Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Щітініної Поліни Ігорівни*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1] *Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Ризик-орієнтовний аудит кіберстійкості організації*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	доц. к.е.н. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2020_року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Щітініної Поліни Ігорівни* **академічної групи** *125м-19-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації *Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Ризик-орієнтовний аудит кіберстійкості організації*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ _____

Розділ	**Зміст**	**Термін виконання**
Розділ 1. Стан питання та постановка задачі	Дослідження існуючих підходів до забезпечення кіберстійкості організації та стандартів IT аудиту. Постановка задачі.	18.09.20-24.11.20
Розділ 2. Спеціальна частина	Розробка рекомендацій щодо проведення аудиту та оцінки рівня кіберстійкості.	24.12.20-14.12.20
Розділ 3. Економіка	Розрахування вартості аудиту кібестійкості та економічної доцільності проведення аудиту.	07.12.20-12.12.20

Завдання видано _____ Тимофєєв Д.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: __01.09.2020_____

Дата подання до екзаменаційної комісії: __18.12.2020_____

Прийнято до виконання _____ Щітініна П.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 68 с., 5 рис., 3 табл., 6 додатків, 102 джерела.

Об’єкт дослідження: процес аудиту кіберстійкості для бізнес організацій.

Предмет дослідження: кіберстійкість організацій.

Мета кваліфікаційної роботи: підвищення рівня кіберстійкості організації.

Методи дослідження: порівняння, аналіз, моделювання, оцінка, опис.

Актуальність теми дослідження зумовлене залежністю бізнес процесів сучасних компаній від ІТ технології та необхідності забезпечувати неперервність роботи бізнес процесів, навіть під час кіберінцидентів.

Основні результати та їх новизна полягають у визначенні особливостей та виборі методики реалізації та планування процесу ризик-орієнтовного аудиту кіберстійкості.

Практична цінність роботи полягає у підвищені рівня кіберстійкості організацій за допомогою ризик-орієнтовного аудиту.

Дана робота надає рекомендації щодо проведення аудиту кіберстійкості. Пропонує набір контролів для проведення такого аудиту, а також модель оцінювання ефективності контролів. Пропонується градація рівнів кіберстійкості, та критерії відповідності до цих рівнів.

В економічній частині було розраховано вартість проведення аудиту кіберстійкості та аудиту за одним із стандартів інформаційної безпеки, для порівняння загальної вартості обох варіантів, а також розрахована економічна доцільність проведення аудиту.

Ключові слова: АУДИТ, ВНУТРІШНІЙ АУДИТ, ЗОВНІШНІЙ АУДИТ, КІБЕРСТІЙКІСТЬ, РИЗК-ОРІЄНТОВНИЙ ІТ АУДИТ, КТИРЕРІЇ АУДИТУ, ОЦІНКА КІБЕРСТІЙКОСТІ.

РЕФЕРАТ

Пояснительная записка: 68 с., 5 рис., 3 табл., 6 приложений, 102 источника.

Объект исследования: процесс аудита киберустойчивости для бизнес организаций.

Предмет исследования: киберустойчивость организаций.

Цель квалификационной работы: повышение уровня обеспечения киберустойчивости организации.

Методы исследования: сравнение, анализ, моделирование, оценка, описание.

Актуальность темы исследования обусловлена зависимостью бизнес процессов современных компаний от ИТ технологий и необходимости обеспечивать непрерывность работы бизнес процессов, даже во время кибер-инцидентов.

Основные результаты и их новизна заключаются в определении особенностей и выборе методики реализации и планирования процесса риск-ориентированного аудита киберустойчивости.

Практическая ценность работы состоит в повышении уровня киберустойчивости организаций с помощью риск-ориентированного аудита.

Данная работа содержит рекомендации по проведению аудита киберустойчивости. Предлагает набор контролей для проведения данного аудита, а также модель оценки эффективности контролей. Предлагается градация уровней киберсустойчивости, и критерии соответствия этим уровням.

В экономической части было рассчитано стоимость проведения аудита киберустойчивости и аудита по одному из стандартов информационной безопасности, для сравнения общей стоимости обоих вариантов, а также рассчитана экономическая целесообразность проведения аудита.

Ключевые слова: АУДИТ, ВНУТРЕННИЙ АУДИТ, ВНЕШНИЙ АУДИТ, КИБЕРУСТОЙЧИВОСТЬ, РИСК-ОРИЕНТИРОВАННЫЙ ИТ АУДИТ, КТИРЕРИИ АУДИТА, ОЦЕНКА КИБЕРУСТОЙЧИВОСТИ.

ABSTRACT

Explanatory note: 68 p., 5 figures, 3 tables, 6 appendices, 102 sources.

Object of research: the process of auditing cyber resilience for business organizations.

Subject of research: cyber resilience of organizations.

The purpose of the qualification work is improving the cyber resilience of the organization.

Research methods: comparison, analysis, modeling, evaluation, description.

The relevance of the research topic is the IT technologies dependence of modern companies' business processes and urgent need to ensure the continuity of business processes, even during cyber incidents.

The main results and novelty are identified features and methodology for the risk-based audit of cyber resilience implementation and planning.

The practical value of the work lies in increasing the level of cyber resilience of organizations using risk-based audit.

This work provides recommendations for cyber-resilience audit conducting. A set of audit controls and a model of controls effectiveness assessing are provided. A gradation of cyber resilience levels and criteria for these levels compliance are proposed.

Economic part includes the cost of cyber-resilience audit conducting and of NIST 800-53 audit calculated. The total costs of both options are compared, and the economic feasibility of conducting an audit is calculated.

Key words: AUDIT, INTERNAL AUDIT, EXTERNAL AUDIT, CYBER RESILIENCE, RISK-BASED IT AUDIT, AUDIT CRITERIA, CYBER RESILIENCE ASSESSMENT.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології;

ІБ – інформаційна безпека;

ІС – інформаційна система

ПК – персональний комп'ютер;

СУІБ – система управління інформаційною безпекою;

ЄС – Європейський Союз;

NIST - National Institute of Standards and Technology;

GDPR - General Data Protection Regulation;

DPIA - Data Protection Impact Assessment;

NIS - Directive on Security of Network and Information Systems;

PCI DSS - Payment Card Industry Data Security Standard;

ERM - Enterprise Risk Management;

COSO - Committee of Sponsoring Organizations of the Treadway Commission;

ISACA - Information Systems Audit and Control Association;

COBIT - Control Objectives for Information and Related Technologies;

AS – audit standard;

PCAOB - The Public Company Accounting Oversight Board;

SP - special publication;

ISO – International Standardization Organization;

IEC -International Electrotechnical Commission;

CIA - Confidentiality, Integrity, Availability.

ЗМІСТ

ВСТУП

Resilience або, українською – стійкість це поняття, яке визначається як "здатність швидко відновлюватися після труднощів і ставати сильнішими", стало ключовим для підприємств, які стикаються з величезною кількістю ризиків. А саме: кібер-атаки, великомасштабні глобальні шахрайські афери і крадіжка персональних даних, потенційно негативні наслідки технологічних досягнень, таких як штучний інтелект, геоінженерія і синтетична біологія, які здатні впливати на навколишнє середовище, економіку і самих людей.

До недавнього часу основними об'єктами для кібер-атак були фінансові організації та урядові органи. Сьогодні розвиток бізнесу будь-якого розміру і в будь-якому секторі в тій чи іншій мірі залежить від Інтернету, і, як наслідок, загрози стали більш універсальними. У міру зростання цих небезпек, поточні підходи до забезпечення кіберстійкості більш не працюють. Управління інформаційною безпекою потребує ретельного перегляду для впровадження нових і більш вдосконалених моделей безпеки[99].

Кіберстійкість - це здатність організації запобігати, виявляти, стримувати та відновлювати загрози кібербезпеки. Кіберстійка компанія може мінімізувати час впливу та вплив незліченних серйозних загроз для даних, програм та IT-інфраструктури.

Таким чином актуальність теми дослідження зумовлене необхідністю сучасних бізнес організацій покладатися на IT технології та з мінімальними витратами на ІБ забезпечувати неперервність роботи бізнес процесів, навіть під час технічних або системних збоїв та зловмисних кіберінцидентів.

Розглядаючи стан кіберстійкості як мету організації важливо говорити про зовнішній або внутрішній аудит. Регулярне тестування контролів за допомогою аудиту, буде давати змогу реально оцінювати кроки організації до своєї цілі. Кожні впроваджені процедури чи технології будуть відбивати свій вплив у звіті

нового аудиту, порівняно з попереднім. До того ж це відмінний спосіб виявлення слабких місць або прогалин у механізмах роботи існуючої IT системи, а рекомендації за результатами аудиту направлять розвиток IT та ІБ відділів.

Об'єктом дослідження даної кваліфікаційної роботи виступає процес аудиту кіберстійкості для бізнес організацій. Предметом дослідження є кіберстійкість організацій.

Мета даної кваліфікаційної роботи полягає у підвищенні загального рівня забезпечення кіберстійкості організації.

РОЗДІЛ 1. СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1. Дослідження підходів до забезпечення кіберстійкості

Кібератаки стали загальною небезпекою для окремих людей та бізнесу: World Economic Forum відносить їх до сьомого найбільш вірогідного та восьмого найбільш ризикованого з факторів та другого за ступенем ризику для ведення бізнесу в глобальному масштабі протягом наступних 10 років[4].

Кожен суб'єкт (компанія, організація або держава) піддаються напруженням, викликаними подіями, змінами і інцидентами, які виникають в їх середовищі. Такі ситуації стресу - це нові виклики, вирішення яких буде впливати на функціонування організації до тих пір, поки не можна буде управляти нею за допомогою автоматизації[99].

Кіберстійкість поєднує в собі елементи кібербезпеки, управління безперервністю бізнесу та стійкість організації, що дозволяє організаціям продовжувати діяльність у разі несприятливих кібер-подій або технічних збоїв.

Чому це важливо для сучасних компаній бо інцидент або порушення нормального функціонування інформаційних систем може призвести до втрати продуктивності праці, штрафу за порушення регулятивних норм, збитку та завдати шкоди репутації компанії. Чим більше потрібно часу витрачаються, задля відновлення роботи бізнес процесів у нормальному режимі, тим більший ефект буде. Можливість організації запобігти порушенням обробки та/або зберігання даних та швидко реагувати на несприятливі інциденти, які неможливо зупинити, може мінімізувати фінансові втрати та шкідливий вплив на репутацію[37].

Оскільки загрози для IT систем та ресурсів компаній та організацій зростають, сучасних підходів до підтримки кіберстійкості вже недостатньо. Менеджмент кібербезпеки потребує оновлення для більш складних моделей безпеки, оскільки бути кіберстійким вже не є варіантом - це вимога. [102].

Але поки усвідомленість в цій області тільки розвивається, і проходить це досить повільно, разом з цим зростає і нерозуміння. Згідно з дослідженням, виконаним на початку 2018 року Forrester Consulting for Hiscox[92], коли було опитано понад ніж 4100 керівників, директорів ІБ, ІТ-директорів та інших ключових співробітників компаній і організацій в США, Німеччині, Великобританії, Іспанії, Нідерландах та інших країнах Євросоюзу, 57 % опитаних компаній заявили, що вони готові реагувати на атаки безпеки. Однак більш детальне вивчення непрямих питань показує, що 73% опитаних компаній мають низький рівень компетенції і досить не впевнено почувають себе у питаннях виявлення та реагування на кібератаки. І тільки 11% організацій мають в своїх департаментах безпеки експертів, а значить, добре підготовлені до вирішення проблем ІБ[92].

Однак, якщо ми подивимося на той же звіт Hiscox але за 2020 рік[91], опитування показують різке та широкомасштабне зростання витрат на кібербезпеку за останній рік - середні витрати склали 2,1 млн. доларів проти 1,5 млн. доларів попереднього року; зростання на 39%. Це відображається і як збільшення загальних ІТ-бюджетів, так і 30-відсотковий стрибок частки, відведеної на кібербезпеку (від 9,9% до 12,9%). Більше того, майже три чверті фірм (72%) мають намір збільшити свої "кібервитрати" в наступному році на 5 і більше відсотків. До того ж відсоток опитаних компаній, що значаться у звіті як «експерти» з вирішення питань кібер-інцидентів зріс до 18. Порівняння 2020, 2019 та 2018го років описаних вище показників наведено у додатку С.

Проте загроза кіберзлочинності ні в якому разі не зменшується - великі фірми все ще опиняються на лінії вогню, і більше половини організацій масштабних підприємств повідомляють про щонайменше один кібер-випадок.

Кожного шостого з тих, кого напали, утримували з метою викупу, що мало дорогі наслідки. Найвищі збитки, пов’язані з вимогами, досягли 50 мільйонів доларів для однієї нещасної організації[82].

У той же час, компанія, яка стала стійкою, буде визнавати, що виникають збої і помилки, і буде мати кошти для відновлення нормальної роботи щодо забезпечення безпеки активів і власну репутацію. Коротше кажучи, організація здатна вийти з інциденту сильнішою, застосовуючи зміни, здатні ще поліпшити її захист[99].

Тож кіберстійкість викликає дедалі більшу стурбованість чи інтерес організацій, важливих секторів інфраструктури, регіонів та держав[66].

Кіберстійкість, як і безпека, є проблемою на багатьох рівнях в організації. Чотири цілі щодо кіберстійкості, які є спільними для багатьох визначень стійкості, включені у визначення та концептуальну основу, щоб забезпечити зв'язок між рішеннями щодо управління ризиками на рівні бізнес-процесу та на системному рівні з тим і на рівні організації. Стратегії управління організаційними ризиками можуть використовувати цілі кіберстійкості та пов'язані із ними стратегії для досягнення кіберстійкості[95].

Зосередження уваги на ризиках та стійкості допомагає планувати та прогнозувати можливі проблеми, швидко вирішувати їх та розвивати здатність процвітати в умовах збоїв, та зловмисних подій[10, 11].

1.1.1 Визначення кіберстійкості та її основних принципів

Кіберстійкість може розглядатися на різних рівнях, від цілих країн до організації, або окремих процесів та технічних систем.

В залежності від контексту та ситуації, слово «Кіберстійкість» має декілька концепцій. Одна з них розглядає термін як міру того на скільки добре об’єкт (організація, система, країна тощо) зможе встояти у разі кібератаки і при цьому не знизивши ефективність бізнес процесів[5]. Інша, як стан захищеності при якому об’єкт зможе нормально функціонувати у разі зловмисних кіберподій, або швидко відновитися після них.

Узагальнюючи, можна сказати, що кіберстійкість - це здатності постійно отримувати передбачуваний результат, незважаючи на несприятливі кіберподії.

У ролі несприятливих кіберподій можуть виступати як дії спричинені людьми так і природними факторами. До другої категорії будуть входити явища на кшталт пожеж, повінів, землетрусів, злив та ураганів[1]. Все це може спричинити пошкодження технічного обладнання та/або шляхів комунікацій, що в свою чергу стає загрозою для цілісності та доступності інформаційних ресурсів та/або засобів їх обробки.

Застосовуючи на практиці кіберстійкість, її слід розглядати як запобіжний засіб для протидії людським помилкам та незахищеному програмному забезпеченню (та апаратному забезпеченню). Тому метою кіберстійкості є активний захист всього підприємства, беручи до уваги всі незахищені компоненти інфраструктури[5].

Документ Розробка кіберстійких систем: інженерний підхід до безпеки систем від NIST[12, 95] визначає головні цілі кіберстійоксті за у вигляді таблиці 1.1.

Таблиця 1.1 - Цілі Кіберстійкості[95]

Ціль	Опис
Передбачити	Підтримуйте стан готовності до інцидентів та збоїв IT систем.
Витримати	Продовжуйте підтримку основних бізнес функції, незважаючи на труднощі.
Відновитися	Відновлюйте нормальну роботу бізнесу під час і після нападу або збою.
Адаптувати	Пристосовуйте бізнес функції та/або підходи до їх підтримки щоби передбачити та опередити можливі зміни у технічному, експлуатаційному середовищах та середовищі загроз.

Ціллю кіберстійкості є забезпечення неперервності бізнес процесів, незважаючи на можливі завади у вигляді кібер-інцидентів. Головний намір у тому щоби швидко та ефективно відновитися після інциденту, або навіть під час нього.

Кіберстійкість орієнтована на бізнес, в тому сенсі, що вона спрямована на постійне досягнення запланованих результатів бізнесу, незважаючи на несприятливі кіберподії. Давайте розглянемо основні характеристики кіберстійкості, і також виділимо відмінності між кіберстійкістю та її кібербезпекою. Виділяють п’ять визначальних характеристик кіберстійкості наведених нижче[1].

Об’єкт характеристика. Хоча загальною метою кібербезпеки є захист мережевих IT та інформаційних систем, кіберстійкість зосереджена на своїй головній цілі – забезпеченні нормального функціонування бізнесу бізнесу. Іншими словами, забезпечення роботи бізнесу - це передбачуваний результат для даного об'єкта. Отже, можна сказати, що система є стійкою, коли вона здатна принести користь бізнесу навіть в умовах несприятливих кіберподій, наприклад використовуючи альтернативні способи ведення бізнесу. Як результат, будь-які зусилля, що стосуються кіберстійкості, повинні сприймати бізнес як вихідну точку, а не інформаційні технології. Наприклад, одним із способів розпочати огляд кіберстійкості є чітке визначення загальних цілей бізнесу[14].

На рисунку 1.1 наглядно показані результати опитування 2018го року, європейських компанії різного профілю направленості бізнесу та масштабу[92]. Питання стосувалися швидкості виявлення та реагувань на кібератаки наприклад проникнення, або витоки інформації. На схемі видно, що у 20% та 17% опитаних на виявлення успішно реалізованої кібератаки в середньому йдуть тижні та місяці, відповідно, а у більшості – 31% компанії роками навидь не підозрюють, про ставишся напад. Не менш цікаві результати щодо строків стримування виявлених атак. Більше половині опитаних потрібно для цього декілька місяців, а для ще 8% навіть років.

Рисунок 1.1 - Тривалість етапів реагування на кібератаки[92, 99]

Намір кіберстійкості. Намір, або ціль, відноситься до основних властивостей системи або систем. З точки зору безпеки, намір полягає в тому, щоб спроектувати або захистити системи так, щоб вони мали властивість бути безпечними. По суті, система повинна працювати в звичайному режимі і мати можливість протистояти кіберподіям. На додаток до цього важливо, щоб еластичні системи могли мати контрольований збій. Ми називаємо це безпечним для збоїв у таблиці 3. Важливість здатності до контрольованого виходу з ладу виявляється в декількох методах для проектування стійких систем. Наприклад, одні автори[15] прямо говорять про необхідність систем для "адаптації" та "відновлення" у рамках кіберстійкості, тоді як звіти MITRE[16] посилаються на подібні але трохи інші дії: "реагування" та “відновлення " систем. Таким чином, стійка система повинна бути за задумом спроможна вийти з ладу.

Підхід. Третім визначальним аспектом кіберстійкості є загальний підхід, що застосовується. Дещо спрощений погляд на безпеку полягає в тому, що він застосовується в системі. Наприклад, зашифровані комунікації можуть застосовуватися до зв'язку між системою та її користувачами. Подібний приклад -

організації можуть створювати окремі команди безпеки, які займаються лише захистом своїх систем. Однак підхід до стійкості мав би набагато глибший вплив на системи, що "захищаються", що призвело б до необхідності дозволити стійкості бути внутрішньою частиною IT-систем та загальним функціонуванням бізнесу. Стійкість просто повинна бути вбудованою, а не надбудовою. Наприклад, Голдман у своїй статті[17] посилається на необхідність використання декількох таких активних методів, як альтернативні операції та динамічний склад функцій при побудові стійких систем.

