МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АУДИТ ЗАХОДІВ З ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ”

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

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

_____ Нікіта МЕЛЬНИЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Нікіта МЕЛЬНИЧЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____
Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельниченку Нікіті Миколайовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аудит заходів з забезпечення безперервності бізнесу ”, керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти" № 36 від 27.02.24

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

3. Вихідні дані до кваліфікаційної роботи: *система управління безперервністю бізнесу, методика аудиту системи управління безперервністю бізнесу, інструменти аудиту, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати методології та стандарти забезпечення безперервності бізнесу
   4.2. Дослідити структуру системи управління безперервністю бізнесу
   4.3. Проаналізувати методи й інструменти аудиту заходів забезпечення безперервності бізнесу.
   4.4. Розробити рекомендації щодо підвищення ефективності заходів із забезпечення безперервності бізнесу.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних основ забезпечення безперервності бізнесу.	08.04.2024	
4.	Дослідження методики проведення аудиту заходів із забезпечення безперервності бізнесу.	22.04.2024	
5.	Розробка рекомендацій щодо підвищення ефективності заходів із забезпечення безперервності бізнесу.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Нікіта МЕЛЬНИЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Мельниченко Н.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Аудит заходів з забезпечення безперервності бізнесу"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач МЕЛЬНИЧЕНКО Нікіта у кваліфікаційній роботі проаналізував методології та стандарти забезпечення безперервності бізнесу; дослідив структуру системи управління безперервністю бізнесу; проаналізував методи та інструменти аудиту заходів із забезпечення безперервності бізнесу; розробив рекомендації щодо підвищення ефективності заходів із забезпечення безперервності бізнесу.

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

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

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Мельниченко Н.М. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Мельниченка Нікіти
на тему “Аудит заходів з забезпечення безперервності бізнесу ”

Актуальність. Безперервність бізнесу має важливе значення в контексті інформаційної безпеки через її роль у забезпеченні стійкості організації до збоїв. Заходи з безперервності бізнесу, такі як плани відновлення після катастроф та стратегії реагування на інциденти, мають вирішальне значення для підтримки цих цілей безпеки під час несприятливих подій, включаючи кібератаки, стихійні лиха та системні збої. Ці заходи знижують ризики, забезпечуючи швидке відновлення, мінімізуючи втрату даних і час простою, гарантуючи відповідність нормативним вимогам та зміцнюючи довіру зацікавлених сторін. Таким чином, безперервність бізнесу є невід'ємною частиною комплексної стратегії інформаційної безпеки. З огляду на зазначене дослідження методів та аудиту заходів із забезпечення безперервності бізнесу є актуальним науковим завданням.

Позитивні сторони.

1. У роботі детально проаналізовано компоненти системи управління безперервністю бізнесу в контексті інформаційної безпеки, досліджено методи їх аудиту, інструменти та показники, які при цьому використовуються.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу: 45 публікацій, в тому числі англомовних.

4. За результатами дослідження запропоновано рекомендації щодо підвищення ефективності компонентів забезпечення безперервності бізнесу в контексті інформаційної безпеки.

Недоліки.

1. Доцільно було б більш детально проаналізувати заходи, які мають бути реалізовані на кожному етапі аудиту.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач МЕЛЬНИЧЕНКО Нікіта заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню особливостей проведення аудиту заходів з забезпечення безперервності бізнесу. Робота складається зі вступу, трьох розділів, що містять 11 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 89 аркушів, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є проведення аналізу процесів аудиту заходів із забезпечення безперервності бізнесу.

Об'єктом дослідження є заходи з забезпечення безперервності бізнесу.

Предмет дослідження – особливості моніторингу та аудиту заходів з забезпечення безперервності бізнесу.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до аудиту заходів з забезпечення безперервності бізнесу.

