розробляють нові методи атак, тому важливо бути на крок попереду і прогнозувати, які загрози можуть виникнути в майбутньому. Якщо підприємство не має плану дій на

випадок кіберінциденту, воно може втратити багато часу та грошей, перш ніж зможе відновити свою роботу. Визначивши потенційні загрози та розробивши план їх запобігання, підприємства можуть значно знизити ймовірність виникнення проблем, оскільки запобігання кіберінциденту є завжди дешевшим, ніж його усунення. Кіберінцидент може серйозно пошкодити репутації підприємства, що може призвести до втрати клієнтів та партнерів.

Проаналізувавши підприємство «Парус», а саме конкретно його робочі процеси, систему забезпечення інформаційної безпеки та управління інформаційною безпекою, можемо надати оцінку підходам, що використовуються. У підприємства відсутній власний департаменту, який забезпечує ІБ підприємства. Їх захист складається з безлічі різних пристроїв і програмних додатків від різних виробників, можливість інтеграції яких між собою вельми обмежена.

3.2 Розробка комплексного підходу до управління інформаційною безпекою підприємств.

Комплексний підхід до УІБ - це всебічний та інтегрований підхід до управління інформаційними ризиками, який охоплює людей, процеси та технології [21].

Принцип комплексного підходу до забезпечення інформаційної безпеки передбачає створення органічно взаємозв’язаної структурності сил, засобів і спеціальних методів, спрямованих на забезпечення безпеки інформації, що підлягає захисту та сфери її обігу. Принцип безперервності забезпечення інформаційної безпеки полягає у повсякденному (безперервному) застосуванні як загальних, так і спеціальних засобів і методів забезпечення інформаційної безпеки на всіх її етапах життєвого циклу [25].

Комплексний підхід до УІБ допомагає захистити конфіденційну, цілісну та

доступність інформаційних активів підприємства, таких як дані, системи та мережі; допомагає ідентифікувати, оцінювати та контролювати інформаційні ризики, що може допомогти запобігти кіберінцидентам та зменшити їх наслідки; допомагає підприємствам відповідати всім застосовним законам, нормам та стандартам, що може допомогти уникнути штрафів та інших санкцій; допомагаэ підвищити довіру клієнтів, партнерів та інвесторів, що може призвести до збільшення продажів та прибутку.

На практиці групи компаній «Парус» можемо зазначити, що першим і найголовнішим етапом організації комплексного підходу інформаційної безпеки підприємства є створення власного департаменту інформаційної безпеки. Це забезпечить об’єкт господарювання можливістю самостійно контролювати безпекове інформаційне серидовище, управляти інформаційною безпекою та своєчасно реагувати на виникнуті загрози ІБ.

Для даної організації комплексний підхід до УІБ буде грунтуватися на ключових компонентах: ідентифікація та оцінка ризиків, розробка та впровадження політики та процедур, впровадження технічних заходів захисту, навчання та підвищення обізнаності, моніторинг та інцидент реагування рис.3.1. Даний комплексний підхід був розроблений індивідуально для групи компаній «Парус».

Рис 3.1 Основні компоненти при формуванні комплексного підходу до УІБ

Джерело: авторська розробка

Першим кроком у формуванні комплексного підходу до управління інформаційною безпекою підприємства є визначення активів інформаційної системи, які потребують захисту, а також ідентифікація потенційних загроз та вразливостей. Після цього проводиться оцінка ризиків, щоб визначити ймовірність та вплив кожної загрози. Даний етап буде ґрунтуватися на міжнародному стандарті ISO/IEC 27001:2022.

ISO (Міжнародна організація зі стандартизації) та IEC (Міжнародна електротехнічна комісія) утворюють спеціалізовану систему світової стандартизації. Національні органи, які є членами ISO або IEC, беруть участь у розробці міжнародних стандартів через технічні комітети, створені відповідними організаціями для роботи в певних галузях технічної діяльності. Технічні комітети ISO та IEC співпрацюють у сферах, що становлять взаємний інтерес. Інші міжнародні організації, урядові та неурядові, які підтримують зв'язок з ISO та IEC, також беруть участь у роботі.