Архітектура та основа кіберстійкості. Архітектура стосується внутрішньої структури системи і виражається як складові модулі систем та їх взаємозв'язки. Що стосується еластичних систем, архітектура повинна бути структурована, щоб забезпечити частковий збій. Отже, це так краще розглядати архітектуру як таку, що складається з декількох шарів захисту, а не являє собою тверду зовнішню оболонку. Потім кожен шар повинен бути спроектований таким чином, щоб він відповідав принципу безпечного відмови, як описано раніше. Хоча при розробці захищених систем зазвичай пропонується використання декількох рівнів захисту, різниця тут полягає в тому, що архітектура повинна бути особливо придатною для відновлення кожного рівня[18].

Обсяг дії/розповсюдження кіберстійкості. Обсяг аналізу кіберстійкості не може враховувати лише одну систему чи організацію та її безпосереднє оточення. Причини на це дві: по-перше, загроза може походити від будь-якого з безлічі взаємозв’язків, які система має та підтримує. По-друге, взаємозв'язок з іншими системами (наприклад, постачальниками) також може бути міцним, коли мова йде про здатність систем відновлюватися від несприятливих подій. Наприклад, якщо мережі піддають систему, або її частину уразливості, то вони також становлять основу стійкості цієї системи. Таким чином, важливо мати широкий спектр і обстежити мережу організацій та систем, частиною якої є система, що розглядаються. Збільшений обсяг є основою як для аналізу вразливості, так і як

джерела стійкості[19]. У принципах кіберстійкості, наведених нижче це чітко відображається.

1.1.1.1 Принципи кіберстійкості

Принципи забезпечують основу, на якій можуть бути розроблені, впроваджена та оцінена стратегія досягнення посиленого стану стійкості організації перед несприятливими кіберподіями[13]. Концепція стійкості по суті розглядає несприятливі кіберподії як частину звичайних операцій. Отже, відмінність від концепції безпеки може бути вирішальною - вона дозволяє організаціям включати заходи протидії та плани на випадок непередбачених ситуацій як частину того, що можна розглядати як новий „нормальний" стан[20].

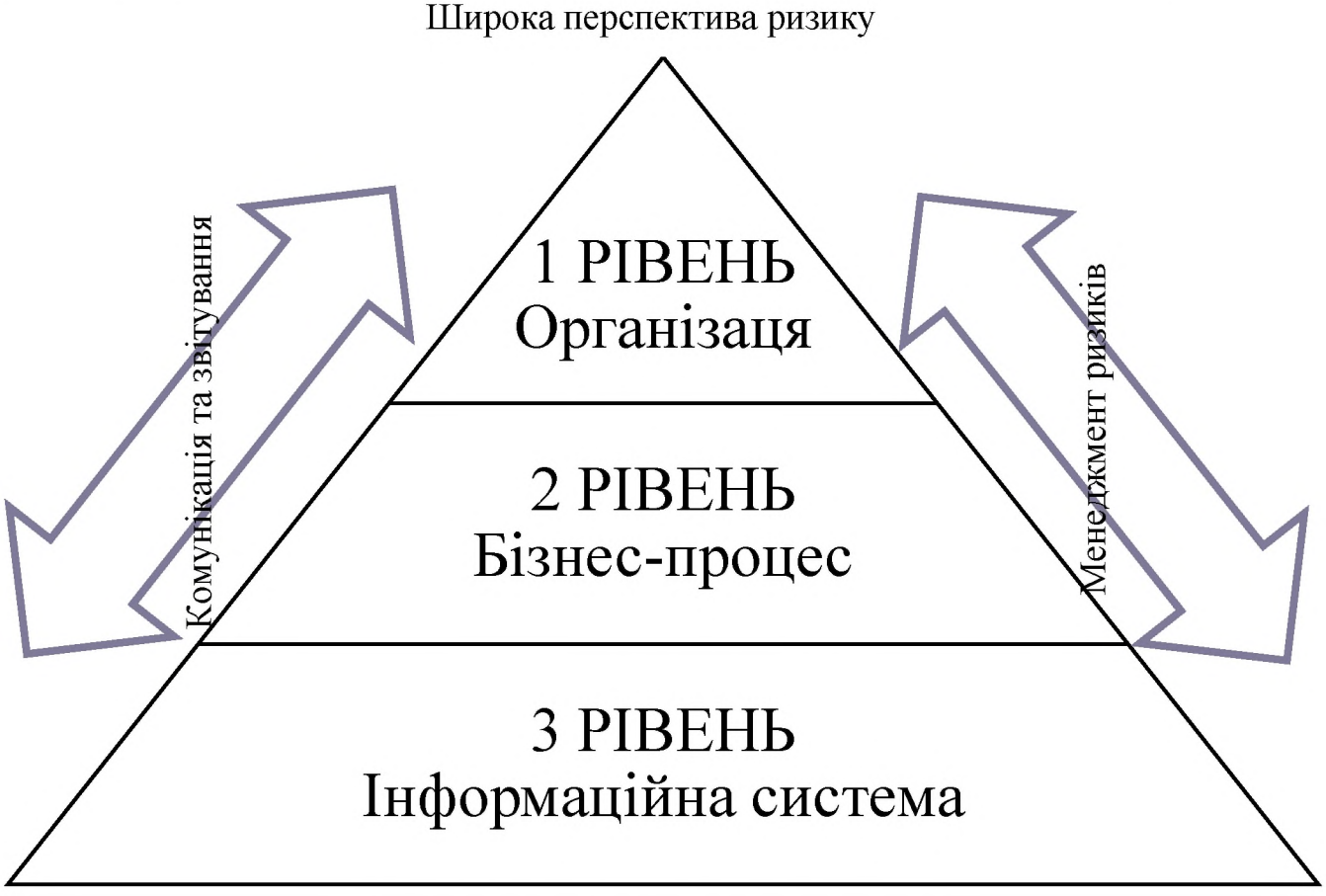

Рисунок 1.2 – Підхід до управління ризиками у масштабах організації[23]

Розглянемо кіберстійкість у контексті стандартної моделі управління ризиками, що зображено на рисунку 1.2. Цілі кіберстійкості (передбачення, відновлення та адаптація та інші) пов'язані з рішеннями щодо управління ризиками на рівнях бізнес-процесу, системи та стратегією управління ризиками організації. Для вирішення питань кіберстійкості стратегія управління ризиками організації повинна включати в себе формування кіберзагроз, стратегії досягнення цілей кіберстійкості та вибір факторів, для визначення пріоритетів та інтерпретацій цілей кіберстійкості на рівні бізнес-процесу та системи. Стратегії досягнення цілей щодо кіберстійкості перераховано та описано нижче.

1. Передбачення. Стримування, уникнення та запобігання - це стратегії передбачення потенційних загроз. Інші стратегії включають планування (тобто виявлення наявних ресурсів та створення планів використання цих ресурсів, якщо загроза матеріалізується), підготовку (тобто зміна набору доступних ресурсів та здійснення планів) та морфінг (тобто постійну зміну системи для того, щоб змінити поверхню атаки).

2. Витривалість. Стратегії протистояння реалізації потенційних загроз, навіть коли ці загрози не виявляються, включають поглинання (тобто прийняття певного рівня шкоди для певного набору елементів системи, вжиття заходів для зменшення впливу на інші елементи системи або на систему як в цілому та автоматичне усунення пошкоджень), відхилення (тобто перенесення подій загрози або їх наслідків на різні елементи системи або в системи, крім тих, на які було націлено або спочатку вплинуло), та відкидання (тобто видалення елементів системи або навіть системи як ціле, засноване на ознаках пошкодження, або замінюючи ці елементи, або дозволяючи системі або бізнес-процесу працювати без них).

3. Відновлення. Стратегії відновлення включають реверсію (тобто тиражування попереднього стану, який, як відомо, прийнятний), відновлення (тобто реплікацію критичних та допоміжних функцій до прийнятного рівня або

використання існуючих системних ресурсів) та заміну (тобто заміну пошкодженого, підозрюваного, або вибрані елементи системи з новими, або переназначення існуючих елементів системи для обслуговування різних функцій з метою виконання критичних та допоміжних функцій, можливо різними способами). Виявлення може підтримати вибір стратегії відновлення. Однак система може застосовувати ці стратегії незалежно від виявлення для зміни поверхні атаки.

4. Адаптувати. Стратегії адаптації включають виправлення (тобто, видалення або застосування нових засобів управління для компенсації виявлених вразливостей або слабких місць) та перевизначення (тобто зміна вимог системи, архітектури, дизайну, конфігурації або операційних процесів)[23].

Стратегія організаційного управління ризиками включає аспекти, які можуть обмежити набір рішень щодо кіберстійкості, які вона розгляне. Ці аспекти включають:

- філософія зменшення ризиків в організації (наприклад, дотримання стандартів належної практики, включення найсучасніших технологій та компроміси між стандартами передової практики та передовими технологіями захисту, просування сучасного рівня).
- типи зовнішньої координації, в якій буде брати участь організація (наприклад, споживач інформації про загрози, двонаправлений обмін інформацією про загрози, співпраця чи координація для протидії загрозам, співпраця).
- чи можна і як використовувати обман.

У таблиці 1.2 узагальнюються аспекти стійкості та наводяться керівні принципи щодо вирішення проблеми кіберстійкості.

Таблиця 1.2 - Принципи кіберстійкості відповідно до характеристик[20]

Характеристика	Принципи кіберстійкості
Об’єкт	Забезпечення нормальної роботи бізнесу: 1) Стійкість спрямована на збереження цілей бізнесу, а не IT-систем, під час несприятливих кібер-подій. 2) Аналіз стійкості повинен мати за початкову точку саме потреби бізнесу, а не IT-систем.
Намір	Формування системи безпечної для відмови: 3) Стійкі системи повинні бути спроектовані таким чином, щоб мати можливість контрольованого виходу з ладу, а не бути спроектованими виключно для захисту від відмов.
Підхід	Побудування безпеки зсередини: 4) Стійкість перед зловмисними кібер-подіями та вбудована в структуру організації та її IT-системи, а не додається окремими функціями або групами.
Архітектура	Захист складений з декількох ступенів: 5) Стійка архітектура містить кілька ступенів, кожен з яких здатний захистити та відновити роботи системи, а не один рівень захисту на який покладаються всі сподівання.
Обсяг	Цілісна мережа організації: 6) Для управління стійкістю бізнес і IT-системи слід розглядати як взаємопов'язану мережу, а не як окремі одиниці аналізу із середовищем. 7) Стійкість розглядає мережеві взаємозв’язки організацій та систем як сили та слабкості, а лише як джерело загроз.

Кіберстійкість - це циклічний процес. Напад аналізується ретроспективно, а зібрані уявлення вливаються в актуалізацію стратегічних вказівок щодо кіберстійкості[101].

Створення "циклу стійкості". Організації повинні розуміти і впроваджувати процес "циклу стійкості", який допоможе співробітникам ІБ постійно працювати з урахуванням досвіду заблокованих і/або виявлених загроз. Фази стійкості наведені далі за текстом та схематичне зображення циклу зображено на рисунку 1.3[99].

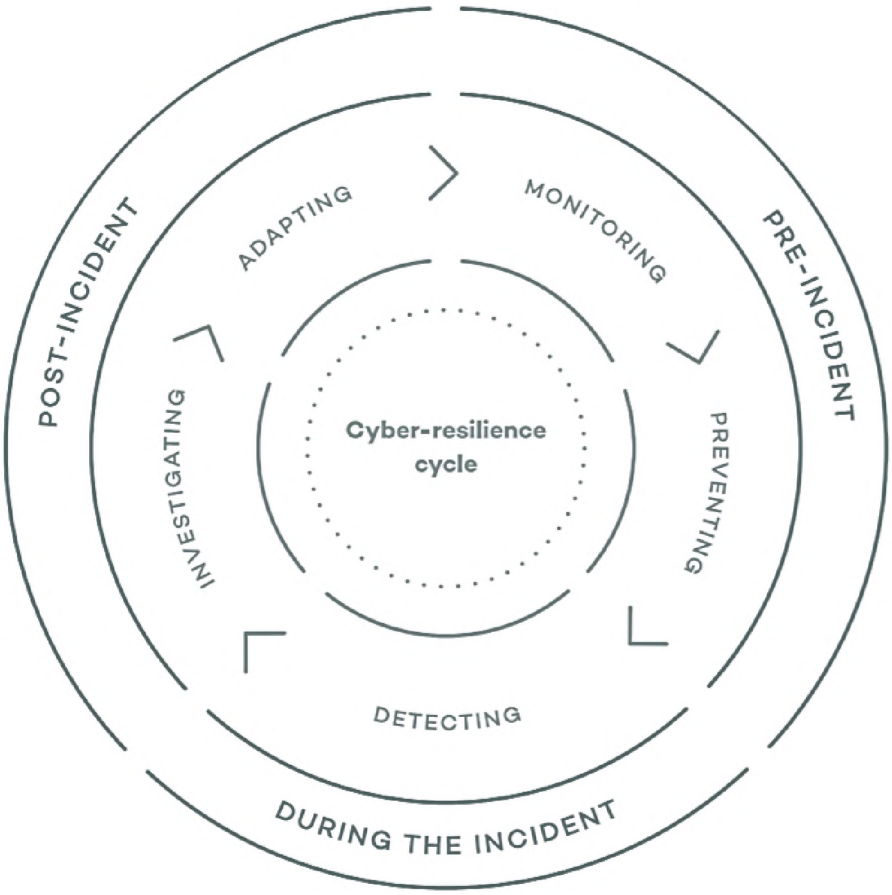

Рисунок 1.3 – Цикл кіберстійкості[99]

На етапі, що передує інциденту, краще запобігати і протистояти загрози, використовуючи вдосконалені технології, які виявляють відомі і невідомі ("нульового дня") шкідливі програми.

Під час інциденту швидко реагувати за рахунок виявлення, стримування і реагування на раптові події, які загрожують організації, щоб мінімізувати їх

наслідки для бізнесу, а також скористатися новими парадигмами, які виникають як результат використання можливостей моніторингу і видимості.

На етапі після завершення інциденту необхідно аналізувати його наслідки поряд з безперервним досягненням стратегічних цілей безпеки і відновленням операційного середовища таким чином, щоб усувати майбутні джерела подібних проблем. Це саме те, що називається "зменшення поверхні атаки"[99].

Адаптація має дуже важливе значення. Корпоративні процеси, технології, інструменти і сервіси безпеки повинні переглядатися й корегуватися в міру розвитку загроз в процесі постійного вдосконалення, заснованого на обережності. "Бути стійким" означає, що така адаптація повинна виконуватися в мінімально короткі періоди часу з максимальною швидкістю (бажано навіть в реальному часі)[99].

1.1.2 Методи досягнення кіберстійкості

Інформаційну безпеку слід розглянути як проблему управління корпоративними ризиками, а не як проблему, пов'язану лише з IT. При такому підході ключові елементи управління містять:

- пріоритетність найбільш цінних активів компаній;
- пріоритетність, знання та розуміння найбільш актуальних противників та загрозу для кожної організації;
- знання та введення найкращих засобів захисту від поточних та потенційних загроз;
- будьте готові до моменту, коли противники можуть переглядати всі технології безпеки та їх виявлення, підтримку та як можна швидше застосовувати їх дії для мінімізації корпоративного господарства;
- приqняття кризисної позиції, в рамках якої здійснюється постійний та активний пошук загроз, та виявлення вразливих місць, які внаслідок цього можуть бути потенційними джерелами загроз, для зменшення масштабу атаки;

- управління корпоративним рівнем будь-яких комунікаційних інцидентів;
- визначення та безперервне виконання ініціативи щодо мінімізації ризиків та відновлення безперервного удосконалення в управлінні корпоративною безпекою[99].

Техніки досягнення кіберстійкості - це сукупність або клас практик та технологій, призначених для досягнення однієї або кількох цілей або завдань шляхом надання можливостей.

Чотирнадцять методів відносять до процесу відбудування системи кіберстійкості відповідно до другої частини стандарту NIST SP 800-160[95].

1. Адаптивна відповідь: впроваджуйте гнучкі дії для управління ризиками;
2. Аналітичний моніторинг: Моніторинг та аналіз широкого спектру властивостей та поведінок у системі, що виконується на постійній основі та узгоджено;
3. Контекстна обізнаність: створювати та підтримувати поточні уявлення про стан бізнес процесів та функцій з урахуванням можливих зловмисних подій або збоїв;
4. Злагоджений захист: забезпечити координаційні та ефективні механізми захисту;
5. Обман: ввести в оману, заплутати, приховати критично важливі активи або викрити противнику підставні активи;
6. Різноманітність: використовуйте неоднорідність, щоб мінімізувати відмови загального режиму, зокрема зловмисні дії, що використовують загальні вразливості;
7. Динамічне позиціонування: розподіл та динамічне переміщення функціональних можливостей або системних ресурсів;

8. Непостійність: генеруйте та утримуйте ресурси за потреби або протягом обмеженого часу;

9. Обмеження привілеїв: обмежте привілеї на основі атрибутів користувачів та елементів системи;

10. Перебудова: націлити системні ресурси на поточну організаційну місію або функції бізнесу, щоб зменшити ризик;

11. Надмірність: майте кілька захищених екземплярів критичних ресурсів;

12. Сегментація: визначте та відокремте елементи системи на основі критичності та надійності;

13. Обґрунтована цілісність: з'ясувати, чи не пошкоджені критичні елементи системи;

14. Непередбачуваність: вносіть зміни випадково або непередбачувано.

Кожна техніка характеризується як своїми можливостями, так і передбачуваними наслідками використання технологій або процесів, які вона включає. Методи кіберстійкості відображають розуміння загроз, а також технологій, процесів та концепцій, пов'язаних з підвищенням кіберстійкості до вирішення загроз. Інженерна система кіберстійкості передбачає, що методики кіберстійкості будуть вибірково застосовуватися до архітектури або дизайну організаційної місії чи ділових функцій та допоміжних системних ресурсів[77, 78, 95].

Очікується, що методики кіберстійкості змінюватимуться з часом у міру розвитку загроз, досягнення на основі досліджень, розвитку безпеки та появи нових ідей.

Методи досягнення кіберстійкості також взаємозалежні. Наприклад, техніка аналітичного моніторингу підтримує контекстну обізнаність. Однак техніка непередбачуваності відрізняється від інших технік тим, що вона завжди застосовується у поєднанні з якоюсь іншою технікою (наприклад, робота з

технікою динамічного позиціонування для встановлення непередбачуваного часу для перестановки потенційних цілей, що представляють інтерес)[95].

Документ ISO 22316 Безпека та стійкість[13] пропонує звернути увагу на такі фактори, що сприяють стійкості, описані нижче.

Визначення показників ефективності, що використовуються в процесі оцінки. Джерела, які можна застосувати для оцінки стійкості ІТ систем організації можуть включати наявну управлінську інформацію та звіти внутрішнього або зовнішнього аудиту, процеси бізнес-аналізу та звітність про проекти.

Для визначення показників ефективності вище керівництво повинно:

- визначити відповідні цілі щодо стійкості організації;
- розробити критерії вимірювання, які використовуватимуться для моніторингу та оцінки стану атрибутів стійкості організації;
- відстежувати та оцінювати загальну зрілість та результативність роботи організації;
- визначити, що потрібно оцінювати та контролювати, а також методи, які дозволять отримати достовірні результати та постійну оцінку стійкості організації;
- визначити пороги, при яких результати оцінки вважатимуться прийнятними;
- прийняти рішення про те, як механізми оцінки та моніторингу будуть паралельними, підтримувати або бути інтегрованими в існуючі процеси моніторингу;
- встановити, як результати моніторингу та вимірювання будуть аналізуватися, оцінюватися та повідомлятися[13].

Визначення вразливостей. Початкова оцінка стійкості організації може бути використана для інформування про будь-яких термінових дій, та посилення концепції стійкості організації із зацікавленими сторонами.

Для цього організація повинна:

- провести огляд, застосовуючи узгоджені показники для визначення стійкості організації перед впровадженням процесу моніторингу;
- визначити, чи є стійкість прийнятною для вищого керівництва або не відповідає вимогам організації;
- розглянути відповідні стратегії для усунення будь-яких суттєвих прогалин, які є в оцінці[13].