Як результат у роботі досліджено основні технології забезпечення безперервності бізнесу в контексті інформаційної безпеки; проаналізовано особливості проведення аудиту заходів із забезпечення безперервності бізнесу; розроблено рекомендації щодо підвищення ефективності заходів із забезпечення безперервності бізнесу.

Галузь застосування. Розроблені підходи можуть бути використані при формування програми та плану аудиту, при проведенні внутрішніх та зовнішніх аудитів системи управління інформаційною безпекою та системи управління безперервністю бізнесу.

Ключові слова: АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ, КІБЕРСТІЙКІСТЬ.

ABSTRACT

The qualification work is devoted to the analysis and evaluation of the effectiveness of information security audit methods and tools. The work consists of an introduction, three chapters containing 11 figures, conclusions and a list of used sources from 45 titles. The total volume of the work is 89 sheets, of which 6 sheets are occupied by a list of conventional abbreviations and a list of used sources.

The purpose of the study is to analyze the processes of auditing business continuity measures.

The object of research is measures to ensure business continuity.

The subject of the study is the peculiarities of monitoring and auditing business continuity measures.

Research methods. In order to solve the above scientific task, the methods of analysis and synthesis, comparison, classification, expert evaluation, and a systematic approach to the audit of business continuity measures were used.

As a result, the study examines the main technologies for ensuring business continuity in the context of information security; analyses the peculiarities of auditing business continuity measures; and develops recommendations for improving the effectiveness of business continuity measures.

Field of application. The developed approaches can be used in the development of an audit program and plan, as well as in internal and external audits of the information security management system and business continuity management system.

Keywords: INFORMATION SECURITY AUDIT, INFORMATION SECURITY MANAGEMENT SYSTEM, BUSINESS CONTINUITY MANAGEMENT SYSTEM, CYBER RESILIENCE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІС	Інформаційна система
ІТ	Інформаційні технології
НСД	Несанкціонований доступ
ПЗ	Програмне забезпечення
СУІБ	Система управління інформаційною безпекою
УВІТ	Управління відновленням інформаційних технологій
BCMS	Система управління безперервністю бізнесу
BCP	План забезпечення безперервності бізнесу

ВСТУП

Актуальність теми. Аудит заходів із забезпечення безперервності бізнесу має вирішальне значення в контексті ІБ, гарантуючи, що організації можуть протистояти збоям, таким як кібератаки, стихійні лиха або системні збої, та відновлюватися після них. Такі аудити відіграють життєво важливу роль у зменшенні ризиків, захисті цілісності, конфіденційності та доступності даних. Виявляючи вразливі місця, аудит забезпечує наявність надійних планів для мінімізації простоїв і втрати даних.

Відповідність нормативним вимогам часто вимагає регулярного аудиту планів забезпечення безперервності бізнесу. Такі аудити допомагають організаціям уникнути юридичних санкцій, зберегти репутацію та продемонструвати прихильність до найкращих практик у сфері ІБ.

Ефективне реагування на інциденти є одним із ключових елементів заходів з забезпечення безперервності бізнесу. Аудити оцінюють готовність команд реагування на інциденти, забезпечуючи швидкі дії для локалізації та усунення інцидентів безпеки, таким чином мінімізуючи вплив на операційну діяльність та захищаючи конфіденційну інформацію.

Розподіл ресурсів є ще одним важливим аспектом, оскільки ефективна ІБ вимагає відповідного персоналу, технологій та бюджету. Аудит заходів з безперервності бізнесу дає уявлення про достатність та ефективність цих ресурсів, що дозволяє організаціям визначати пріоритети інвестицій, які посилюють їхні можливості у сфері безпеки.

З точки зору взаємодії із зацікавленими сторонами аудит забезпечує прозорість, запевняючи клієнтів, партнерів та інвесторів у готовності організації підтримувати операційну цілісність та її зобов'язання щодо цього. Така впевненість є особливо важливою в секторах, де довіра та надійність мають першорядне значення, таких як фінанси, охорона здоров'я та об'єкти критичної інфраструктури.