Цей документ призначений для організацій усіх типів і розмірів. Його слід використовувати як довідник для визначення та впровадження засобів управління ризиками інформаційної безпеки в системі управління інформаційною безпекою (СУІБ) на основі стандарту ISO/IEC 27001. Він також може бути використаний як керівний документ для організацій, які визначають і впроваджують загальноприйняті засоби контролю інформаційної безпеки. Крім того, цей документ призначений для використання при розробці галузевих та організаційних настанов з управління інформаційною безпекою з урахуванням специфічного середовища ризиків інформаційної безпеки. Заходи контролю, специфічні для організації або середовища, відмінні від тих, що включені в цей документ, можуть бути визначені за допомогою оцінки ризиків, якщо це необхідно [30].

Важливо, щоб організація визначила свої вимоги до інформаційної безпеки. Існує три основні джерела вимог до інформаційної безпеки:

а) оцінка ризиків для організації з урахуванням загальної бізнес-стратегії та цілей організації. Цьому може сприяти або допомагати оцінка ризиків, специфічних для інформаційної безпеки. Результатом цього має бути визначення засобів контролю, необхідних для забезпечення того, щоб залишковий ризик для організації відповідав її критеріям прийнятності ризику;

б) правові, статутні, регуляторні та договірні вимоги, яким має відповідати організація та її зацікавлені сторони (торгові партнери, постачальники послуг тощо), а також їхнє соціально-культурне середовище

в) набір принципів, цілей та бізнес-вимог для всіх етапів життєвого циклу інформації, які організація розробила для підтримки своєї діяльності.

Етапами розробки системи управління інформаційною безпекою на підприємстві є:

1. Основне. Визначення поля застосування СУІБ.

Першим кроком перед впровадження СУІБ є визначення області застосування системи інформаційної безпеки підприємства. Слід враховувати підчас визначення сфери застосування СУІБ певні фактори:

- інформаційні активи. В даному випадко на основі бази підприємства «Парус» під інформаційними активами мається на увазі: дані, сервери та робочі станції, мережеве обладнання, ПЗ та інше. Створення СУІБ на підприємстві починає свій старт з повної інвентаризації та оцінки інформаційних активів підприємства.
- вимоги до застосування інформаційних технологій: вимоги, які зумовленні необіхідністю їхнього використання інформаційними технологіями, програмного забезпечення.
- вимоги законів. А саме: нормативно-правові акти а також договори з третіми особами, які мають вплив на особливості використання фізичних та інформаційних активів підприємства «Парус».

2. Обробка та оцінка ризиків інформаційної безпеки підприємства.

Визначивши область впровадження СУІБ варто провести оцінку і обробку ризиків інформаційної безпеки підприємства. Аналізуючи зібрану інформацію на підприємстві можемо визначити перелік дій.

За думкою спеціалісті інформаційної безпеки підприємства, підчас оцінки ризиків інформаційної безпеки необхідно:

- виявити поточні ризики інформаційної безпеки;
- визначити можливість реалізації загроз інформаційній безпеці та ймовірні негативні наслідки від їх реалізаці.
- створити «карту ризиків» інформаційної безпеки і визначити рівні та їх прийнятність для організації.
- визначити заходи, які необхідно профінансувати для усунення ризиків інформаційної безпеки;
- визначення цільових рівні залишкових ризиків інформаційної безпеки, які у разі захистних заходів необхідно профінансувати.

Оцінювання ризиків ІБ – це ітеративний процес, але результати первинного оцінювання відіграють важливе значення при прийнятті рішення про черговість впровадження в рамках СУІБ захисних заходів [22].