Моніторинг та оцінка стійкості організації допомагає виявити ознаки можливих проблем. Неможливість виявити ці ознаки може обмежити здатність організації вирішувати проблеми до того, як вони матимуть вплив на системи та бізнес функції, а також може обмежити ефективність та збільшити витрати на будь-які пом'якшувальні дії.

Для зменшення зловмисного впливу на ІТ системи, організація повинна:

- застосовувати існуючі методи та процеси моніторингу для оцінки атрибутів, що сприяють їх стійкості;
- контролювати ефективність ініціатив, створених для управління ризиками, в тому числі тих, що керуються встановленими дисциплінами управління;
- розглянути можливість використання опитувань працівників та споживачів, що забезпечують показники стійкості в організації;
- намагатись зрозуміти, які дані потрібні для оцінки стійкості та забезпечити процес оцінки, що підтверджує це[13].

Вище керівництво повинно проводити періодичні огляди, щоб гарантувати, що стійкість організації продовжує відповідати очікуванням. Огляд повинен враховувати зміни в контексті організації, включаючи:

- зміни в організаційному баченні, стратегії чи цілях;
- основні структурні зміни або зміни бізнес-моделі, включаючи злиття, поглинання та продажі;
- нові ринки або території, на які вийшла організація;

- нещодавно представлені товари та послуги;
- значні кадрові зміни, в тому числі вищого керівництва;
- ефективність удосконалень, здійснених з попереднього огляду;
- відгуки про ефективність стійкості організації;
- зміна ризиків, які потребують вирішення.

Вище керівництво повинно:

- порівнювати результати процесу оцінки стійкості організації з іншими відповідними процесами перегляду, такими як результати відповідних внутрішніх аудитів, описи подій, планування стратегії, близькі пропуски та відповідність законодавству;
- підтвердити, що механізми моніторингу є доречними, та забезпечити внесок у виявлення та обробку питань до того, як їх наслідки стануть занадто шкідливими або буде втрачена можливість[13].

Результати моніторингу стійкості організації можуть включати підсумкові звіти, даючи вищому керівництву оцінку стійкості щодо атрибутів, що найбільш відповідають організації. Для цього вище керівництво повинно:

- використовувати поточні звіти про моніторинг для відстеження тенденцій у даних, які використовувались для оцінки стійкості організації;
- підтвердити, що поточні системи управління інформацією надають необхідні дані для підтримки вхідних даних, необхідних для моніторингу стійкості організації;
- використовувати результати процесу звітності для розробки планів дій для підвищення стійкості організації[13].

Кібер-ризики продовжують зростати в періодичності, різноманітності та потенційній збитки, які вони можуть завдати компаніям, їх торговим партнерам та їх клієнтам. Внутрішній аудит відіграє вирішальну роль у допомозі організаціям у поточній битві з управління кіберзагрозами, як шляхом надання незалежної оцінки

існуючих та необхідних засобів контролю, так і допомоги аудиторському комітету та правлінню зрозуміти та вирішити різноманітні ризики цифрового світу[36].

1.1.2.1 Відповідність стандартам, як метод досягнення кіберстійкості

GDPR (General Data Protection Regulation)[40] - Загальний регламент про захист даних це загальноєвропейський закон про захист даних, який вступив у силу 25 травня 2018 року[38, 44].

GDPR, в першу чергу націлений на захист фізичних осіб щодо обробки їх персональних даних та є їх основним правом. Документ розкриває принципи та правила щодо захисту обробки особистих даних фізичних осіб. Цей Регламент призначений сприяти досягненню простору свободи, безпеки та справедливості та економічного союзу, економічному та соціальному прогресу, зміцненню та зближенню економік внутрішнього ринку та добробуту фізичних осіб [39].

Значний за обсягом, GDPR передбачає підхід 21-го століття до захисту даних. Це розширює права приватних осіб контролювати спосіб збирання та обробки їхніх персональних даних, а також покладає цілий ряд нових зобов'язань на організації (як контролери, так і обробники), щоб вони більше відповідали за захист даних.[38, 41-43]

GDPR перелічує шість принципів обробки даних, яким повинні відповідати контролери даних. Персональні дані повинні бути:

1. Обробляється законно, справедливо та прозоро.
2. Збирається лише для конкретних законних цілей.
3. Адекватний, відповідний і обмежений необхідним.
4. Точні та, де це необхідно, постійно оновлюються.
5. Зберігається лише стільки, скільки потрібно.
6. Оброблено таким чином, що забезпечує відповідну безпеку[38, 40].

Слід також звернути увагу на DPIA (Data protection impact assessment)[49] це процедура, метою якої є визначення можливого впливу обробки персональних

даних на стан захисту персональних даних суб'єктів даних. Проведення такої процедури регламентовано статтею 35 GDPR та така процедура оцінки ризиків може стати у нагоді при загальному оцінені ризиків кіберстійкості[48].

Однак організації за межами ЄС також повинні переглянути свою цифрову діяльність, щоб визначити, чи дійсно вони підпадають під вимоги GDPR, і, якщо ні, то розробити та розпочати впровадження проектів щодо дотримання GDPR адже така доля української жінки та це поліпшить процес зберігання та обробки даних, відкриє нові можливості для роботи компанії, та випередить потенційні погіршення репутації через порушення конфіденціальності персональних даних клієнтів і/або працівників[45-57].

Directive on Security of Network and Information Systems (NIS)[58, 59] - Директива про безпеку мереж та інформаційних систем зосереджена на мережевих та інформаційних системах, з метою захисту критичної інфраструктури та економіки Європейського Союзу.

PCI DSS (Payment Card Industry Data Security Standard)[60] - це стандарт захисту інформації, призначений для зменшення шахрайства з платіжними картками за рахунок посилення контролю за безпекою даних власників карток. Стандарт є результатом співпраці між основними платіжними брендами (American Express, Discover, JCB, Mastercard та Visa), і адмініструється PCI SSC (Рада стандартів безпеки платіжних карток)[60-61].

Основні тезіси для досягнення та розвиток високого рівню кіберстійкості :

- постійний моніторинг нових тенденцій у кібератаках та оновлення захисних механізмів є ключовими;
- необхідно зосередитися не лише на технологіях, але враховувати також процеси та людей;
- необхідно проектувати, протестувати, впровадити та оновити як превентивні, так і детективні засоби контролю
- не забувайти про 4 найважливіших елементи кібербезпеки:

a) встановлення належного управління;

b) визначення та визначення пріоритетів ризиків;

c) використання встановлених рамок;

d) ризик, пов'язаний з третіми сторонами та новими технологіями, повинен бути визначений та керований[97].

1.2 Аудит як один із методів досягнення кіберстійкості

За суб'єктом виконання розрізняють внутрішній і зовнішній аудити інформаційних технологій. У додатку В, таблиці В.1 наглядно показана різниця цих варіантів за основними ознаками аудиту[67, 73, 74, 76].

Нині найбільш розповсюдженими є два основні способи застосування зовнішнього IT-аудиту в системі управління організацією: як самостійної консалтингової (аудиторської) послуги; або у складі інших видів аудиту організацій (комбінований аудит).

Як самостійна консалтингова послуга зовнішній аудит інформаційних технологій застосовується з метою отримання аудиторського висновку щодо поточного стану об'єкта аудиту)[67]. Якщо говорити про план підвищення рівня кіберстійкості IT структури організації – зовнішній консалтинговий зовнішній аудит може стати доброю відправною точкою и значно допоможе IT та ІБ відділам оцінити ризики, виявити прогалини та отримати корисні рекомендації щодо їх усунення.

Але одноразового зовнішнього аудиту буде не достатньо. Щоб оцінити вплив впроваджених засобів, поліпшених процесів, процедур тощо, необхідно проводити аудити з певною періодичністю, наприклад раз на рік. С кожною ітерацією повинна проводитися оцінка проведеної роботи та розроблятися нові плани поліпшення кіберстійкості IT систем. Замовлення послуг зовнішнього аудиту кожен рік вочевидь буде коштувати на багато більше, ніж проведення внутрішнього аудиту силами самої організації.

Внутрішній IT-аудит, зазвичай, проводиться на постійній основі з метою неперервного удосконалення IT-середовища, підвищення зрілості IT-процесів, гарантування надійності та ефективності заходів ризик-менеджменту IT, а також обґрунтування відповідних інвестицій організації тощо[67-68]. Що є ідеальним варіантом для безперервного процесу удосконалення кіберстійкості системи.

1.2.2 Основні існуючі стандарти IT аудиту

Основні діючі стандарти аудиту інформаційних систем та безпеки:

1. Концептуальні засади управління ризиками організацій ERM COSO[26, 27, 29];
2. Стандарт CoBiT від ISACA[30, 83, 81]
3. Серія стандартів AS PCAOB[24, 25];
4. Серія стандартів ISO27000;
5. Серія документів NIST SP 800 (зокрема документ NIST SP 800-53)[12, 23, 28, 77, 78, 94].

1.2.2.1 ERM COSO

ERM COSO було заплановано як структуру, яка легко використовувалася б керівництвом для оцінки та вдосконалення управління корпоративними ризиками в своїх організаціях. У свій час концептуальні засади управління ризиками організацій від COSO набули значної популярності[27].

Управління ризиками на підприємстві, згідно до ERM складається з восьми взаємопов'язаних компонентів. Ці компоненти описані нижче.

Внутрішнє середовище. Внутрішнє середовище являє собою атмосферу в організації і визначає, яким чином ризик сприймається співробітниками організації, і як вони на нього реагують. Внутрішнє середовище включає філософію управління ризиками і ризик-апетит, чесність і етичні цінності, а також те середовище, в якій вони існують.

Постановка цілей. Цілі мають бути визначені до того, як керівництво почне виявляти події, які потенційно можуть вплинути на їх досягнення. Процес управління ризиками надає «розумну» гарантію того, що керівництво компанії має правильно організований процес вибору і формування цілей, і ці цілі відповідають місії організації і рівню її ризик-апетиту.

Визначення подій. Внутрішні і зовнішні події, що впливають на досягнення цілей організації, повинні визначатися з урахуванням їх поділу на ризики або можливості. Можливості повинні враховуватися керівництвом в процесі формування стратегії і постановки цілей.

Оцінка ризиків. Ризики аналізуються з урахуванням ймовірності їх виникнення та впливу з метою визначення того, які дії щодо них необхідно зробити. Ризики оцінюються з точки зору властивого і залишкового ризику.

Реагування на ризик. Керівництво вибирає метод реагування на ризик - ухилення від ризику, прийняття, скорочення або перерозподіл ризику, - розробляючи ряд заходів, які дозволяють привести виявлений ризик у відповідність з допустимим рівнем ризику і ризик-апетитом організації.

Засоби контролю. Політики і процедури розроблені і встановлені таким чином, щоб забезпечувати «розумну» гарантію того, що реагування на що виникає ризик відбувається ефективно і своєчасно.

Інформація та комунікації. Необхідна інформація визначається, фіксується і передається в такій формі і в такі терміни, які дозволяють співробітникам виконувати їх функціональні обов'язки. Також здійснюється ефективний обмін інформацією в рамках організації як по вертикалі зверху вниз і знизу вгору, так і по горизонталі.

Моніторинг. Весь процес управління ризиками організації відстежується і в разі потреби коригується. Моніторинг здійснюється в рамках поточної діяльності керівництва або шляхом проведення періодичних оцінок.

Однак, ERM від COSO не зовсім про аудит, але він широко розкриває оду із його частин – аналіз та оцінку ризиків, тому так широко використовуються аудиторською практикою. Особливо це стосується ризик-орієнтовного аудиту про який буде сказано згодом. Розглянуті, концептуальні засади управління ризиками організацій розповідають та розкривають наступні теми:

1. Виявлення та оцінка ключових ризиків;
2. Розробка та впровадження процесів, за допомогою яких можна управляти цими ризиками;
3. Підтримання залишкових ризиків на рівні, прийнятному для організації;
4. Пов’язання ризиків із організаційними цілями[29].

1.2.2.2 CoBiT від ISACA

CoBiT - це відкритий стандарт. Вперше відредагований у 1996 році, він полегшив роботу професійних IT аудиторів. Цей стандарт - це спосіб подолати розрив у комунікації між IT-функціями, бізнесом та аудиторами, а також об’єднати безліч інших стандартів та критеріїв в єдиний ресурс, що дозволяє отримати певне уявлення про завдання та цілі ІС та керувати ними. на сучасному рівні. CoBiT враховує практично всі особливості ІС будь-якої складності та розміру.

При розробці загального плану аудиту IT слід дотримуватися відповідного підходу до оцінки ризиків, один із варіантів - використовувати COBIT для цієї мети. Концепція обертається навколо каскаду цілей COBIT, який демонструє зв'язок між рушіями та потребами зацікавлених сторін та цілями управління та управління. Каскад цілей підтримує встановлення пріоритетів управління та цілей управління на основі пріоритетності цілей підприємства[31]. Нижче наведені компоненти COBIT.

Структура. Організовує цілі управління IT та найкращі практики IT-доменів та процесів та пов'язує їх із вимогами бізнесу.

Описи процесів. Довідкова модель процесу та загальна мова для всіх в організації. Процеси відображаються у сферах відповідальності планування, побудови, запуску та моніторингу.

Цілі контролю. Надає повний набір вимог високого рівня, які слід враховувати керівництву для ефективного контролю кожного IT-процесу.

Керівні принципи управління. Допомагає розподілити відповідальність, узгодити цілі, виміряти результативність та проілюструвати взаємозв'язок з іншими процесами.

Моделі зрілості. оцінює зрілість та можливості для кожного процесу та допомагає усунути прогалини[32, 33].

Деякі переваги COBIT наведені нижче[83].

1. COBIT узгоджується з іншими стандартами та найкращими практиками і повинен використовуватися разом із ними.

2. Ця структура та підтримка найкращих практик забезпечують добре кероване та гнучке IT-середовище в організації.

3. COBIT забезпечує середовище управління, яке відповідає потребам бізнесу та служить управлінню та аудиторські функції з точки зору їх контрольних обов'язків[81].

4. Він надає інструменти для управління IT-діяльністю.

COBIT багато в чому сприяє IT-аудиту, але важливо зазначити, що це інструкція, що вимагає індивідуальних налаштувань для кожної організації. COBIT - це не універсальне рішення, а фреймворк[31].

1.2.2.3 Серія стандартів AS PCAOB

Серія стандартів AS PCAOB, що отримав найбільше розповсюдження і широко використовуються у компаніях «Великої четвірки»[34], встановлює вимоги та надає вказівки до аудиту як фінансової звітності компанії, так і оцінки керівництвом ефективності внутрішнього контролю за фінансовою звітністю[24,

25]. Так, на відміну від інших офіційних стандартів щодо безпеки інформаційних систем чи внутрішніх контролів IT, стандарти PCAOB в першу чергу були розроблені для проведення зовнішніх аудитів фінансової звітності у публічних компаніях. Однак, швидке розвинення інформаційних технології, рівня кіберзлочинності та ступеню покладання компанії на IT процеси з приводу формування фінансової звітності, буквально змусило ораганізацію включити IT аудит як обов'язкову складову фінансового аудиту. Так аудиторський стандарт 5, опублікований Радою з нагляду за обліком в публічних компаніях (англ. Public Company Accounting Oversight Board), вимагає від аудиторів використовувати для виконання аудиту системи внутрішнього контролю за підготовкою фінансової звітності таку-ж підходящу і загальновизнану модель контролю, яку менеджмент використовує для своєї щорічної оцінки ефективності внутрішнього контролю Товариства за підготовкою фінансової звітності.

Такий аудит буде вперше за все орієнтований на основні системи генерації та зберігання фінансової звітності, та допоміжні операційні системи, системи керування базами даних, програмні інструменти різного типу.

1.2.2.4 Серія документів NIST SP 800

NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" - Контролі безпечності та приватності для федеральних інформаційних систем і організацій. Суть документа полягає в описі контролів безпеки, а також інструкціях про те, як ними грамотно користуватися. Варто зауважити, що документ дуже об'ємний і опис контролів займає майже 250 сторінок, а загальна їх кількість налічує кілька сотень[77, 78, 94].

Ця публікація містить каталог контролю безпеки та конфіденційності для інформаційних систем та організацій для захисту організаційних операцій та активів, осіб, інших організацій та нації від різноманітного набору загроз та ризиків, включаючи ворожі напади, людські помилки, стихійні лиха, структурні

збої, суб'єкти зовнішньої розвідки та ризики конфіденційності. Елементи керування є гнучкими та відкритими для персонального налагодження та впроваджуються як частина загальноорганізаційного процесу управління ризиками. Елементи контролю враховують різноманітні вимоги, що випливають із потреб місії та бізнесу, законів, розпоряджень, директив, положень, політик, стандартів та керівних принципів. Нарешті, зведений каталог управління розглядає питання безпеки та конфіденційності з точки зору функціональності (тобто сили функцій та механізмів, що забезпечуються елементами керування), а також з точки зору впевненості (тобто міри впевненості у можливостях безпеки або конфіденційності, що надаються засобами управління). Звернення до функціональних можливостей та гарантій допомагає забезпечити достатню надійність продуктів інформаційних технологій та систем, які покладаються на ці продукти[24].

У порівнянні з тим же ISO 27001[85], NIST SP 800-53[28] до контролів безпеки має більше за кількістю та більш деталізовані компенсуючі заходи, оскільки ISO все ж більше орієнтований на управління ІБ, а не на конкретні компенсуючі заходи[24, 77].

Стандарт включає в себе такі групи контролів:

1. Обізнаність і навчання;
2. Аудит і звітність;
3. Авторизація та оцінка безпеки;
4. Управління конфігурацією;
5. Планування безперервності бізнесу;
6. Ідентифікація та аутентифікація;
7. Реагування на інциденти;
8. Обслуговування / технічна підтримка;
9. Захист носіїв інформації;
10. Захист від стихійних лих і фізична безпека;

11. Планування;
12. Безпека персоналу;
13. Оцінка ризиків;
14. Придбання систем і сервісів;
15. Захист систем і комунікацій;
16. Цілісність систем та захисту інформації;
17. Управління програмою ІБ[23, 28, 77, 78].

1.2.2.5 Серія стандартів ISO27000

Сімейство стандартів ISO 27000 - це низка стандартів інформаційної безпеки, що забезпечують глобальну основу для практики управління інформаційною безпекою. Вони опубліковані та розроблені International Organization for Standardization (ISO) - Міжнародною організацією зі стандартизації[92] та International Electrotechnical Commission (IEC) - Міжнародною електротехнічною комісією.

ISO / IEC 27000: 2018 зосереджується на інформаційних технологіях, методів та системах управління інформаційною безпекою[90].

ISO/IEC 27001 визначає вимоги до впровадження засобів контролю безпеки, пристосованих до потреб окремих організацій або їх частин. СУІБ призначений для забезпечення вибору адекватних та пропорційних засобів контролю, які захищають акти інформації та надають впевненість зацікавленим сторонам. Запропоновані вимоги структуровані в класифікації з 11 пунктів, які включають 39 цілей, спрямованих на 133 засоби контролю [85-87].

ISO/IEC 27001 визначає, як компанія повинна відповідати вимогам конфіденційності, цілісності та доступності своїх інформаційних активів, та включати це в Систему управління інформаційною безпекою (СУІБ) [88, 89]. Цей стандарт використовується в усьому світі організаціями, як комерційними, так і державними, як основа для управління політикою організації та реалізації

інформаційної безпеки. Він використовується малими, середніми та великими організаціями у різних сферах бізнесу. Насправді стандарт розроблений настільки гнучко, щоб його можна було використовувати в усіх типах організації. Стандарт фактично став „загальномовною" для управління інформаційною безпекою [84, 86, 87].

Дотримання стандартів серії ISO 27000 має ряд корисних переваг. Для початківців це дозволяє організації захищати критично важливі для бізнесу дані, а також допомагає захистити дані про співробітників та клієнтів. Це може допомогти надати вашим клієнтам та співробітникам більше віри у ваші процеси, кардинально покращивши вашу репутацію та потенційно уникнувши будь-яких вражень щодо того, наскільки ви надійні в очах аудиторії.

Порушення даних також може спричинити дорогі штрафи, особливо якщо ви порушите такі стандарти, як Загальний регламент про захист даних. Ці дорогі штрафи можуть неймовірно завдати шкоди не лише вашому фінансовому становищу, але й репутації. Штрафні санкції можуть також зупинити ваш бізнес, що може бути руйнівним, часто достатньо, щоб повністю зруйнувати ваш бізнес. Нарешті, дотримання стандартів серії ISO 27001 та отримання сертифікату на відповідність стандарту ISO 27001 означає, що ви підвищите довіру клієнтів і продемонструєте, що ваша компанія здатна дотримуватися найсуворіших та найвірогідніших практик безпеки[90, 93].

Також варто відмітити що організація ISACA має публікацію про відповідність(MAPPING) CobiT до ISO27001[80] та NIST переписують деякі серії SP 800, щоб вони відповідали ISO27001[24].

1.2.2 Загальний опис та етапи IT Аудиту

IT Аудит підприємства – це комплекс мір та контролів для загальної оцінки, стану IT середовища компанії, процесів, систем тощо, або оцінки відповідності до певних норм, стандартів, або критеріїв[27].

Основні функції аудиту ІБ:

- аналіз бізнес-процесів, технологій та структур ІС та їх ризиків;
- відповідність політики установи щодо управління ризиками існуючим ризикам;
- ефективність системи моніторингу ризиків та системи контролю ризиків;
- незалежна оцінка ризиків, неупереджена перевірка результатів самооцінки ризиків, реалізованих підрозділами бізнесу;
- виявлення потенційних проблем та ризиків;
- незалежний аудит проблемних ситуацій та ефективності їх вирішення;
- звіт про моніторинг та контрольний аналіз, спрямований на вдосконалення існуючої практики управління ризиками;
- аналіз та надання компанії повного профілю щодо ризиків та висновків щодо стратегій, процедур та методів управління ризиками.[30]

Аудит інформаційних технологій, при будь-якому з підходів завжди буде проходити перелічені нижче фази:

1. Планування;
2. Визначення об'єктів та обсягу аудиту;
3. Збір та оцінка доказів;
4. Документування, формування звіту та рекомендацій[3].

Етапи аудиту, що будуть розглядатися більш детально далі за розділом схематично зображено на рисунку 1.4. Наведена схема запропонована міжнародною організацією стандартизації – ISO. Загальний процес аудиту поділений на шість різних за тривалістю етапів:

1. Визначення обсягів аудиту та обстеження перед початком аудиту;
2. Планування та підготовка;
3. Збір даних та доказів;
4. Аналіз;

5. Звітування;
6. Закриття.

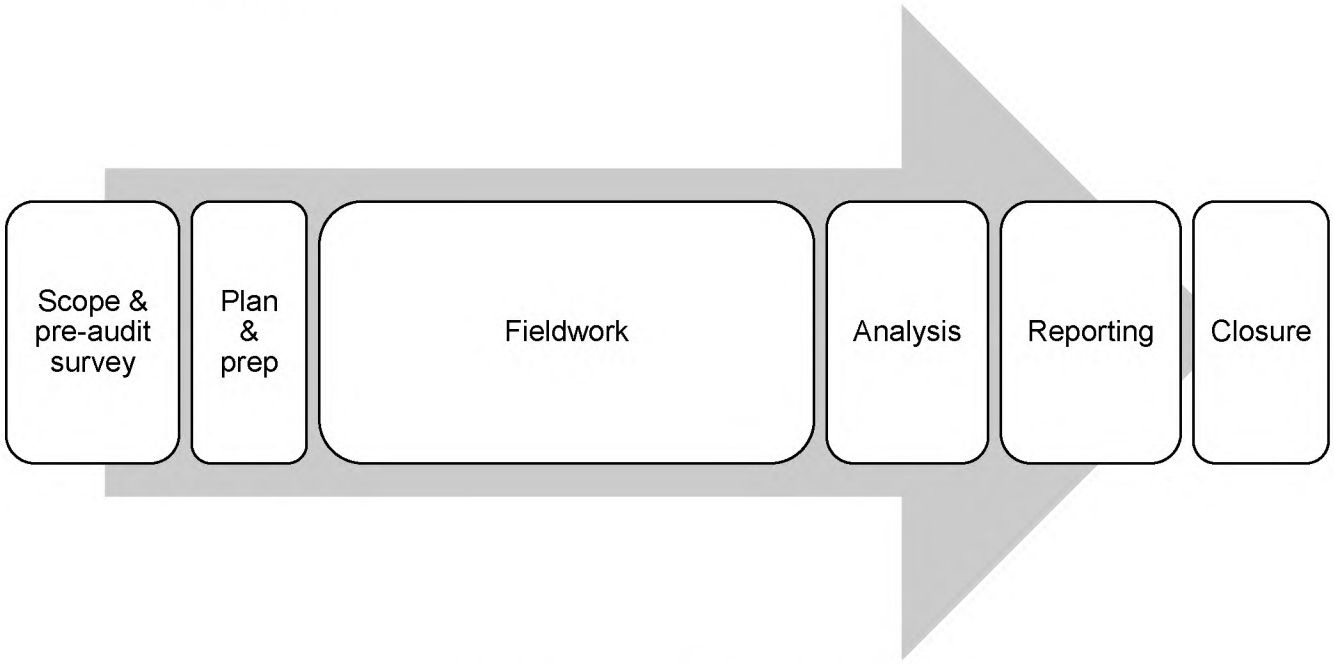

Рисунок 1.4 – Етапи аудиту[21]

1.2.2.1 Етап 1. Визначення об'єктів та обсягів аудиту та обстеження перед початком аудиту

На цьому етапі аудитори визначають основні напрямки, за якими буде проходити аудит. Визначаються будь-які об'єкти, які будуть або не будуть входити у обсяги аудиту за вибраним напрямом. Як правило, такі рішення приймаються на основі первинної оцінки ризиків та обговорення з замовниками аудиту.

Інформаційні джерела включають: загальні дослідження галузі та організації, а також стандарти на які орієнтується організація та належну практику безпеки, попередні звіти про аудит та нормативні документи організації, такі як, План розподілення та мінімізації ризиків та Політика ІБ. При визначенні об'єктів та обсягу аудиту в перш за все проводиться аналіз ризиків. У ході аналізу може використовуватися най простіший метод з переліком ризиків і їх подальшим

розподіленням на категорії: не значній, значній, дуже значний, або інші, складніші алгоритми[21].

Під час попереднього аудиторського опитування ІТ аудитори визначають та в ідеалі встановлюють контакти з основними зацікавленими сторонами що обслуговують та підтримують ІТ, несуть відповідальність за систем та інші робітники, що можуть бути задіяні у процесі аудиту. Це можуть бути менеджери з управління інформаційними ризиками та безпекою керівники відділів ІТ та ІБ, а також іншими професіоналами, такими як інженері безпеки та адміністратори безпеки; ІТ підтримка, кадровий персонал, відділ фізичної безпеки, розробники та відповідальні за впровадження оновлень у ІТ структурі, або її елементах.

На цьому етапі також запитується відповідна документація, яка буде задіяна та перевірена під час аудиту.

Зазвичай керівництво призначає одного або кількох аудиторів «супроводжуючих» - осіб, які відповідають за те, щоб аудитори могли вільно пересуватися організацією та швидко знаходити людей, інформацію тощо, необхідні для ведення їх роботи, виконуючи функції керівництва, фасилітатора та пунктів зв’язку керівництва[21].

На цьому ж етапі визначаються критерії аудиту, за якими буде оцінено отримані результати. Критерії аудиту – це принципи (або норми), які використовуються для оцінки чи тестування об’єкта аудиту[27].

Для оцінки інформаційної безпеки часто використовують критерії оцінювання захищеності інформації та інформаційних технологій (Common Criteria), що фактично визначають собою методологію, що допомагають визначати чіткі вимоги та показники рівня захищеності комп'ютерних систем. Таким чином критерії перетворюють абстрактне поняття кібербезпеки або інформаційної безпеки до чітких показників у вигляді визначених рівнів або чисельних значень. Такі показники, визначені за однаковими критеріями можна порівнювати на етапі періодичної переоцінки стану захищеності об’єкту. Показник буде змінюватися

відповідно по проведених робіт, покращуватися, якщо були присутні елементи вдосконалення, та навпаки, за умов втрати раніше присутніх контролів і/або суттєвих змін у переліку критичних складових. Окрім того такі показники наочно зображують різницю ефективності різних методів, засобів та стратегій досягнення інформаційної захищеності[7, 14, 22].

Основною базою характеристики основних критеріїв, щодо інформаційної безпеки використовують тріаду CIA. Модель тріади CIA (Confidentiality, Integrity, Availability) зводить всю інформаційну безпеку в три основних критерії: конфіденційність, цілісність та доступність[14].

Під оцінку критеріями до аналізування потрапляють три головні складові будь-якої інформаційні системи, це: технічні засоби, програмне забезпечення і комунікації. Також визначають три основні рівні: фізичний, особистий та організаційний[14, 96].

Common Criteria загальних критеріїв - це міжнародно визнана оцінка функцій безпеки, а також процесів розробки та тестування, пов'язаних з продуктами інформаційних технологій[8].

У сфері українських державно затверджених стандартів, також можна знайти документи, які можна адаптувати і застосовувати для досягнення кіберстійкості. Наприклад документ: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99[6]. Використовуючи описану у документу структуру критеріїв і роблячи акцент на таких пунктах як: стійкість до відмов, відновлення після збоїв, горяча заміна, самотестування тощо, документ може бути застосовним до оцінювання кіберстійкості у ІТ системі підприємства.

Основним результатом цього етапу є визначення переліків об'єктів аудиту, статут, лист про залучення або подібне, узгоджені між аудиторами та керівництвом клієнтів. Також отримуються списки контактів та інші попередні документи, а файли аудиту відкриваються, щоб містити документацію (робочі

документи аудиту, докази, примітки, відгуки, проекти та остаточні звіти тощо), що випливають з аудиту.

1.2.2.2 Етап 2. Планування аудиту та підготовка

Перший етап, з якого починається кожен аудит – це планування. Не дивлячись на те, що більшість робіт з цього приводу сконцентровано саме на початку, продовжуватися планування буде майже до самого формування звітності про аудит. Пов'язано це з тим, що не усі первинні оцінки ефективності контролів щодо систем та процесів певної організації виявляться точними після більш детального вивчення.

Визначення найважливіших цілей управління та управління може бути здійснено за допомогою COBIT[30, 83, 81]. Після розробки пріоритетного списку цілей цілі, звичайно, слід пристосувати до контексту підприємства, наприклад, визначивши обсяг для кожного аудиту[31].

Одна із задач планування це отримати розуміння організації і середовища у якому вона функціонує. Частіше за все, це знання набувається у процесі інтерв'ю з керівниками відділів організації. Теми та питання які повинні бути розкриті у ході опитування наведені нижче:

- основні функції та бізнес процеси організації;
- структура організації (втому числі і співпраця з зовнішніми постачальниками послуг);
- внутрішня нормативна документація стосовно іт та кібербезпеки (політики, положення, інструкції, процедурі, тощо);
- критичні інформаційні системи, та їх системи підтримки;
- природа програмного та апаратного забезпечення, що використовується;
- основні ризики які компанія сама для себе визначає;

- внутрішні чи зовнішні аудити, перевірки, тестування, що були проведені за останні рік-два;

Зібрана інформація використовується аудиторами для виявлення потенційних проблем, формулювання цілей дослідження та визначення обсягу роботи[3].

Плани аудиту визначають та встановлюють широкі межі навколо решти фаз аудиту (наприклад, часові рамки). Плани аудиту часто також включають "контрольно-пропускні пункти" - конкретні можливості для аудиторів надавати неформальні проміжні оновлення своїх управлінських контактів, включаючи попереднє повідомлення про будь-які виявлені невідповідності або потенційні невідповідності тощо. Це також можливості для висловлення будь-яких проблем з приводу обмеженого доступу до інформації або людей , а керівництву підняти будь-які занепокоєння щодо характеру аудиторської роботи. Хоча аудитори є обов'язково незалежними, вони повинні встановити рівень довіри та робоче середовище для співпраці, щоб достатньо залучитись та отримати інформацію, необхідну для аудиту IT систем. Професійний підхід, компетентність та доброчесність мають вирішальне значення.

Нарешті, можуть бути визначені терміни виконання важливих елементів аудиторської роботи, особливо для того, щоб визначити пріоритетні аспекти, які, як вважають, становлять найбільший ризик для організації, якщо внутрішні IT контролі виявиться неафективними[21].

Результатом цього етапу є план аудиту, погоджений з керівництвом.

1.2.2.3 Етапи 3 та 4. Збір та аналіз доказів

Як правило, це найдовший етап аудиту, хоча звітування може бути і тривалим також.

Аудиторські докази збираються спеціалістами, що проводять аудит, або задіяними особами, безпосередньо із систем, що підлягають аудиту. Аудитори

працюють методично за допомогою контрольного списку аудиту, наприклад, опитування співробітників, менеджерів та інших зацікавлених сторін, пов'язаних із об'єктом дослідження, перегляд документів, роздруківки та даних (включаючи записи діяльності IT систем, таких як журнали подій), спостереження за процесами IT та перевірка конфігурацій безпеки системи тощо. Аудиторські тести проводяться для оцінки та перевірки доказів у міру їх збирання. Готуються робочі документи з аудиту, в яких документуються проведені тести, зібрані докази та початкові результати[21].

Перша частина польових робіт, як правило, передбачає перегляд документації. Аудитор читає та робить примітки щодо документації, що стосується і випливає на процеси IT (наприклад, політика резервного копіювання, процедура реагування та обробки інцидентів, тощо). Аудитор формує аудиторську документацію, що складається з аудиторських доказів та приміток у формі заповнених контрольних переліків аудиту та робочих документів.

Результати огляду документації часто вказують на необхідність проведення специфічних аудиторських випробувань, щоб визначити, наскільки точно існуючі процеси IT, що реалізуються в даний час, відповідають. Результати аудиторських випробувань, як правило, реєструються аудиторами в контрольних списках, разом із доказами, примітками та іншою документацією у файлі аудиту[21].

Тести на відповідність технічним вимогам можуть бути необхідними для підтвердження того, що IT-системи налаштовані відповідно до політики, стандартів та керівних принципів інформаційної безпеки організації. Автоматизована перевірка конфігурації та інструменти оцінки вразливості можуть прискорити швидкість, з якою проводяться перевірки технічної відповідності, але потенційно можуть створити власні проблеми безпеки, які потрібно враховувати[21].

Результатом цього етапу є накопичення аудиторських робочих документів та доказів у аудиторських файлах.

Накопичені аудиторські докази сортуються та подаються, переглядаються та вивчаються з урахуванням інформаційних ризиків та цілей чи вимог стандартів та обсягу та цілей аудиту. На цьому етапі можуть бути складені попередні висновки, висновки та рекомендації щодо будь-яких визначених важливих питань[21].

1.2.2.4 Етапи 4 та 5. Документування, формування звіту та рекомендацій

Звітність є важливою частиною процесу аудиту. У подальшому, цей документ стане основою для наступних аудитів, внутрішніх проектів компанії з IT безпеки, аналізу ризиків. Аудиторська документація повинна бути чіткою та повною. До повного переліку документації обов'язково повинні бути додані усі зібрані у процесі аналізу та оцінки докази[3].

Типовий звіт про IT аудит містить такі елементи, деякі з яких можна розділити на додатки або окремі документи:

- назва та вступ, що називає організацію та уточнює обсяг, цілі, період охоплення та характер, час та обсяг виконаної аудиторської роботи;
- резюме із зазначенням ключових висновків аудиту, короткий аналіз та коментарі, а також загальний висновок;
- запланований звіт містить перелік конкретних одержувачів (оскільки вміст може бути конфіденційним) та містить відповідну класифікацію документів або інструкції щодо обігу;
- опис повноважень, методів аудиту тощо окремих аудиторів та членів групи;
- детальні висновки та аналіз аудиту, іноді з витягами з підтверджуючих доказів у файлах аудиту, де це допомагає зрозуміти;
- висновки та рекомендації аудиту, які, можливо, спочатку були представлені як попередні пропозиції для обговорення з керівництвом та врешті включені як узгоджені плани дій залежно від місцевої практики;

- офіційна заява аудиторів про будь-які застереження, кваліфікацію, обмеження сфери застосування або інші застереження щодо аудиту;
- залежно від звичайної практики аудиту, керівництву може бути запропоновано дати короткий коментар або офіційну відповідь, прийнявши результати аудиту та взявши на себе будь-які узгоджені дії[21].

Важливо, щоб існувала фактична база, що означає достатню кількість належних аудиторських доказів для підтвердження повідомлених висновків. Процеси забезпечення якості аудиту повинні забезпечувати звітність про все, що підлягає звітуванню, і про все, про що повідомляється, як правило, на основі перегляду файлу аудиту досвідченим старшим аудитором. Формулювання проекту аудиторського звіту перевіряється для забезпечення читабельності, уникнення двозначності та непідтримуваних тверджень. Після схвалення керівництвом аудиту до обігу, проект звіту про аудит зазвичай представляється та обговорюється з управлінням. Подальші цикли розгляду та перегляду звіту можуть мати місце до його остаточного завершення. Завершення, як правило, передбачає дотримання керівництвом плану дій[21].

Відповідно до домовленостей та обставин, аудитор може пропонувати офіційні або неофіційні рекомендації, вказівки та поради (наприклад, сприяння передовій практиці та іншим вдосконаленням), але конкретного рішення не обов'язково надавати. Якщо висновок аудиту висловлюється ефективно, а питання дискретне, рішення часто буде само собою зрозумілим. Зрештою, завдяки незалежності аудиту відповідальність керівництва, а не аудиту, полягає у вирішенні питань, діючи в найкращих інтересах організації та враховуючи інші пріоритети та цілі бізнесу. Керівництво повинно вирішити, що робити і коли це робити, якщо взагалі. Коротше кажучи, аудит має лише рекомендаційний характер.

Результатом цього етапу є заповнений звіт про аудит ІТ систем, підписаний, датований та розподілений відповідно до умов листа про аудиторську діяльність.

Після формування звіту аудиту та рекомендацій за його результатами, завжди буде проходити дискусія чи доклад, з цього приводу. Планується зустріч з керівництвом організації, ІТ та ІБ відділів та можливо інші, де спеціаліст з ІТ аудиту, або аудиторська команда повинна донести результати обстеження об'єкту аудиту, висновки, та поради щодо вдосконалення процесів, документів, тощо. Це повинно відбутися незалежно від того чи проводився внутрішній аудит, чи незалежною третьою стороною[21, 30].

Для внутрішнього аудиту, дале ще може йти етап відстеження результатів впровадження аудиторських рекомендацій, який не буде актуальним для більшості зовнішніх перевірок[30]. Однак гарною практикою є отамання підтвердження від керівників відповідних відділів про те, що вони були ознайомлені з результатами аудиту, що вони згодні або оскаржують результати та рекомендації надані для виконання, та зобов'язується впровадити перелічені поради.

1.2.3 Дослідження основних підходів аудиту інформаційних технологій

До основних підходів, щодо аудиту інформаційних технологій відносять:

- аудит процедури – розглядає окремі процедуру, всі пов'язані з нею аспекти (задіяні частини систем, процедури, транзакції тощо);
- системно-орієнтований підхід – розглядає окрему систему, усі пов'язані з нею контролі;
- ризик-орієнтований підхід – визначає перелік ризиків і перевіряє чи всі вони покриті у повній мірі, за результатами аудиту;
- аудит прикладної програми – перевіряє заходи контролю прикладних програмам;
- аудит проекту – розглядає певний проект, процес його реалізації та документування[2, 30].