Наступний крок – визначення, як реагувати на ідентифіковані ризики

інформаційної безпеки. Спеціалістом з інформаційної безпеки даного підприємства приймається рішення, які варто впроватити заходи захисту ІБ підприємства у рамках СУІБ. Першочергово при прийнятті рішень спеціаліст підприємства керується поняттям чи ефективно компенсуватиметься дане впровадження по відношенню до втрат на реалізацію протидії неприйнятним ризикам ІБ на підприємстві.

3. Впровадження заходів захисту.

Наступний етап, який потрібно здійснювати після оцінки та прийнятт конкретних рішень по обробці ризиків ІБ є впровадження заходів захисту.

Підприємство керується вимогами до процесів управління ІБ встановленими у стандарті ISO/IEC 27001:2022. Вимоги технічного характеру і процесів забезпечення ІБ встановленні у стандарті ISO/IEC 27002:2022. В процесі впровадження заходів захисту перелік вимог змінюється ґрунтуючись на результатах оцінки та обробки ризиків ІБ підприємства.

4. Внутрішній аудит.

Внутрішній аудит інформаційної безпеки підприємства проводиться за стандартни планом який практикується на підприємстві. План внутрішнього аудиту частково побудований на аспектах вказаних у стандарті ISO/IEC 27001:2022. Завданням внутрішнього аудиту є необхідність визначити, чи так працюють впроваджені захисні заходи, як очікувалося і що конкретно можна поліпшити в побудованій СУІБ [23].

5. Робота над помилками. Поліпшення СУІБ.

Завершальним етапом створення СУІБ є упровадження механізму зворотного зв'язку для перманентного покращення всієї системи. Підхід до виконання цієї вимоги полягає в прийнятті моделі зрілості для всіх елементів СУІБ.

6. Безперервне вдосконалення.

Таблиця 3.2

Етапи реалізації суіб за стандартом ISO/IEC 27001:2022

Етап	Опис
Визначення поля застосування СУІБ та ініціалізація	Визначення цілей та завдань впровадження системи УІБ. Призначення відповідального за впровадження системи УІБ. Визначене сфери застосування системи УІБ. Виявлення інформаційних активів. Ідентифікація загроз та вразливостей.
Обробка та оцінка ризиків інформаційної безпеки підприємства.	Аналіз та оцінка ризиків інформаційної безпеки підприємства
Розробка та впровадження заходів захисту	Розробка політики інформаційної безпеки. Розробка процедур та інструкцій з питань ІБ. Впровадження технічних заходів захисту (антивірусне програмне забезпечення, брандмауери тощо). Впровадження організаційних заходів захисту (контроль доступу, резервне копіювання тощо).
Внутрішній аудит	Виявлення невідповідностей і шляхів поліпшення готової системивідповіднодо ISO/IEC 27001.
Робота над помилками	Аналіз і усунення всіх невідповідностей, виявлених у ході сертифікації.
Безперервне вдосконалення	Постійний моніторинг інформаційних систем та активів для виявлення потенційних загроз та вразливостей.

Безперервне вдосконалення ІБ - це динамічний процес, який передбачає постійне виявлення, аналіз та усунення ризиків інформаційної безпеки з метою підвищення загального рівня захисту інформаційних систем та активів організації. Даний процес є необхідним для підприємства «Парус» задля забезпечення постійного забезпечення інформаційної безпеки на підприємстві.

Ключовими етапами безперервного вдосконалення ІБ є: постійний аудит та діагностика діючих СУІБ, визначення показників ефективності, формування цілей та пріорітетів, постановка ключових цілей, постійне навчання персоналу, інтеграція корпоратиної стратегії рис 3.2.

Рис. 3.2 Етапи безперервного вдосконалення СУІБ

Джерело: авторська розробка

Забезпечення безперервного процесу вдосконалення СУІБ допоможе організації підтримувати постійний моніторинг та інцидент реагування.