1.2.3.1 Ризик-орієнтований підхід

Цей підхід може бути чи не найпопулярнішим підходом серед усіх визначених раніше. Основна концепція підходу, заснованого на оцінці ризиків, полягає у тому, щоб робити менше робіт, але при цьому все ж знижувати аудиторські ризики, та відповідати поставленим перед аудитом цілям.

Цей підхід головним чином здійснюється шляхом глибокого розуміння бізнесу, середовища, а також внутрішніх контролів, що практикує організація, аудит якої належить зробити. Після розуміння, аудиторам доведеться проаналізувати сфери можливих ризиків. Як тільки аудитори визначать зони ризику, буде створено програму аудиту.

При такому підході аудиторам не доведеться витрачати багато часу на тестування контролів, які покривають незначні або недостатньо значні ризики у рамках цілей аудиту[2].

1.3 Постановка задачі

Виходячи з проведеного дослідження щодо кіберстійкості та підходів до проведення IT аудиту виділяємо наспані задачі:

- використовуючи проведе дослідження, щодо основних принципів кіберстійкості та рекомендації стандартів інформаційної безпеки, визначити перелік контролів;
- розробити рекомендації щодо проведення аудиту кіберстійкості та використання запропонованого переліку контролів;
- для переліку контролів кіберстійкості визначити тип контролю;
- розробити рекомендації оцінювання ефективності контролів аудиту;
- для оцінки результатів аудиту, визначити рівні кіберстійкості та відповідні до них критерії;
- розрахувати капітальні витрати на проведення аудиту кіберстійкості та визначити економічну доцільність таких витрат.

1.4 Висновок за першим розділом

У першій частині кваліфікаційної роботи було проведено дослідження підходів до реалізації кіберстійкості організацій. Розглянуто визначення кіберстійкості, її принципів, цілей та об’єктів.

Серед методів досягнення кіберстійкості більш детально було розглянуто: відповідність стандартам, я саме GDPR; DPIA, PCI DSS; та аудит.

Було розглянуто та досліджено вимоги та стандарти щодо IT аудиту. А саме: ERM COSO, CoBiT від ISACA, AS PCAOB, NIST SP 800 53 та ISO 27001.

Описані основні етапи аудиту та підходи до його реалізації та планування.

Поставлені задачі для подальшої роботи за темою.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Контролі ризик-орієнтовного аудиту кіберстійкості

Для проведення аудиту кіберстійкості пропонується набір контролів представлених у таблиці 2.1. Всі 98 контролів умовно поділені на 7 груп:

1. Організація інформаційної безпеки;
2. Управління активами;
3. Керування доступом;
4. Аудит, моніторинг та управління інцидентами;
5. Фізична безпека та безпека середовища;
6. Безпека та цілісність операцій, систем, мереж та інформації;
7. Відносини з постачальниками послуг.

Список контролів для аудиту кіберстійкості сформовано спираючись на рекомендації стандартів інформаційної безпеки ISO/IEC 27001[80] та NIST SP 800-53[28] та принципи кіберстійкості, які були розглянуті у першому розділі роботи. У подальшому для більш чіткого розуміння та опису проведення процедур аудиту рекомендуємо використовувати відповідні контролі з вказаних вище джерелах.

На етапі планування, відповідно до особливостей організації, аудит кіберстійкості якої проводиться, ті чи інші контролі або навіть група контролів можуть бути вилучені з плану. Це допоможе уникнути виконання зайвої роботи та заощадить час. Наприклад, якщо організація використовує хмарові сховища, або послуги оренди серверів у постачальників послуг, то майже вся група контролів – «Фізична безпека та безпека середовища», буде не актуальною. Однак, у такому випадку слід приділити значну увагу групі контролів «Відносини з постачальниками послуг».

Також у списку зустрічаються досить загальні контролі, які потребують подальшої конкретизації, наприклад: «Контролі мережі». Визначення, які саме контролі мережі будуть актуальні для аудиту організації, слід визначити виходячи

з особливостей побудування, використання та обслуговування мережі та оцінки і аналізу ризиків, що передує аудиту. Дана задача покладається на професійне судження спеціаліста з аудиту, та аналізу ризиків. Аналогічна стратегія конкретизації контролів застосовна для усіх загальних контролів у переліку таблиці 2.1. Для спеціалістів аудиту, рекомендуємо аргументовано описувати чому ті чи іншу контролі є не актуальними у конкретному випадку.

Окрім того, контролі також визначені за типами дії яку вони спричиняють. Типи контролів, що використовуються у таблиці 2.1:

- стримування – міри, що знеохочують потенційного зловмисника відтворювати атаки, вселяючи сумнів чи страх перед наслідками, а робітників заохочує більш обережно ставитися до безпеки інформаційних систем з тієї ж причини;
- уникнення – міри направлені на усунення вже відомих вразливих місць уникнення створенню нових слабкостей;
- запобігання – захист інформаційних активів від ймовірних небезпечних подій, перш ніж вони відбудуся;
- виявлення – контроль допомагає ідентифікувати небезпечну подію чи інцидент кібербезпеки якомога швидше, задля мінімізації їх впливу на системи та бізнес процеси;
- реагування – контроль допомагає мінімізувати вплив кібер-інцидентів, швидко та ефективно реагувати та протидіяти ним.
- відновлення – відновлення пошкоджених технічних або інформаційних ресурсів до нормального функціонування.

Така класифікація контролів застосована для подальшого визначення рівня кіберстійкості організації, за результатами аудиту.

Таблиця 2.1 – Контролі для аудиту кіберстійкості

Назва контролю	Типи контролів					
	Стримування	Уникнення	Запобігання	Виявлення	Реагування	Відновлення
Організація інформаційної безпеки						
Політики інформаційної безпеки	+	+	+	-	+	+
Періодичний перегляд політик інформаційної безпеки на актуальність	+	+	+	-	+	+
Визначені та затверджені ролі та обов'язки щодо інформаційної безпеки	+	+	+	-	-	-
У ІТ та ІБ процедурах виконується принцип розподілу обов'язків	+	+	+	-	-	-
Наявність регулярних тренінги та навчання персоналу щодо інформаційної безпеки	+	+	+	+	+	-
Використання принципів інформаційної безпеки в управлінні проектами	-	+	+	-	-	-
Управління активами						
Інвентаризація активів	-	+	+	-	-	+
Затверджені відповідальні власники активів	-	+	+	+	+	+
Визначено допустиме використання активів	-	+	+	-	-	-
Відновлення активів	+	+	-	-	-	-
Визначена класифікація інформації	-	+	-	-	-	-
Виконується позначення файлів в залежності від типу інформації	+	-	+	+	-	-
Використання та зберігання активів	+	-	+	+	-	-

Продовження таблиці 2.1.

Управління знімними носіями інформації	+	+	+	-	-	-
Утилізація фізичних носіїв інформації	-	+	+	-	-	-
Передача фізичних носіїв інформації	-	+	+	-	-	-
Керування доступом						
Політики контролю доступу	+	-	+	-	-	-
Доступ до мереж та мережевих сервісів	-	+	+	-	-	-
Створення та видалення облікових записів користувачів	+	+	-	-	-	-
Надання доступу користувачам	-	+	+	-	-	-
Управління привілейованими правами доступу	-	+	+	-	-	-
Перегляд прав доступу користувачів	+	-	+	+	-	-
Видалення або коригування прав доступу	-	+	+	-	-	-
Процедури безпечного входу у системи те сервіси	+	+	+	-	-	-
Використання службових програм привілейованого доступу	-	-	+	-	-	-
Контроль доступу до вихідного коду програм	-	+	+	-	-	-
Обмеження часу сесії користувача	-	-	+	-	-	-
Аудит, моніторинг та управління інцидентами						
Журнал подій	+	-	-	+	+	-
Захист файлів журналів подій	+	+	+	-	-	-
Журнали дій адміністраторів та операторів	+	-	-	+	-	-
Моніторинг процесів ведення журналів подій та системного аудиту	+	+	+	-	-	-

Продовження таблиці 2.1.

Реагування на помилки процесів ведення журналів подій та системного аудиту	-	+	+	-	-	-
Обов'язки та процедури реагування на інциденті ІТ та ІБ	-	-	-	-	+	+
Контроль аудиту інформаційних систем	+	-	-	+	-	-
Звітування про події інформаційної безпеки	-	-	-	+	+	-
Звітування про слабкі місця інформаційної безпеки	+	-	-	+	-	-
Оцінка та прийняття рішення щодо подій інформаційної безпеки	-	-	-	+	+	-
Реагування на інциденти інформаційної безпеки	-	-	-	-	+	+
Внесення відповідних заходів після інцидентів кібербезпеки	-	+	-	-	-	+
Зберігання доказів	+	-	+	-	+	-
Фізична безпека та безпека середовища						
Периметр фізичної безпеки	+	+	+	-	-	-
Контроль фізичного доступу	+	+	+	+	-	-
Безпека офісів, серверних кімнат та інших приміщень	+	+	+	+	-	-
Захист від зовнішнього впливу погодних умов та стихійних лих	-	+	+	-	-	-
Стабільне забезпечення комунальних потреб	-	+	+	-	+	+
Розташування та захист технічного обладнання	-	+	+	+	-	-
Безпека кабелів	-	-	+	-	-	-

Продовження таблиці 2.1.

Обслуговування обладнання	-	+	+	+	-	-
Вилучення активів	+	+	+	+	-	-
Безпека обладнання та майна поза приміщеннями	-	+	-	-	-	-
Контроль технічних вразливостей	-	+	-	-	-	-
Моніторинг фізичних активів	+	-	-	+	-	+
Безпека та цілісність операцій, систем, мереж та інформації						
Документовані операційні процедури	-	+	+	-	+	+
Управління змінами	+	+	+	-	-	-
Управління потужностями	-	+	-	-	-	-
Поділ середовищ розробки, тестування та експлуатації	+	+	+	-	-	-
Контроль проти зловмисних програм	+	-	+	+	+	+
Встановлення програмного забезпечення у середовище операційної системи	-	+	+	-	-	-
Політика та процедури передачі інформації	-	+	+	-	-	-
Тестування безпеки системи	-	+	+	-	-	-
Електронні листування	+	-	+	-	-	-
Перевірка функцій забезпечення безпеки інформації	-	+	+	+	-	+
Мінімально необхідні строки зберігання інформації	-	-	+	-	-	+
Альтернативні способи збереження інформації	-	-	+	-	-	+
Перевірка інформації що вноситься у системи	+	-	+	+	-	-

Продовження таблиці 2.1.

Фрагментація інформації	-	+	+	+	-	+
Резервне копіювання інформації	-	+	+	-	-	+
Аналіз та специфікація вимог до інформаційної безпеки	-	+	-	-	-	-
Захист споміжних програмних додатків у загальнодоступних мережах	+	+	+	-	-	-
Захист транзакцій програмних додатків	+	+	+	-	-	-
Політика безпечної програмної розробки	+	-	+	-	-	-
Процедури контролю системних змін	-	+	-	-	-	-
Технічний огляд програм після змін операційної платформи	-	-	-	+	-	-
Принципи безпечної системної інженерії	-	+	+	-	-	-
Безпечне середовище розробки	-	+	+	-	-	-
Захист системи та мережі від аналізу даних	-	+	+	-	-	-
Контролі мережі	-	-	+	-	-	-
Безпека мережевих сервісів	-	+	+	+	-	-
Сегментування мережі	+	-	+	-	-	-
Захист пам’яті технічного обладнання	-	-	+	-	-	+
Костумізовані допрацівання критичних компонентів	-	+	+	-	-	-
Програма інформованості про загрози (співробітництво з іншими компаніями)	-	-	+	-	-	-
Розділення функціональності системи та користувача	+	+	+	-	-	-
Ізоляція функцій кібербезпеки	-	+	+	-	-	-

Продовження таблиці 2.1.

Перевірка цілісності(не змінності даних)	-	-	+	+	-	-
Відносини з постачальниками послуг						
Інформаційна безпека у відносинах з постачальниками послуг	+	+	+	-	-	-
Вирішення питань безпеки в рамках угод з постачальниками послуг	+	+	+	+	+	+
Ланцюг постачання інформаційно-комунікаційних технологій	+	+	+	-	-	-
Моніторинг та огляд послуг постачальників	-	-	-	+	-	-
Управління змінами в послугах постачальників	-	+	+	-	-	-
Обов'язки та процедури у відносинах постачальниками послуг	-	-	-	-	+	+
Реагування на інциденти кібербезпеки зі сторони постачальників послуг	+	-	-	-	+	-
Курування доступу постачальників послуг	+	-	+	+	-	-
Розробки програмного забезпечення третіми сторонами	+	+	+	-	-	-
Управління безперервністю бізнесу						
Планування безперервності інформаційної безпеки	-	-	-	-	+	+
Впровадження безперервності інформаційної безпеки	-	-	-	-	-	+
Наявність засобів обробки інформації	-	+	+	-	+	+
Визначення чинного законодавства та контрактних вимог	-	-	+	-	-	-

2.2 Критерії аудиту та оцінка рівня кіберстійкості

Критерії, пов'язані зі здатністю системи задовольняти вимоги, можуть виражатися кількісними показниками (тобто метриками та пороговими значеннями), якісними показниками (включаючи межі порогових значень) або категоріями визначених форм доказів. Критерії кіберстійкості - це критерії щодо того, наскільки архітектура чи дизайн системи або елемента системи відповідає обраним принципам проектування кіберстійкості; чи в якій мірі архітектура, дизайн або реалізація включає обрані методики або підходи до кіберстійкості чи в якій мірі можна очікувати, що архітектура, дизайн або реалізація дозволять досягти обраних цілей щодо кіберстійкості; як і в якій мірі архітектура, дизайн або реалізація управляє ризиком або впливає на діяльність зловмисника; або як і в якій мірі архітектура, дизайн або реалізація дозволяють досягти місії чи бізнес-цілей в умовах зловмисного впливу або збоїв IT систем. Подібно до критеріїв безпеки, критерії кіберстійкості можуть бути виражені кількісно або якісно[95].

2.2.1 Оцінка ефективності контролів

Далі цим розділом буде описана рекомендована модель для оцінки ступенів ефективності контролів кіберстійкості перелічених у таблиці 2.1.

У списку запропонованих вище контролів, за об'єктом тестування, можна виділити такі типи:

- огляд документації;
- перевірка процедур.

Для визначення повноти нормативної документації організації, іншими словами, визначення ступеню виконання контролю пропонуємо використовувати наступні пункти.

1. Документ передивляється на предмет актуальності та оновлюється:

a. раз на рік, або частіше за планом та позапланово у разі необхідності, у випадку вагомих змін по відношенні до системи або процедури що описується у документі – додається 2 бал;

b. рідше ніж раз на рік, але не рідше ніж раз на 4 роки за планом та позапланово за необхідністю – додається 1 бал;

c. тільки за необхідності - бали не додаються та не віднімаються;

d. віднімiть 3 бали якщо документу немає або він не актуальний.

2. Додайте ще 1 бал, якщо документ затверджується керівництвом організації і/або керівниками відповідних відділів.

3. Відповідно до того наскільки детально описані вимоги налаштувань, відповідальні особи, алгоритм виконання процесів дорахуйте від одного до 4 балів. Для прикладу розподілення балів використаємо приклад з політикою управління змінами де:

a. 1 бал – процедура описана мінімально, на рівні: «Кожне внесена у систему зміна повинна тестуватися та затверджуватися менеджментом»;

b. 2 бали – наводиться загальний опис алгоритму дій, кожного етапу окремо, але без конкретних деталей;

c. 3 бали – до описів етапів та загального опису додаються уточнення, як то визначені відповідальні особи за посадами;

d. 4 бали – у документі розглядаються різні види змін, схематично або тестом описані етапи для кожного виду, включаючи деталі з конкретними показниками або описом, наприклад: визначені відповідальні особи, кожного етапу процедури, вказані конкретні посади, імена та методи зв’язку, альтернативні відповідальні, є приклад як повинен виглядати звіт або інцидент за проведеною дією, має додаткові інструкції тощо.

4. Якщо документ суперечить іншому прийнятому у організації документу віднімiть 2 бали.

5. В залежності від ознайомленості робітників на яких розповсюджується документ додайте або віднімітe 1 бал де:

a. 1 бал віднімається, якщо робітники не знають про існування відповідного документу, не знають де на нього можна подивитися та про що йдеться у документі;

b. 1 бал додається якщо, робітники після кожного оновлення документу ознайомлюються з ним, знають де можна з ним ознайомитися, знають загальні і основні вимоги описані у ньому;

c. бали не додаються та не віднімаються у випадку якщо робітники знають про існування певного документу, знають де з ним ознайомитися, але не переглядають документ після оновлень, якщо на це немає необхідності, та не знають основних вимог описаних у ньому.

Для контролів що перевіряють процедури:

1. Додайте 1 бал, якщо для процедури, що перевіряється існує документована інструкція, алгоритм, методологія, політика тощо.

2. Відповідно до ступенів відповідності виконання процедур до документів додайте бали де:

a. 3 бали - повна відповідність налаштувань, звітів або інших доказів до о детально описаного документу;

b. 2 бали – більшість доказів повністю відповідають до детально описаного документу, але є декілька випадків відхилення, причини відхилення можливо з’ясувати і вони адекватно пояснюють відхилення, та ступень відхилення незначна і не становиться причиною виникнення потенційних ризиків, або одиничні серйозні відхилення, але для яких були проведені відповідні дії для зменшення потенційних ризиків;

c. 1 бал - більшість доказів повністю відповідають до детально або загально описаного документу, але є декілька випадків відхилення, причини відхилення не можливо з’ясувати, ступень відхилення незначна і не становиться

причиною виникнення потенційних ризиків, або одиничні серйозні відхилення, але для яких були проведені відповідні дії для зменшення потенційних ризиків;

d. 1 чи більше балів віднімається - у випадку коли є випадки відхилення, причини відхилення не можливо з'ясувати, для серйозних відхилень не були проведені відповідні дії для зменшення потенційних ризиків;

3. Додайте 1 бал, якщо усі або більшість робітників задіяних у процедурі мають відповідну до своїх обов'язків кваліфікацію.

4. Відповідно до актуальності існуючої процедури:

a. віднімiть 3 бали, якщо процедура не повна, потребує додаткових етапів підтвердження, документації, перевірки, тощо, або зміну підходу до її виконання, у тому виді в якому вона існує зараз вона не ефективна;

b. віднімiть 1 бал, якщо процедура потребує незначних коректив або покращень;

c. додайте 2 бали, якщо процедура впевнено покриває основні потреби моніторингу, розподілу обов'язків, відновлення та охоплює очікувані об'єми ресурсів, користувачів тощо;

5. Відповідно до того чи залишає процедура документаційний слід:

a. додайте 1 бал, якщо за допомогою документації, електронних запитів, тощо, можна детально відновити подію, зафіксовані, дати та час, задіяні особи, результати та висновки, тощо;

b. віднімiть 1 бал, якщо документаційний сліду процедури не повний, не має очевидного опису, результату, задіяної особи дати, тощо;

c. віднімiть 2 бали, якщо процедура не залишає неяких документаційних доказів.

Відповідно до наведених вище критеріїв формується оцінка контролю, яка складається з накопичених балів і не може перевищувати значення 8.

Для оцінки ефективності контролів пропонується модель із трьох ступенів: мінімальний(до 3 балів), середній(4-6 балів) та максимальній ступень повноти(7-8 балів). Крім того, контроль може бути визначений як не ефективний.

Спираючись на професійне судження та конкретну специфіку організації для якої проводиться аудит кіберстійкості, аудитор може додавати свої додаткові критерії оцінювання контролів, або модифікувати запропоновані. У такому разі розподілення чисельних показників оцінок контролів за ступенями ефективності контролів також може бути змінено.

2.2.2 Визначення ступеню ефективності контролів за категоріями

До кожного запропонованого для аудиту кіберстійкості контролю у таблиці 2.1, наведено відповідну категорію. Більшість контролів відносяться до більше ніж однієї категорії. Якщо контроль відноситься до двох типів, вин буде враховуватися Для визначення ступеню повноти категорії контролів слід враховувати ступені повноти кожного контролю який відносить до категорії та обраний для аудиту. Пропонується використовувати саме значення ступенів: мінімальний, середній та максимальний, а не чисельних показників.

Максимальним рівень ефективності контролів за певним типом рекомендується визначати у ситуації коли жоден контроль, що відноситься до цього типу не оцінений, як низького ступеня ефективності або не ефективний та хоча би половина контролів оцінені, як контролі максимальної ефективності.

Середній рівень ефективності контролів за певним типом визначається, якщо не більше 10% контролів, що відносяться до цього типу визначені, як контролі мінімальної ефективності або не ефективні.

Мінімальній рівень ефективності контролів за певним типом рекомендується визначати коли більшість контролів оцінено мінімальним ступенем ефективності, але не більше 10% контролів визначені як не ефективні.

2.2.3 Градація рівнів кіберстійкості

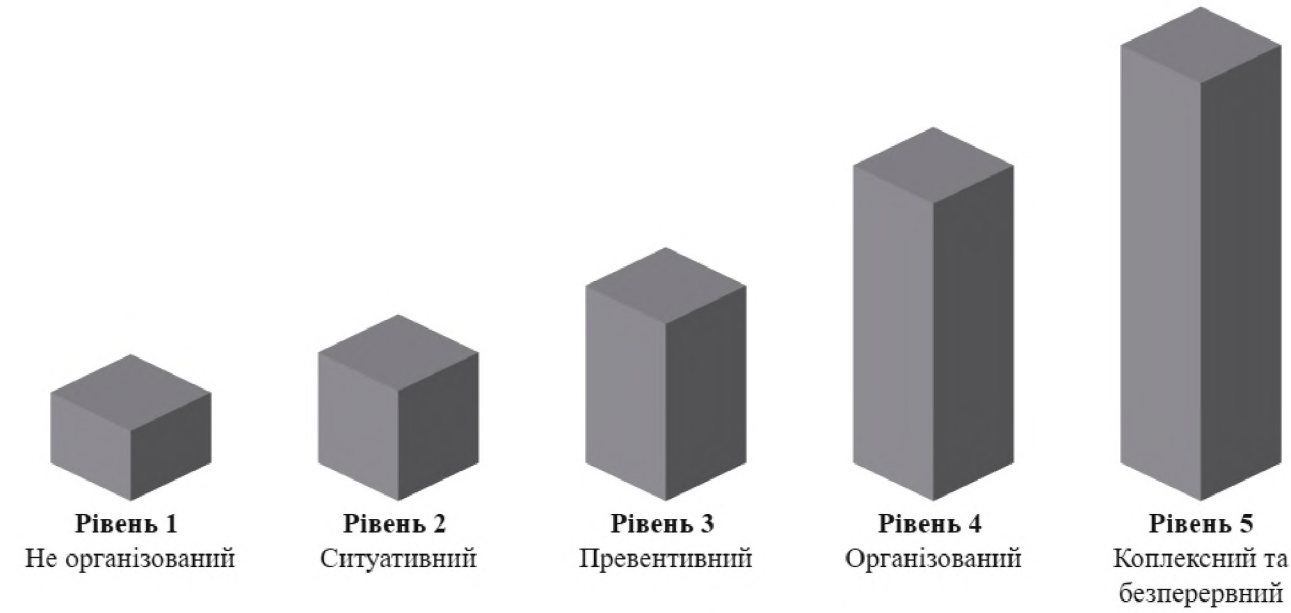

Рисунок 2.1 – Градація рівнів кіберстійкості

За результатами аудиту пропонується оцінити загальний рівень стійкості в організації. Виділені 5 рівнів кіберстійкості з необхідними для них показниками контролів за типами:

1 Не організований. Цей рівень фактично можна назвати нульовим, бо як такої кіберстійкості на ньому не існує у рамках IT систем компанії. Все, що буде нижче показників рівнів описаних далі за тестом потрапляє під цю категорію.

2 Ситуативний. На цьому рівні організація використовує ситуаційний підхід до підтримки роботи бізнес процесів організації. Проблеми із забезпеченням бізнесу вирішуються у міру їх надходження. Очікувані ступені ефективності контролів за типами: Відновлення: середній; Реагування: середній; Виявлення: мінімальний; Уникнення: мінімальний; Запобігання: мінімальний; Стримування: мінімальний.

3 Превентивний. Компанія готова реагувати на кіберподії, що вже сталися та намагається попереджувати потенційні. Відновлення: середній;

Реагування: середній; Виявлення: середній; Уникнення: середній; Запобігання: середній; Стримування: середній.

4 Організований. На цьому рівні організація знає свої вади, щодо кіберподій, та застосовує комплексне рішення щодо їх усунення. Очікувані рівні контролів за типами: Відновлення максимальний; Реагування: максимальний; Виявлення: максимальний; Уникнення: максимальний; Запобігання: середній; Стримування: середній.

5 Комплексний та безперервний. Даний рівень описує кіберстійкість організації як налагоджену систему, що перебуває у стані постійного балансування. Враховуються усі аспекти кіберстійкості. Налагоджені процедури: моніторингу, відновлення, реагування на кіберподії. Прийняті превентивні міри задля уникнення можливих зловмисних дій та збоїв. Забезпечується максимально безперервність роботи бізнес процесів. На даному рівні, ми очікуємо бачити контролі всіх типів на максимальному рівні. Однак, навіть якщо за результатами аудиту IT системи та процеси відповідають найвищому рівню, за представленою градацією це не означає, що організація досягла ідеалу кіберстійкості, та встоїть перед будь-якими кіберподіями та збоями та може забути про розвиток цього направлення. Бізнес і технології завжди розвиваються і обидва ці фактори будуть потребувати змін у IT середовищі, що в свою чергу призведе до корекцій структури і буде вимагати оновлення та актуалізації вже існуючих заходів кіберстійкості.

2.3 Висновок за другим розділом

У другому розділі кваліфікаційної роботи у виді таблиці, було наведено лист контролів для проведення ризик-орієнтованого аудиту кіберстійкості організації. Було надано опис принципу відбору контролів та використані міжнародні стандарти-джерела. До цього списку було визначено умовні групи контролів за

темою. До кожного контролю визначено категорії за принципом дії. Ці категорії у подальшому будуть використані для оцінки кіберстійкості.

Також у другому розділі надані рекомендації щодо планування аудиту кіберстійкості за допомогою запропонованого списку контролів. Надані рекомендації щодо розуміння процедур аудиту та перелічені джерела до яких можна звернутися за уточненнями.

Розроблена модель оцінки ефективності контролів. Цей підхід також використовується у розробленій методології оцінки кіберстійкості організації цвілому. Запропонована модель градації рівнів кіберстійкості та опис до кожного з них. Надано рекомендації щодо прийняття рішень про оцінку ефективності контролів аудиту та кіберстійкості організації.

РОЗДІЛ 3. ЕКОНОМІКА

3.1 Вступ до економічної частини

Метою даного економічного розділу є розрахунок економічної ефективності проведення ризик-орієнтовного аудиту кіберстійкості організації порівняно із проведенням повного аудиту інформаційної безпеки за американським стандартом NIST 800-53.

Для визначення економічної ефективності типового аудиту, що розглядається у даній роботі було обрано порівняння саме з аудитом за документом NIST 800-53 за такими причинами:

- обраний стандарт має досить детальний опис і не потребує додаткових допрацювань контролів зі сторони аудитора;
- документ з повним переліком контролів, процедур та описом методології розповсюджується безкоштовно, та не потребує додаткових витрат на оплату ліцензії.

Для визначення описаної вище ефективності необхідно розрахувати:

1. Вартість проведення внутрішнього аудиту ризик-орієнтовного аудиту кіберстійкості;
2. Вартість проведення внутрішнього аудиту за стандартом NIST 800-53;
3. Визначення економічного ефекту від проведення аудиту та подальших удосконалень, на шляху до кіберстійкості організації;
4. Порівняти отримані результати і визначити економічно вигідніший варіант проведення аудиту з наміром підвищення кіберстійкості організації.

Розрахунок експлуатаційних витрат на проведення аудиту не потребує розрахування. Частота проведення зовнішнього або внутрішнього аудиту визначається потребами організації, керівництвом організації та/або відділів ІТ та ІБ. Кожне окреме проведення аудиту буде потребувати нових капітальних витрат.

Отже далі у розрахунках значення С – щорічні витрати на експлуатацію – не враховується.

3.2 Визначення трудомісткості проведення ризик-орієнтовного аудиту кіберстійкості

Трудомісткість проведення ризик-орієнтовного аудиту кіберстійкості кваліфікованими співробітниками відділу внутрішнього ІТ аудиту компанії, починаючи з планування аудиту і закінчуючи оформленням документації, формуванням звіту з рекомендаціями та обговоренням отриманих результатів з керівництвом та відділами ІБ та ІТ:

$$t=t_{па}+t_{зі}\times k+t_{ад}\times k+t_{ср}\times k+t_{пз}\times k+t_{ор}\times k=$$

$$=30+10\times 98+8\times 98+4\times 98+0{,}1\times 98+0{,}25\times 98=2220{,}3\text{люд./годин},$$

(3.1)

де k =98 – кількість контролів ризик-орієнтовного аудиту кіберстійкості;

$t_{па}$=30 – тривалість планування аудиту, люд./години;

$t_{зі}$=10 – середня тривалість збору інформації для одного контролю, люд./годин;

$t_{ад}$=8 – середня тривалість аналізу отриманих даних та документування одного контролю, люд./години;

$t_{ср}$ =4 – середня тривалість складання рекомендацій для одного контролю, люд./годин;

$t_{пз}$ =0,1 – середня тривалість підготовки аудиторського звіту та підготовку до обговорення результатів аудиту і відповідних рекомендацій для одного контролю, люд./годин;

$t_{ор}$ =0,25 – середня тривалість обговорення результатів з керівництвом, ІТ та ІБ відділами організації, одного контролю та рекомендацій за ним, люд./годин.

Розрахунки часу виконані за умов, що:

- над аудитом працює один спеціаліст;

- організація - об’єкт аудиту, охоплює декілька сфер діяльності і має широко розвинену структурі ІТ та ІБ так що усі контролі аудиту актуальні;
- рекомендації, за результатами проведення аудиту будуть надано до кожного трестованого контролю приблизно в однаковому обсязі;
- на аналіз та документування одного контролю витрачається в середньому 8 годин;
- на збір інформації за одним контролем витрачається в середньому 10 годин;
- на складання рекомендацій за результатами аудиту, спеціаліст витрачає в середньому 4 година на один контроль;
- на обговорення результатів з керівництвом, ІТ та ІБ відділами організації, одного контролю та рекомендацій за ним витрачається в середньому 15 хвилин;
- на формування звіту та підготовку до обговорення результатів аудиту і відповідних рекомендацій аудитор витрачає в середньому 4 хвилини на один контроль.

Витрати на проведення ризик-орієнтовного аудиту кіберстійкості складаються з витрат на заробітну плату виконавця аудиту $З_{зп}$, вартості витрат машинного часу, що необхідний для опрацювання даних аудиту на ПК $З_{мч}$:

$$К_{аіб}=З_{зп}+З_{мч}=488466+4951,27=493417.27грн,$$

(3.2)

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування єдиного соціального внеску (22%) і визначається за формулою:

$$З_{зп}=З_{пр}\times t=220\times 2220,3=488466грн,$$

(3.3)

де t=2220,3 – загальна тривалість проведення ризик-орієнтовного аудиту кіберстійкості, годин;

$З_{пр}$=220 – середня заробітна плата спеціаліста з нарахуваннями, грн/годину.

Вартість машинного часу для обробки зібраної інформації на ПК спеціаліста з аудиту визначається за формулою:

$$З_{мч}=t\times С_{мч}=2220,3\times 2,23 =4951,27грн,$$

(3.4)

де t=2220,3 – трудомісткість підготовки документації на ПК, годин (розрахована за формулою 3.1);

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість однієї години машинного часу ПК визначається за формулою:

$$С_{мч}=Р\times С_е+\frac{Ф_{зал}\times Н_а}{F_р}=0,55\times 1,68+\frac{5000\times 0,5}{1920}=2,23грн,$$

(3.5)

де Р=0,55 – встановлена потужність ПК, кВт;

$С_е$=1,68 – тариф на електричну енергію(з урахуванням ПДВ), грн/кВт×година[79];

$Ф_{зал}$=5000 – залишкова вартість ПК на поточний рік, грн.;

$Н_а$=0,5 – річна норма амортизації на ПК, частки одиниці;

$F_р$=1920 – річний фонд робочого часу (за умови 40-годинного робочого тижня $F_р$=1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації, як різниця між первісною вартістю та зносом за час використання.

Розрахунки вартості аудиту проведено за умов, що:

- організація відмовилась від паперової документації і не потребує урахування витрат на роздрукування звітів, тощо;
- ліцензовані програмні продукті, що використовуються у процесі проведення, документування та обговорення аудиту (Microsoft Word, Excel,

PowerPoint ті інші) оплачуються організацією на всіх працівників, у тому числі і на спеціаліста з аудиту інформаційних технологій, в не залежності від того, чи проводиться аудит чи ні, тому врахування витрат на ліцензії програмного забезпечення не потребується.

З проведених вище розрахунків отримуємо вартість одноразового проведення ризик-орієнтовного аудиту кібербезпеки $К_{аіб}$=493417.27грн.

3.3 Визначення трудомісткості проведення аудиту інформаційної безпеки за стандартом кіберстійкості

Для розрахунків трудомісткість та вартості проведення аудиту за процедурами NIST 800-53 використовувались ті ж самі формули, що і для розрахунку аналогічних показників ризик-орієнтованого аудиту кіберстійкості. Усі умови розрахунків і значення аналогічні, окрім значення k=322 – кількість контролів за NIST 800-53[28].

Використовуючи нове значення k отримуємо такі розрахунки:

t=7226,7 - загальна тривалість проведення аудиту за переліком контролів NIST 800-53, годин (розраховано за формулою 3.1);

$З_{мч}$=16115,54 - вартість машинного часу для обробки зібраної інформації на ПК спеціаліста з аудиту, грн. (розраховано за формулою 3.4);

$З_{зп}$=1589874 - заробітна плата виконавця (з урахуванням основної та додаткову заробітну плату, а також відрахування єдиного соціального внеску (22%)), грн. (розраховано за формулою 3.3);

$К_{аіб}$=1605989,54 - повна сума витрат за одноразове проведення аудиту за переліком контролів NIST 800-53, грн. (розраховано за формулою 3.2).

3.4 Оцінка можливих збитків від кіберінцидентів та ІТ збоїв

Для визначення можливих збитків від кіберінцидентів за рік, буде використана статистика опитування Hiscox для їх щорічного звіту, щодо кіберстійкості[91]. Інформацію для формування звіту 2020 року надали 1971

компаній різного масштабу зі Сполучених Штатів Америки, Іспанії, Бельгії, Германії, Франції та інших країн Європи. Вибірку для формування статистики звіту вважаємо достатньо повною, щоби спиратися на її результати.

Тож за показниками Hiscox, середні збитки від кіберінцидентів для компанії у 2020 році становить 57 тисяч доларів США, майже 1,6 мільйонів гривень. Беручи до уваги минулорічні показники, де середня вартість збитків складала 10 тисяч доларів США, будь-яка не запланована та не стандартна ситуація, як всесвітній карантин 2020 року в рази збільшують збитки через інциденти кібербезпеки (рисунок 5 у додатку С). До того ж через всесвітньої пандемії залежність бізнесу від ІТ технологій значно збільшилася[62]. Більше того, для великомасштабної організації, що охоплює декілька сфер діяльності, і складається з понад 1000 співробітників, середні збитки через кіберінциденти та технічні і системні збої складають 504 тисячі доларів США, що складає більше 14ти мільйонів гривень. За результатами того ж опиту Hiscox, більше половини всіх підприємств, що мають понад 1000 працівників, а саме 51%, - заявили, що мали принаймні один кіберінцидент. Вони також повідомили про найбільшу кількість кібер-інцидентів (медіана 100) і збоїв (80).

Отже петиційні річні збитки через кіберінциденти та ІТ збої становлять:

$$E=B\times R=14033000\times 0,51=7156830\text{грн.},$$

(3.6)

де B=14033000 – загальний збиток від кіберінцидентів та ІТ збоїв за рік, грн;

R=0,51 – очікувана імовірність реалізації кібератак ті/або виникнення збоїв ІТ, частки одиниці.

3.5 Висновки до економічної частини

В економічному розділі наведено обґрунтування економічної доцільності проведення ризик-орієнтовного аудиту кібербезпеки. Були виконані розрахунки повної вартості одноразового проведення ризик-орієнтовного аудиту

кіберстійкості та аудиту безпеки IT за процедурами NIST 800-53. Капітальні становлять приблизно 493417,27грн та 1605989,54грн, відповідно. Порівнюючи отримані результати робимо висновки, що перший варіант аудиту буде коштувати організації на 30% ніж другий.

Для порівняння економічної ефективності обох варіантів аудиту знайдемо коефіцієнти ROSI для обох:

$$ROSI=\frac{E}{K}=\frac{7156830}{493417}=14,5, \text{ частки одиниці,}$$

(3.7)

де E=7156830 - петиційні річні збитки через кібер-інциденти та IT збої, грн;

K=493417,27 та 1605989,54 – капітальні витрати на аудит кібербезпеки та аудит за NIST 800-53 відповідно, грн. (розраховано за формулою 3.2).

Отже, значення коефіцієнту ROSI для аудиту кіберстійкості запропонованого у роботі становить 14,5 частки одиниці, а для аудиту за NIST 800-53 – 4,45 частки одиниці.

Визначимо доцільність подібних витрат для компанії. При допущені, що компанія буде здійснювати фінансування капітальних інвестицій для аудиту за рахунок реінвестування власних коштів (частини прибутку та амортизаціях відрахувань), то в якості значення E_H приймаємо бажану норму прибутковості альтернативних варіантів вкладення коштів K з урахування інфляції:

$$E_H=\frac{N_{деп}-N_{інф}}{100}=\frac{9,5-4,1}{100}=0,054, \text{ частки одиниці,}$$

(3.8)

де $N_{деп}$=9,5 – річна депозитна ставка, %[63];

$N_{інф}$=4,1 - річний рівень інфляції, %[64].

Витрати на проведення аудиту будуть вважатися доцільними, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI>E_H$$

(3.9)

де ROSI=14,5 та 4,45– коефіцієнт повернення інвестицій для аудиті за проектом запропонованим у роботі та за NIST 800-53, відповідно, частки одиниці;

E_H= – бажаний показник ефективності, частки одиниці.

Отже нерівність 3.9 виконується для обох варіантів аудиту і їх можна вважати економічно ефективними та доцільними. Однак, у розрахунках не передбачаються потенційні витрати на реалізацію рекомендацій аудиту, які вплинули би на коефіцієнти ROSI зменшивши його в два-чотири рази. Але навіть при таких розрахунках, обидва варіанти аудиту зберігають за свою економічну доцільність.

Розрахуємо також термін окупності капітальних внесків для обох варіантів аудиту:

$$T_o=\frac{1}{ROSI}=\frac{1}{14,5}=0,06\text{року}, \quad (3.10)$$

де ROSI=14,5 та 4,45– коефіцієнт повернення інвестицій для аудиті за проектом запропонованим у роботі та за NIST 800-53, відповідно, частки одиниці.

Таким чином отримуємо термін окупності для аудиту кіберстійкості менше ніж місяць та для аудиту за NIST 800-53 – два з половиною місяці.

Також для обох варіантів аудиту, проведені розрахунки не враховують людино/години працівників та керівників ІТ, ІБ та інших відділів організації задіяних у зборі свідоцтва та інформації для проведення аудиту, а також обговоренні результатів аудиту та рекомендацій. Не врахована вартість машинного часу для персональних комп'ютерів та інших електронних пристроїв задіяних у процесі аудиту (сканери, проектори, тощо).