Навчання та підвищення обізнаності працівників підприємства ризикам інформаційної безпеки (ІБ) є одним з найефективніших способів запобігти кіберзагрозам та інцидентам ІБ. Це допоможе підвищити розуміння працівниками ризиків ІБ, таких як фішинг, шкідливе програмне забезпечення, соціальна інженерія та кібератаки, навчити працівників правильно використовувати паролі, захищати конфіденційну інформацію та повідомляти

про підозрілу активність, сформувати культуру кібербезпеки на підприємстві, де працівники розуміють свою відповідальність за захист інформаційних активів.

Методи навчання працівників:

1. Залучення працівників до проходження онлайн курсів з ІБ.
2. Проведення вебінарів, які дозволять працівникам дізнатися про ризики ІБ від експертів.
3. Проведення симуляцій кібератак, фішингу, шкідливого програмного забезпечення.
4. Розробка авторської програми по навчанню працівників стосовно питань ІБ.

Навчання та підвищення обізнаності працівників про ризики ІБ є важливою інвестицією, яка може допомогти Вашому підприємству захистити свої інформаційні активи та запобігти кіберзагрозам.

3.3 Перваги комплексного підходу управління інформаційною безпекою в противагу існуючому

На основі проведених досліджень можна визначити, що для групи компаній «Парус» на даному етапі фунціонування розроблений комплексний підхід до управління інформаційною безпекою підприємства є найактуальнішим.

Весь період існування компанії «Парус», організація залучала до процесів УІБ аутсорсингові компанії. З плином часу та розширенням послуг та масштабів компанії в умовах глобальної диджеталізації даний підхід до УІБ є недоречним.

Переваги самостійної організації УІБ за допомогою комплексного підходу порівняно з власним департаментом ІБ в порівнянні з аутсорсингом забезпеченням різними компаніями:

Таблиця 3.3

Переваги розробленого комплексного підходу з існуючим

Комплексний підхід до управління ІБ	Наявний підхід до управління ІБ
Контроль та відповідальність	
Наявний повний контроль над процесом, є можливість визначати пріоритети, обирати методи та технології, а також нести пряму відповідальність за результат.	Делегування частини відповідальності аутсорсинговим компаніям, що може призвести до розрізненості дій та складнощів у координації.
Глибоке розуміння бізнесу	
Повноцінне розуміння специфіки бізнесу, його критичних активів, ризиків та потреби, що дозволяє оптимізувати УІБ під конкретні завдання.	Відсутність глибокого розуміння бізнесу, , що може призвести до неефективних рішень та неповного захисту.
Інтеграція з іншими процесами	
УІБ може бути інтегрований з іншими процесами компанії, що забезпечує цілісність та ефективність управління.	Інтеграція аутсорсингових послуг з іншими процесами може бути складною та потребувати додаткових зусиль.
Конфіденційність та безпека даних	
Контроль конфеденційних даних їх обробки та зберігання, гарантуючи конфіденційність та безпеку.	Частина даних передається для аутсорсингових компаній, що може нести ризики витоків або несанкціонованого доступу.
Перспективи розвитку	
Повністю контрольований процес розвитку команди фахівці УІБ, що є цінним активом для компанії.	Залежність від зовнішніх постачальників послуг, що може обмежувати можливості розвитку власної експертизи.
Вартість	
Початкові інвестиції можуть бути більшими, але в довгостроковій перспективі самостійне УІБ може бути більш економічно вигідним.	Витрати на аутсорсингові послуги можуть бути непередбачуваними та рости з часом.

Доцільним є створення власного департаменту ІБ, що дозволить контролювати інформаційну безпеку та підсилить довіру контрагентів до ступеня безпечності інформації на підприємстві «Парус». Крім того, центральной оператор отримує можливість контролювати стан всієї

інформаційної інфраструктури в реальному режимі часу.

Варто постійно підвищувати рівень обізнаності персоналу щодо інформаціної безпеки на підприємстві за рахунок створеного департамену інформаційної безпеки.

Впровадити постійний моніторинг безпеки всієї інформаційної інфраструкутури підприємтсва за рахунок наявних фахівців при створенні департаменту інформаційної безпеки. Результати моніторингу безпеки будуть враховуватися при комплексонму управлінні безпекою конкретно для кожного інцидента кібербезпеки.

Висновки до третього розділу

У третьому розділі кваліфікаційної роботи нами був проведений аналіз наявного підходу до управління інформаційною безпекою підприємсва. Були визначенні основні прогалени в системі УІБ підприємства «Парус».

На підставі сформованої матриці ризиків у розділі 2.3 рис. 2.6, ми визначили основні ризики інформаційної безпеки та степінь забезпечення безпеки на підприємстві. Внаслідок чого був сформований комплексний підхід до управління інформаційною безпекою підприємства «Парус». Нами були сформавані основні етапи у комплексному підході та описаний перелік дій.

Визначенно що група компаній «Парус» потребує створення власного департаменту інформаційної безпеки на базі підприємсва. Що забезпечить якісне функціонування та зменшить ризики інформаційної безпеки.

Було визначенно що працівники компанії потребують якісного навчання в сфері ІБ , за для зменшення ризиків інформаційної безпеки які провокуються людським фактором, тобто соціальна інженерія.

Порівнявши розроблений комплексний підхід та наявний підхід до УІБ на підприємстві, можемо зробити висновок, що є доцільним впровадити етапи комплексоного підходу в тандемі зі створення власного департаменту ІБ на підприємства. Це дозволить для організації повноцінно контролювати всі

аспекти у забезпеченні інформаційної безпеки та побудувати повний цикл надання послуги ІБ на своєму підприємстві. Що в наслідок зменшить кількість інформаційних загроз для організації.

ВИСНОВКИ

Комплексний підхід до управління інформаційною безпекою підприємства є необхідним в сучасних реаліях диджеталізації. У першому розділі кваліфікаційної роботи було розглянуто поняття «безпека підприємства» та «інформаційна безпека підприємства», а також розглянута сутність управління інформаційною безпекою підприємства та широко використовувані підходи до управління інформаційною безпекою.

У другому розділі було проведено ознайомлення з групою компаній «Парус», аналіз безпечності інформаційного поля підприємства та аналіз управління інформаційною безпекою. Був визначений перелік теперішніх практик, які використовує компанія.

У третьому розділі була проведена оцінка наявного підходу до управління інформаційною безпекою підприємства та виявлення прогалин. Після збору інформації та аналізу був розроблений комплексний підхід до управління інформаційною безпекою підприємства. Після чого були визначені переваги комплексного підходу управління інформаційною безпекою в противагу існуючому на базі підприємства.

Провівши аналіз можемо надати висновки, що необхідно впровадити комплексний підхід до управління інформаційною безпекою, оскільки спектр надання послуг компанією передбачає використання декількох підходів з метою охоплення всіх задіяних інформаційних активів на підприємстві. Доцільним є створення власного департаменту ІБ, що дозволить контролювати інформаційну безпеку та посилить довіру контрагентів до ступеня безпечності інформації на підприємстві «Парус». Крім того, центральной оператор отримує можливість контролювати стан всієї інформаційної інфраструктури в реальному режимі часу.

Варто постійно підвищувати рівень обізнаності персоналу щодо інформаціної безпеки на підприємстві за рахунок створеного департамену інформаційної безпеки.

Впровадити постійний моніторинг безпеки всієї інформаційної інфраструкутури підприємтсва за рахунок наявних фахівців при створенні департаменту інформаційної безпеки. Результати моніторингу безпеки будуть враховуватися при комплексонму управлінні безпекою конкретно для кожного інцидента кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tupkalo Vitalii, Cherepkov Serhii. Information security system structural modelling concept of digital processoriented enterprise (дата звернення:01.04.2024).

2. Шевчук Михайло Олександрович. Система управління інформаційною безпекою в контексті сучасних викликів (дата звернення: 01.04.2024).