Таким чином, для зменшення грошових витрат рекомендується використовувати саме запропонований перелік контролів для аудиту, що проводиться з метою вдосконалення кіберстійкості організації. Адже його вартість

менша, а різниця коефіцієнта ROSI та E_H у рази більша, що дає запаси грошових ресурсів на реалізацію рекомендацій по підвищенню рівня кіберстійкості організації за результатами аудиту.

ВИСНОВКИ

Під час виконання даної кваліфікаційної роботи було проаналізовано основні принципи та методи досягнення кіберстійкості, основні етапи IT аудиту та підходи до його виконання. Були розглянуті та порівняні існуючі міжнародні стандарти з рекомендаціями, щодо проведення аудиту інформаційних технологій та безпеки.

В спеціальній частині були розроблені рекомендації щодо проведення аудиту кіберстійкості бізнес організацій. Було запропоновано перелік контролів аудиту і модель оцінки їх ефективності. Також розроблено модель оцінки загальної кіберстійкості організації за результатами аудиту та запропоновані рівні градації кіберстійкості для порівняння результатів.

В економічному розділі розрахована величина капітальних витрат на проведення аудиту кіберстійкості, визначені можливі збитки від реалізації кіберзагроз, обґрунтована економічна ефективність проведення ризик-орієнтовного аудиту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber Resilience – Fundamentals for a Definition, Article in Advances in Intelligent Systems and Computing January 2015, Björck, Fredrik; Henkel, Martin; Stirna, Janis; Zdravkovic, Jelena. URL: https://www.researchgate.net/publication/283102782
2. What are The Essential Audit Approaches? URL: https://www.backoffice.com.my/audit/what-are-the-essential-audit-approaches/
3. IT Auditing – Planning the IT Audit. URL: https://cyberexperts.com/it-audit/
4. The Global Risks Report 2020, Insight Report 15th Edition. URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
5. What is Cyber Resilience? Juliana De Groot, 04.02.2019. URL: https://digitalguardian.com/blog/what-cyber-resilience
6. Нормативний Документ Системи Технічного Захисту Інформації, Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99: Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від "28" квітня 1999р. № 22. URL: https://web.archive.org/web/20121202025850/http://am-soft.ua/files/KSZI/2.5-004-99.pdf
7. Common Criteria. URL: https://www.commoncriteriaportal.org/
8. Common Criteria: an effective deployment, CETIC, J.F. Molderez, Discussion meeting 02/06/2005. URL: https://www.cetic.be/IMG/pdf/GDD0206-v4.pdf
9. Generic verification of security protocols Abdul Sahid Khan, Madhavan Mukund and S. P. Suresh. URL: https://www.cmi.ac.in/~spsuresh/pdfs/spin05.pdf
10. Connecting Cyber Risk Managers to Executives: Understanding Risk Governance and Appetite. URL: https://youtu.be/8kcTZPHrFag

11. Enterprise Risk and Resilience Management URL: https://www.sei.cmu.edu/our-work/enterprise-risk-resilience-management/index.cfm
12. NIST Cybersecurity Framework. URL:https://www.nist.gov/cyberframework
13. ISO 22316 Security and resilience — Organizational resilience — principles and attributes Merrell, S. A., Moore, A. P., & Stevens, J. F. "Goal-based assessment for the cybersecurity of critical infrastructure." IEEE International Conference on Technologies for Homeland Security (HST), cc. 84-88, IEEE, (2010).
14. What is Common Criteria Certification, and Why Is It Important? Katie Moss Jefcoat , 08.12.2017. URL: https://www.blancco.com/blog-what-is-common-criteria-certification-why-is-it-important.
15. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A.: Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), cc.471-476, 2013. URL: https://www.researchgate.net/publication/263176904_Resilience_metrics_for_cyber_systems
16. Bodeau, Deborah, and Richard Graubart, "Cyber Resiliency Engineering Framework", MITRE Report 2011, c.37.
17. Goldman, H., McQuaid, R., & Picciotto, J.: Cyber resilience for mission assurance. In Technologies for Homeland Security (HST), 2011 IEEE International Conference on, pp. 236-241, 2011.
18. Williams, Patricia AH, and Rachel J. Manheke.: Small Business-A Cyber Resilience Vulnerability. Proceedings of the 1st International Cyber Resilience Conference, Research Online, (2010).
19. Joseph, J.: Resilience in UK and French Security Strategy: An Anglo Saxon Bias?. Politics, 33(4), cc. 253-264, (2013).
20. Kaufmann, M: Cyber-resiliens i EU, Internasjonal Politikk, 71(02), cc. 274-282, 2013.

21. ISMS Auditing Guideline ISO The International Standards of Supreme Audit Institutions, or ISSAIs, are issued by INTOSAI, the International Organisation of Supreme Audit Institutions.
22. CYBER EDU, What is Common Criteria? Common Criteria Defined, Explained, and Explored. URL: https://www.forcepoint.com/cyber-edu/common-criteria
23. IT Auditing and Controls – Auditing Organizations, Frameworks and Standards URL: https://resources.infosecinstitute.com/certification/itac-organizations/
24. PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. URL: https://pcaobus.org/oversight/standards/auditing-standards/details/Auditing_Standard_5
25. PCAOB, AS 2201: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. URL: https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201
26. Enterprise Risk Management — Integrated Framework by Committee of Sponsoring Organizations of the Treadway Commission (COSO). URL: https://www.cfo.com/accounting-tax/2006/03/the-trouble-with-coso/
27. Практична Методологія Іт-Аудиту, Гаврилова Л.В., Ян ван Тайнен, Шкуропат О.Г., Манфред ван Кестерен, Герард ван ден Берг, Рудніцька Р.М.,Чорнуцький С.П., Тимохін М.Г., Боровкова Т.В., Любиш-Родченко А.Г., Горбачев С.В. URL: http://dkrs.kmu.gov.ua/kru/doccatalog/document?id=134082
28. NIST, Security and Privacy Controls for Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
29. Enterprise Risk Management (Erm) –Failure Is Not An Option by Robert B. Matthews, Sam Houston State University, Ronald J. Daigle, Sam Houston State University, Paul Vanek, Sam Houston State University

30. Аудит інформаційних систем. URL: http://www.itsway.kiev.ua/index.php?language=ua&main_managemen=services&managemen=audit
31. ISACA, Top Cyberattacks of 2020 and How to Build Cyberresiliency, Frank Downs, 06.11.2020. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency
32. Haes, S.D.; Grembergen, W.V. (2015). "Chapter 5: COBIT as a Framework for Enterprise Governance of IT". Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.). Springer. pp. 103–128. ISBN 9783319145471. Retrieved 24.06.2016. URL: https://books.google.com.ua/books?id=zNgRBwAAQBAJ&pg=PA102&redir_esc=y#v=onepage&q&f=false
33. ISACA, A COBIT Approach to Regulatory Compliance and Defensible Disposal, 01.09.2013. URL: https://www.isaca.org/resources/isaca-journal/past-issues/2013/a-cobit-approach-to-regulatory-compliance-and-defensible-disposal
34. Компанії "Великої четвірки" URL: https://osvita.ua/vnz/add-education/glossary/10674/
35. CFO, PCAOB Revises AS2, Sarah Johnson, 11.09.2006. URL: https://www.cfo.com/accounting-tax/2006/09/pcaob-revises-as2/
36. Where insights lead Cybersecurity and the role of internal audit: An urgent call to action URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf
37. IT Governance, The 4 stages of cyber resilience, Luke Irwin, 30.09.2019. URL: https://www.itgovernance.eu/blog/en/the-4-stages-of-cyber-resilience

38. IT Governance, The EU GDPR (General Data Protection Regulation) – Overview. URL: https://www.itgovernance.eu/en-ie/eu-general-data-protection-regulation-gdpr-ie
39. Regulation (Eu) 2016/679 Of The European Parliament And Of The Council URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
40. General Data Protection Regulation - GDPR URL: https://gdpr-info.eu/
41. General Data Protection Regulation Summary, Robert Mazzoli, 30.11.2020. URL: https://docs.microsoft.com/uk-ua/compliance/regulatory/gdpr
42. Microsoft 365 GDPR action plan — Top priorities for your first 30 days, 90 days, and beyond, Robert Mazzoli, 30.11.2020. URL: https://docs.microsoft.com/uk-ua/compliance/regulatory/gdpr-action-plan
43. Support your GDPR program with Accountability Readiness Checklists, Robert Mazzoli, 30.11.2020. URL: https://docs.microsoft.com/uk-ua/compliance/regulatory/gdpr-arc
44. Lack of GDPR knowledge is a danger and an opportunity, Sean McGrath. URL: https://www.computerweekly.com/microscope/news/2240234469/Lack-of-GDPR-knowledge-is-a-danger-and-an-opportunity
45. Extraterritorial Scope of GDPR: Do Businesses Outside the EU Need to Comply? Imran Ahmad. URL: https://www.americanbar.org/groups/business_law/publications/blt/2018/04/01_speirs/
46. Что вам стоит знать о GDPR, Olga Rusnak URL: https://dou.ua/lenta/articles/what-gdpr-is/
47. GDPR — новые правила обработки персональных данных в Европе для международного IT-рынка, Артем Козлюк. URL: https://habr.com/ru/company/digitalrightscenter/blog/344064/

48. GDPR (Общий регламент про защиту данных) – имитация или compliance? Тарасюк Антон. URL: https://legalitgroup.com/ru/gdpr-obshhij-reglament-pro-zashhitu-dannyh-imitatsiya-ili-compliance/
49. Оценка рисков в рамках GDPR, Дубас Катерина. URL: https://legalitgroup.com/ru/otsenka-riskov-v-ramkah-gdpr/
50. GDPR: Data Protection Impact Assessment и Data Protection Officer, By Дубас Катерина. URL: https://legalitgroup.com/ru/gdpr-data-protection-impact-assessment-i-data-protection-officer/
51. DPIA на практике, Andrey Prozorov. URL: https://www.securitylab.ru/blog/personal/80na20/347261.php
52. GDPR и оценка влияния на защиту данных, Богарада Сергей. URL: https://legalitgroup.com/ru/gdpr-i-otsenki-vliyaniya-na-zashhitu-dannyh/
53. What does the ePrivacy Regulation mean for the online industry? Dr Frank Eickmeier. URL: https://www.eprivacy.eu/en/news/news-detail/article/what-does-the-eprivacy-regulation-mean-for-the-online-industry/
54. Data protection reform: Council adopts position at first reading, Council of the European Union. URL: https://www.consilium.europa.eu/en/press/press-releases/2016/04/08/data-protection-reform-first-reading/#
55. California's New Data Privacy Law Could Begin a Regulatory Disaster, Danny Allan. URL: https://fortune.com/2018/10/23/california-data-privacy-law-gdpr/
56. A Human-centric Perspective on Digital Consenting: The Case of GAFAM, Soheil Human and Florian Cech. URL: https://epub.wu.ac.at/7523/1/HCIS2020_A%20Human-centric%20Perspective%20on%20Digital%20Consenting_The%20Case%20of%20GAFAM_Soheil%20Human_Florian%20Cech.pdf
57. GDPR Reality Check – Claiming and Investigating Personally Identifiable Data from Companies, Fatemeh Alizadeh, Gunnar Stevens, Timo Jakobi, Jens Boldt. URL: https://eusec20.cs.uchicago.edu/eusec20-Alizadeh.pdf

58. The NIS Directive and NIS Regulations. URL: https://www.itgovernance.eu/en-ie/nis-directive-ie
59. Directive (Eu) 2016/1148 Of The European Parliament And Of The Council of 06.07.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
60. The PCI DSS (Payment Card Industry Data Security Standard).. URL: https://www.itgovernance.eu/en-ie/what-is-the-pci-dss-ie
61. PCI Security Standards Council, Document Library. URL: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
62. Cybercriminals are exploiting fears of the pandemic to steal personal information, Saheli Roy Choudhury, 15.04.2020. URL: https://www.cnbc.com/2020/04/15/coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html
63. Річний відсоток депозиту URL: https://alfabank.ua/private-persons/deposits/products/profitable?gclid=Cj0KCQiAzsz-BRCCARIsANotFgPwauNGQTIstSNMA_y-pnjjoDLW9eJuzskFP7K-AXQTyuGpEmLb42saAhCsEALw_wcB&gclsrc=aw.ds (дата звернення 11.12.2020)
64. Індекс інфляції в Україні URL: https://index.minfin.com.ua/economy/index/inflation/2020/ (дата звернення 11.12.2020)
65. SANS, Behind the Curve? A Maturity Model for Endpoint Security, G. Mark Hardy, Жовтень 2015. URL: https://www.tripwire.com/-/media/tripwiredotcom/files/white-paper/tripwire-sans_endpoint_security_white_paper.pdf?rev=9ffc9d43039746e0950822bd68fc01d4

66. Systems Engineering Approaches, Deborah J. Bodeau and Richard D. Graubart, cc 197-214. URL: https://link.springer.com/chapter/10.1007%2F978-3-319-77492-3_9
67. Узагальнена Класифікація Видів Аудиту Інформаційних Технологій, Ус Р. Л.
68. Выгода от ИТ-аудита, М. Бартенева. URL: http://www.osp.ru/text/print/302/4278440.html.
69. Методологія і організація аудиту, В. С. Рудницький. – Тернопіль: Економічна думка, 1998, 196 с.
70. Аудит інформаційних технологій – новий вид аудиту організацій, Р. Л. Ус. Формування ринкових відносин в Україні: зб. наук. праць. – К.: НДЕІ, 2013.
71. Digital SBA. URL: https://www.sba.gov/about-sba/open-government/digital-sba
72. Smal Business Information Technology Strategic Plan (ITSP). URL: https://www.sba.gov/sites/default/files/resources_article/SBA_IT_Strategic_Plan_2012-2016_1.pdf
73. Introduction to IT Audit Student Notes. – INTOSAI, 2007.
74. Office of Internal Audit, IT Audit. URL: https://oacp.upenn.edu/audit/it/
75. Office of Internal Audit, Information Technology Internal Controls. URL: https://oacp.upenn.edu/audit/audit101/internal-controls-guidance/information-technology-internal-controls/
76. Office of Internal Audit, Construction Audit. URL: https://oacp.upenn.edu/audit/construction/
77. ИБ по-американски. Часть 1. Что такое NIST 800-53 и как выглядят контроли безопасности? Ivan Rumiantsev. URL: https://habr.com/ru/post/238245/

78. ИБ по-американски. Часть 3. Что из себя представляет базовый набор контролей и как определять критичность систем? Ivan Rumiantsev. URL: https://habr.com/en/post/238977/

79. Тарифи на електричну енергію, що відпускається для різних категорій побутових споживачів (у грн/кВт·год з ПДВ). URL: https://yasno.com.ua/b2c-tariffs (дата звернення 08.12.2020)

80. Using COBIT 5 to Assess IT Processes Capabilities and Evaluate Compliance With the World Lottery Association Security Control Standard and ISO 27001 Author: Ioannis Panopoulos, Maria Melliou, 11.10.2017. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2017/using-cobit-5-to-assess-it-processes-capabilities-and-evaluate-compliance-with-the-world-lottery-ass

81. IT Governance Institute, "Control Objectives for Information and related technologies (COBIT)", 2005. URL: www.isaca.org

82. Meeting the cyber challenge head-on. URL: https://www.hiscox.co.uk/cyberreadiness

83. Governing Information Security In Conjunction With Cobit And ISO 27001 Tolga Mataracioglu And Sevgi Ozkan. URL: https://www.researchgate.net/publication/51930390_Governing_Information_Security_In_Conjunction_With_Cobit_And_Iso_27001/fulltext/02a83e510cf2fb757aff2af9/Governing-Information-Security-In-Conjunction-With-Cobit-And-Iso-27001.pdf

84. An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, Razieh Sheikhpour and Nasser Modiri. URL: https://www.researchgate.net/publication/292833500_An_approach_to_map_COBIT_processes_to_ISOIEC_27001_information_security_management_controls

85. ISO/IEC 27001: 2005, "Information technology- Security techniques - Information security management systems- requirements," ISO Office, 2005.

86. A. Tsohou, S. Kokolakis, C. Lambrinoudakis and S. Gritzalis, "Information Systems Security Management: A Review and a Classification of the ISO Standards", Next Generation Society, Vol.26, Technological and Legal Issues, Part 6, 2010, cc. 220-235.
87. E. Humphreys, "Information security management standards: Compliance, governance and risk management", J Information Security Technical Report, Vol.13, No. 4, 2008, cc. 47-55.
88. K. L.,Thomson and R. von Solms, "Information security obedience: a definition", J Computers & Security, Vol. 24, 2005, cc. 69-75.
89. J. Heasuk, K. Seungjo and W. Dongho, "A Study on Comparative Analysis of the Information Security Management Systems", Lecture Notes in Computer Science, Vol. 6019, 2010, cc. 510-519.
90. What is the ISO 27000 Series of Standards? 08.05.2019, Jason Miller. URL: https://www.bitlyft.com/what-is-iso-27000/
91. Hiscox Cyber Readiness Report 2020. URL: https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf
92. 2018 Hiscox, Cyber Readiness Report. URL: https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf
93. What is the ISO 27000 series of standards? Luke Irwin 19th October 2020. URL: https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards
94. National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Resource Center, SP 800 series. URL: https://csrc.nist.gov/publications/sp800
95. NIST Developing Cyber Resilient Systems: A Systems Security Engineering Approach, Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau,

Rosalie Mcquaid, Листопад 2019. URL: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

96. Common Criteria (CC) for Information Technology Security Evaluation, Margaret Rouse, https://whatis.techtarget.com/definition/Common-Criteria-CC-for-Information-Technology-Security-Evaluation
97. Fundamentals of cybersecurity and the Cyber Resilience Oversight Expectations (CROE), CEMLA, Emran Islam, Constantinos Christoforides, Листопад 2019.
98. Ofgem, RIIO-2 Cyber Resilience Guidelines, 05.02.2020.
99. Panda security summit, cyber-resilience: the key to business security 2018. URL: https://www.pandasecurity.com/en/mediacenter/src/uploads/2018/05/Cyber-Resilience-Report-EN.pdf
100. 90% of companies acknowledge that they are not cyber-resilient, 24.09.2018. URL: https://www.pandasecurity.com/en/mediacenter/security/companies-not-cyber-resilient/
101. Rise in cyber criminality calls for increased IT resilience, Urs Küderli, 23.05.2019. URL: https://www.pwc.ch/en/insights/digital/rise-in-cyber-criminality-calls-for-increased-it-resilience.html
102. Cyber Resilience: What It Is and Why It's Important, 07.06.2018. URL: https://www.pandasecurity.com/en/mediacenter/news/what-is-cyber-resilience/

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи.

Формат	Найменування	Кількість листів	Примітки
А4	Реферат	3	
А4	Список умовних скорочень	1	
А4	Зміст	2	
А4	Вступ	2	
А4	Стан питання. Постановка задачі	41	
А4	Спеціальна частина	16	
А4	Економічна частина	8	
А4	Перелік посилань	11	
А4	Додаток А	1	
А4	Додаток В	3	
А4	Додаток С	4	
А4	Додаток D	1	
А4	Додаток Е	1	
А4	Додаток F	2	

ДОДАТОК В. Додаткові таблиці

Таблиця В.1 - Відмінності між зовнішнім і внутрішнім ІТ-аудитом[67].