3. Драб Ю., Ящук В. Основні підходи до побудови системи управління інформаційною безпекою (дата звернення: 01.04.2024).

4. Дудатьєв А. В., Войтович О. П. Моделі інформаційної підтримки управління комплексною інформаційоною безпекою (дата звернення:01.04.2024).

5. Шевченко І. Особливості формування системи економічної безпеки підприємства (дата звернення: 01.04.2024).

6. Helen Hasan, Peter Hyland. A practical approach to enterprise IT security

7. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec (дата звернення: 01.04.2024).

8. https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (дата звернення: 01.04.2024).

9. Іванченко Н.О., Подскребко О.С. Особливості реалізації системи управління інформаційною безпекою. (дата звернення: 04.04.2024).

10. О.І.Волот, Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання (дата звернення: 20.04.2024).

11. Ірина Вовк, Класифікація ресурсів підприємства. Сучасні підходи (дата звернення: 20.04.2024).

12. Скоробогатова В.В., Сутність категорії «активи»: аналіз наукових джерел (дата звернення: 20.04.2024).

13. Бланк І., Управління підприємством (дата звернення: 20.04.2024).

14. М.О. Мельник, Г.Д. Нікітин, К.О. Мезенцева Аналіз побудови моделі політики інформаційної безпеки підприємства (дата звернення:

20.04.2024).

15. https://softline.org.ua/news/analiz-informacijnoi-bezpeki-osoblivosti-ta-perevagi-novoi-poslugi-vid-softline.html (дата звернення: 20.04.2024).

16. ISO Standard. Information Technology—Security Techniques—Information Security Risk Management; ISO/IEC 27005:2018; ISO Standard: Geneva, Switzerland, 2018 (дата звернення: 20.04.2024).

17. Ievgeniia Kuzminykh, Bogdan Ghita,Volodymyr Bakhshi, Information Security Risk Assessment (дата звернення: 20.04.2024).

18. Williams, J.; OWASP Risk Rating Methodology. OWASP. (дата звернення: 20.04.2024).

19. Pipkin, D. L., Information Security: Protecting the Global Enterprise, Prentice Hall (дата звернення: 20.04.2024).

20. https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%8E_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%BE%D1%8E (дата звернення: 22.04.2024).

21. НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ, ISO/IEC 27001:2005, MOD (дата звернення: 22.04.2024).

22. О.О. Бакалинський, “Роль та місце міжнародного стандарту ISO/IEC 27032:2012 в системі стандартів серії 27к” (дата звернення: 22.04.2024).

23. О.О. Бакалинський, О.М. Богданов, В.В. Мохор, та В.М. Безштанько “Аналіз проекту ГСТУ СУІБ 1.0/ISO/IES 27001:2010 “Інформаційні технології, методи захисту, система управління ІБ. Вимоги.”(ISO/IES 27001:2005, MOD)” (дата звернення: 22.04.2024).

24. Adam Barth, Benjamin I. P. Rubinstein, Mukund Sundararajan, John C. Mitchell, Dawn Song, and Peter L. Bartlett, A Learning-Based Approach to Reactive Security (дата звернення: 22.04.2024).

25. Олійник О.В., ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ (дата звернення: 22.04.2024).

26. https://www.slideshare.net/gpaharenko/iso-27001-01dmytriyevkiev2010july (дата звернення: 24.04.2024).

27. https://intercert.com.ua/articles/posts/282-it-grundshutz-metodika-smib (дата звернення: 24.04.2024).

28. https://dduvs.edu.ua/wp-content/uploads/files/Structure/library/student/nmm/2021/da/n/nad14.pdf (дата звернення: 3.05.2024).

29. https://ela.kpi.ua/server/api/core/bitstreams/59d67094-675d-4e61-b83e-6ff98185ab7f/content (дата звернення: 3.05.2024).

30. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en (дата звернення: 8.05.2024).