Ознака	Зовнішній ІТ-аудит	Внутрішній ІТ-аудит
Мета	Отримання незалежного професійного висновку щодо стану ІТ-середовища, його сильних і слабких сторін, а також рекомендацій стосовно його покращення	Постійне удосконалення ІТ-середовища, підвищення зрілості ІТ-процесів, гарантування надійності та ефективності заходів ризик-менеджменту ІТ, а також обґрунтування відповідних інвестицій тощо
Масштаб	Вибірковий	Повний
Замовник	Вище керівництво об’єкта аудиту, контрагенти, власники, інвестори, регулюючі органи тощо	Вище керівництво об’єкта аудиту, акціонери
Виконавець	Приватна аудиторська фірма або аудитор-підприємець	Спеціальний підрозділ організації (служба внутрішнього ІТ-аудиту)
Підстава для проведення	Договір між замовником аудиту і виконавцем	Положення про службу внутрішнього ІТ-аудиту, узгоджений план аудиторських перевірок, наказ керівництва тощо
Правове регулювання відносин між сторонами	Відносини регулюються юридичними нормами цивільного законодавства на засадах партнерства і рівності сторін	Відносини регулюються нормами законодавства про працю. Наявна субординація виконавця перед вищим керівництвом замовника аудиту

Продовження таблиці В.1.

Залежність від національних стандартів аудиту	Обов'язкове дотримання і використання у роботі	На рівні рекомендацій
Оплата послуг	Оплата консалтингових послуг за умовами укладеного господарського договору про ІТ-аудит	Заробітна плата за трудовою угодою
Результат	Аудиторський висновок за формою і вимогами національних стандартів аудиту	Акти, звіти, рекомендації тощо, визначені внутрішніми угодами (Положенням про СВА-ІТ)[71, 72]
Незалежність	Висока	Середня або низька
Регулярність	Періодична - залежить від потреб замовника аудиту (зацікавлених сторін)	Неперервний процес
Знання бізнесу замовника	Середні (є потреба у тривалому вивченні особливостей бізнесу замовника)	Високі (це обумовлено безперервним процесом аудиту, структурною приналежністю до об'єкта аудиту)
Обов'язковість	Немає	Немає

Таблиця В.2 – Кіберінциденти за участю зловмисного програмного забезпечення та вимаганням за розблокування ресурсів жертви атаки за 2020 рік[91]

	Без вимагання	З вимаганням
Кількість атак	173	411
Середні збитки(тисячі доларів США)	492	927
Максимальні збитки однієї компанії(мільйони доларів США)	10,1	50.6
Найбільший разовий збиток(мільйони доларів США)	1,5	7
Загальна сума збитків(мільйони доларів США)	85	381

ДОДАТОК С. Діаграми та графіки зі звіту Hiscox за 2020 рік

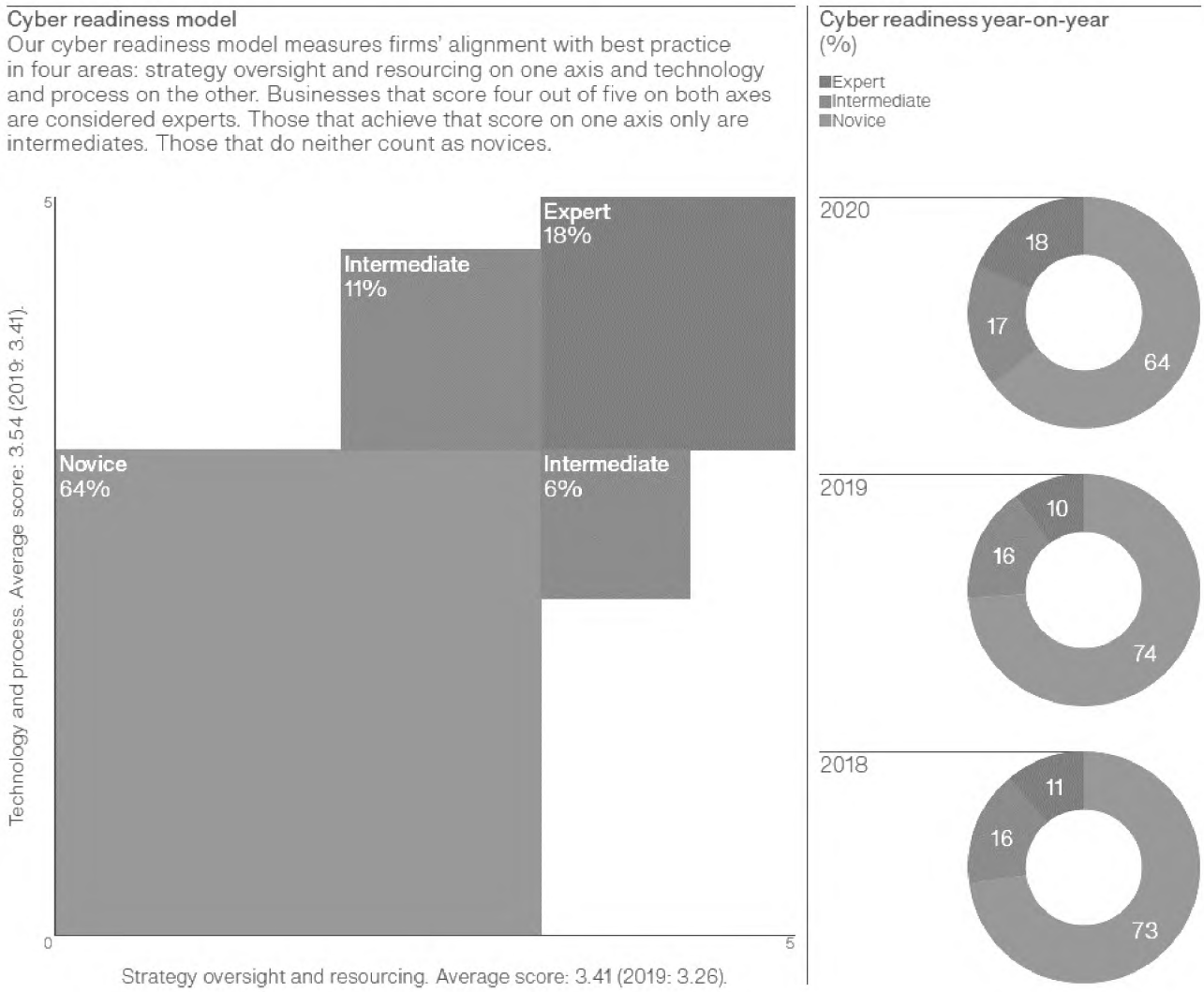

Рисунок С.1 - Розподіл кібер-готовності[91].

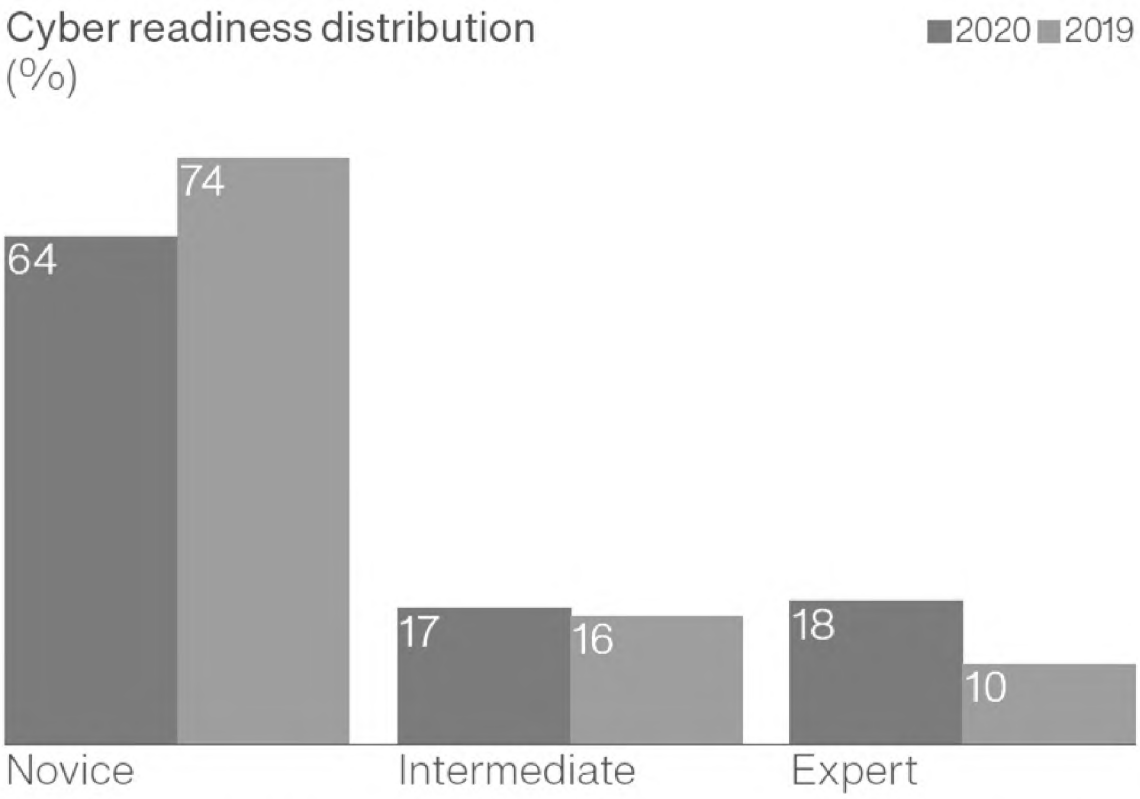

Рисунок С.2 - Розподіл кібер-готовності у порівнянні з 2019 роком[91].

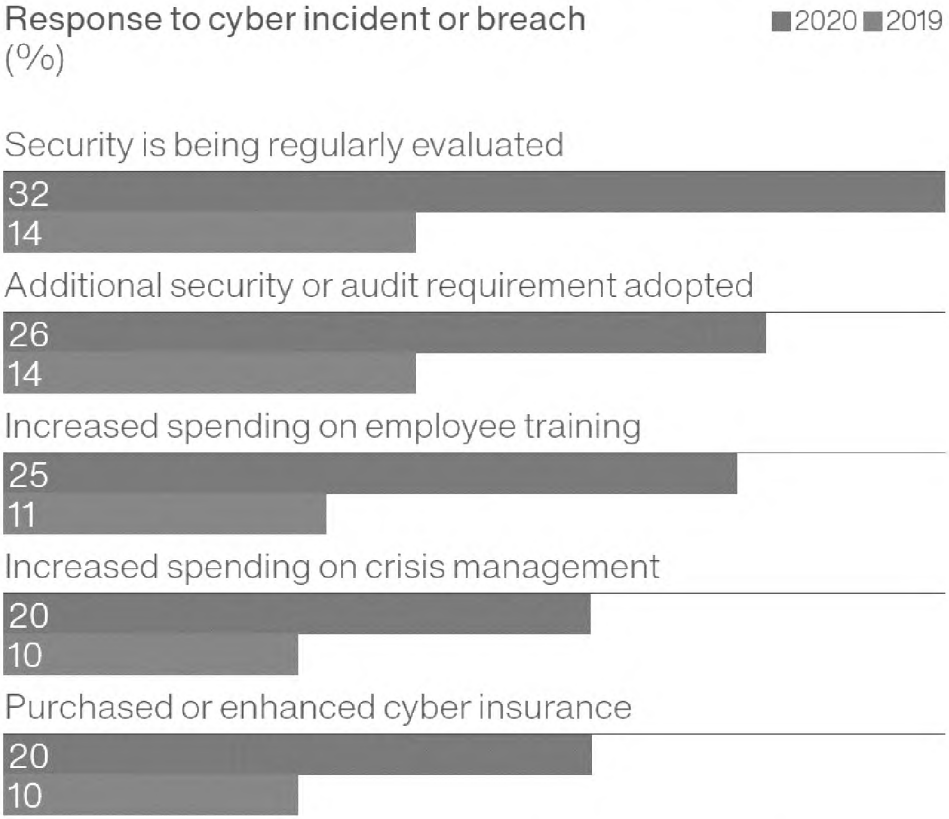

Рисунок С.3 - Реакція на кіберінциденти або порушення[91].

Рисунок С.4 – Витрати на кібербезпеку компаній за країнами[91].

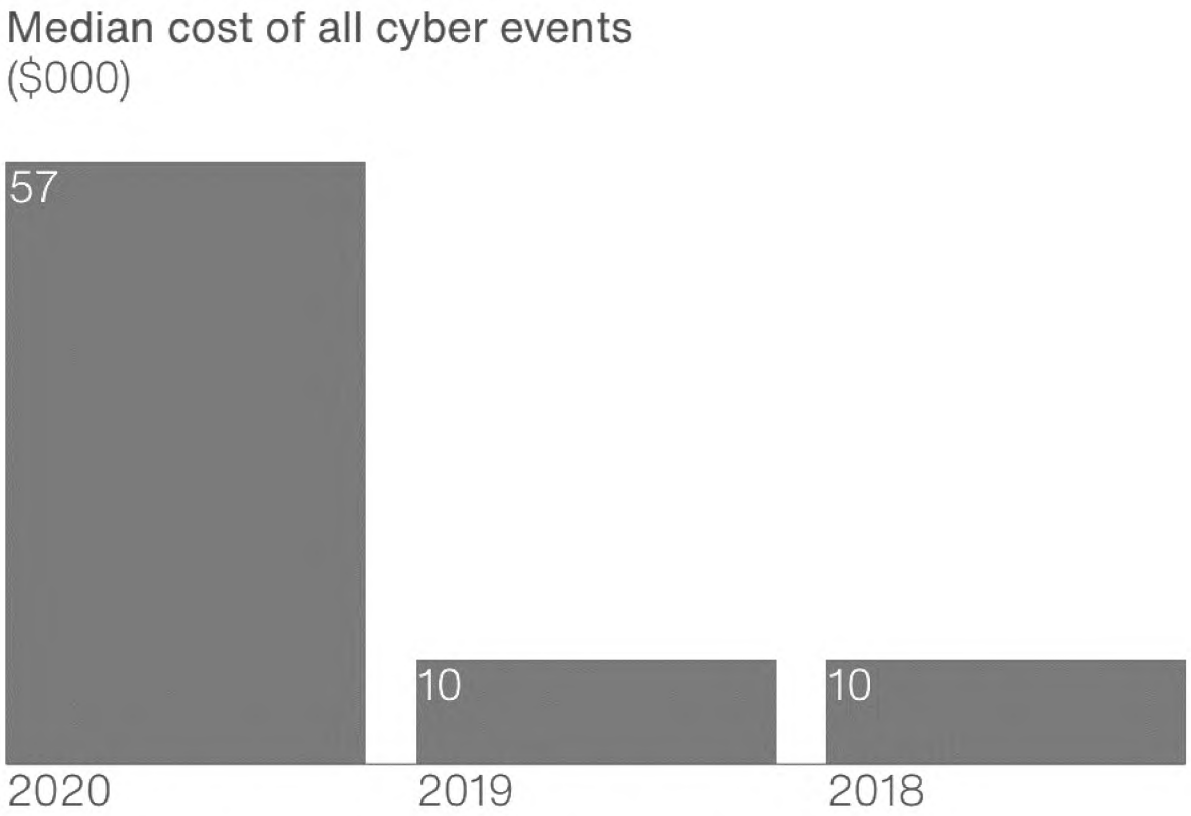

Рисунок С.5 – Середня вартість усіх кіберподій за роками[91].

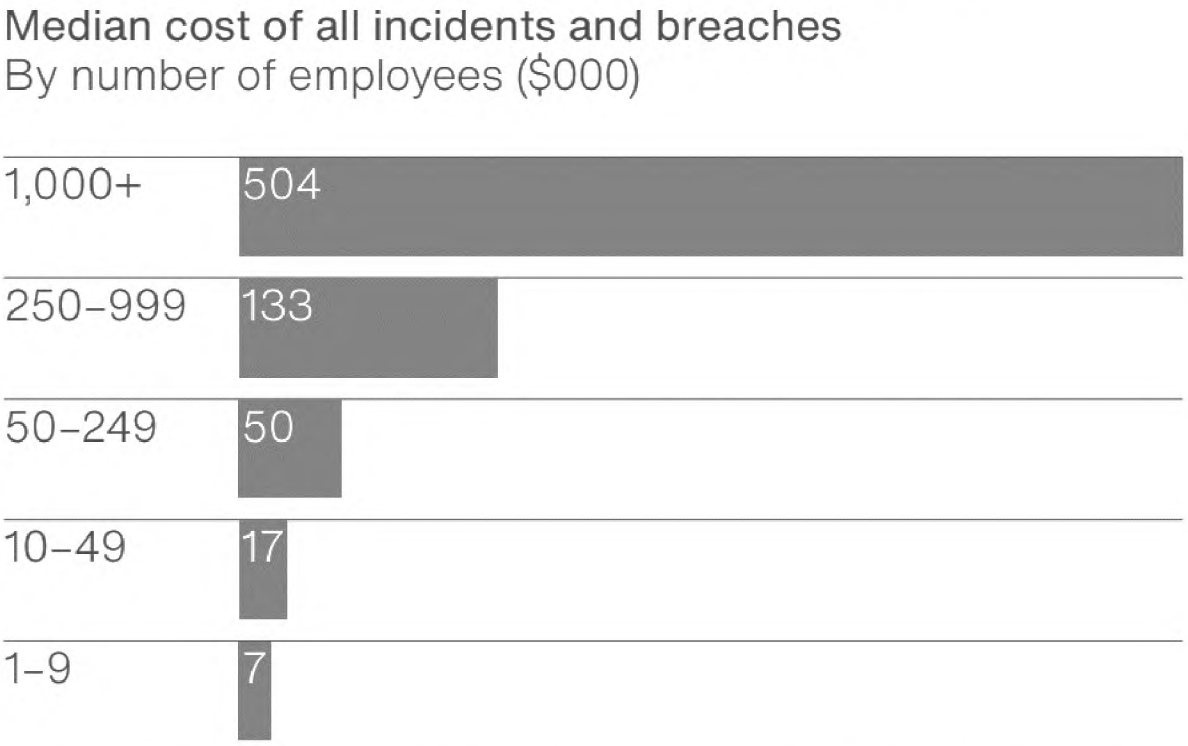

Рисунок С.6 – Середня вартість усіх кіберінцидентів та порушень за 2020 рік за кількістю співробітників у компанії (величини вказані у тисячах доларів)[91].

ДОДАТОК D. Перелік документів на оптичному носії

1. Пояснювальна записка Щітініна ПІ 125м-19-1.docx
2. Презентація кваліфікаційної роботи Щітініна ПІ 125м-19-1.pptx

ДОДАТОК Е. Відгук керівника економічного розділу

ДОДАТОК F. Відгук керівника кваліфікаційної роботи

на кваліфікаційну роботу магістра на тему: "Ризик-орієнтовний аудит кіберстійкості",

студентки групи 125м-19-1 Щітініної Поліни Ігорівни

Мета роботи – підвищення рівня забезпечення кіберстійкості організації.

Обрана тема є актуальною у зв'язку зі значною залежністю сучасного бізнесу від інформаційних технологій і необхідності підтримки бізнес функцій під впливом кіберінцидентів.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності фаху 125 "Кібербезпека" – аналіз принципів кібербезпеки та методів її досягнення, розробка рекомендацій проведення аудиту кібербезпеки та оцінки його результатів.

Задачі кваліфікаційної роботи: підвищення рівня кіберстійкості бізнес організації, розробка рекомендацій щодо проведення аудиту кіберстійкості, - віднесені до класу евристичних, вирішення яких основане на знаковорозумових уміннях фахівця.

Оригінальність рішень полягає у визначенні особливостей та виборі методики реалізації процесу аудиту кіберстійкості.

Практичне значення результатів рекомендацій полягає у запропонуванні ефективного рішення щодо підвищення рівня кіберстійкості за допомогою аудиту.

Оформлення пояснювальної записки виконано з незначними відхиленнями від стандартів.

Щітініна Поліна Ігорівна виявила себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, заслуговує оцінки "відмінно", а Щітініна Поліна Ігорівна присвоєнню їй

кваліфікації магістра за спеціальністю 125 Кібербезпека за освітньою програмою Кібербезпека

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Керівник дипломної роботи,
д.ф.-м.н., проф, _____ Кагадій Т.С.

Керівник спеціальної частини,
ст. викл. кафедри БІТ, _____ Тимофєєв Д.С.