З огляду на зазначене дослідження методів аудиту заходів із забезпечення безперервності бізнесу має важливе значення для захисту інформаційних активів, забезпечення дотримання нормативних вимог, підвищення стійкості та підтримки довіри зацікавлених і є актуальним науковим завданням.

Мета роботи полягає у проведенні аналізу процесів аудиту заходів із забезпечення безперервності бізнесу.

Об'єктом дослідження є заходи із забезпечення безперервності бізнесу.

Предмет дослідження – особливості моніторингу та аудиту заходів з забезпечення безперервності бізнесу.

Для досягнення цієї мети в роботі необхідно виконати наступні ***завдання:***

1. Проаналізувати методології та стандарти забезпечення безперервності бізнесу.
2. Дослідити структуру системи управління безперервністю бізнесу
3. Проаналізувати методи й інструменти аудиту заходів забезпечення безперервності бізнесу.
4. Розробити рекомендації щодо підвищення ефективності заходів із забезпечення безперервності бізнесу.

Методи дослідження. Вирішення завдань, поставлених у дослідженні, здійснювалося за допомогою методів аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до аудиту заходів з забезпечення безперервності бізнесу.

Практичне значення одержаних результатів. Розроблені у дослідженні підходи можуть бути використані при формування програми та плану аудиту, при проведенні внутрішніх та зовнішніх аудитів системи управління інформаційною безпекою та системи управління безперервністю бізнесу, а також оцінці ефективності цих систем або окремих їх компонентів.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

Перед початком дослідження теми кваліфікаційної роботи необхідно ознайомитися з основними визначеннями у галузі кіберінцидентів, регуляторними вимогами, стандартами, основними компонентами системи управління безперервністю бізнесу, застосованими методологіями у сфері забезпечення безперервності бізнесу.

1.1 Аналіз концепцій та принципів безперервності бізнесу в контексті ІБ

Безперервність бізнесу відноситься до стратегій і процесів, які організація впроваджує для забезпечення можливості функціонування критичних бізнес-процесів під час і після катастроф або збоїв, а також щоб мінімізувати вплив таких порушень на операційну діяльність, доходи та репутацію організації. Ця концепція особливо важлива в контексті ІБ, де різноманітні кіберзагрози і збої в роботі ІТ-систем можуть мати серйозні наслідки (табл. 1.1).

Таблиця 1.1.

Види порушень та їх наслідки

Види порушень	Фінансові наслідки	Юридичні наслідки	Репутаційні наслідки	Приклади
Витік даних	Прямі фінансові втрати через шахрайство, витрати на відновлення систем, компенсації клієнтам	Юридичні покарання за недотримання вимог захисту даних, судові позови клієнтів та партнерів	Втрата довіри клієнтів та партнерів, негативні відгуки у ЗМІ, зниження рейтингу компанії	Витік ПД клієнтів через НСД
Кібер-атаки	Витрати на відновлення систем, втрати від зупинки бізнес-процесів, штрафи за недотримання контрактних зобов'язань	Відповідальність за недотримання стандартів безпеки, розслідування регуляторних органів	Втрата довіри інвесторів та клієнтів, публічне розслідування, негативне висвітлення у ЗМІ	Атака типу DDoS, злом мережі організації

Продовження таблиці 1.1.

Види порушень	Фінансові наслідки	Юридичні наслідки	Репутаційні наслідки	Приклади
Фішингові атаки	Фінансові втрати через шахрайство, витрати на підвищення рівня безпеки та навчання персоналу	Судові позови від постраждалих, відповідальність за недотримання внутрішніх політик безпеки	Зниження довіри до організації, негативне висвітлення у ЗМІ	Розголошення ПД внаслідок успішної соціоінженерної атаки (фішинговий лист)
Шкідливе ПЗ та віруси	Витрати на видалення шкідливого ПЗ, втрати через простій систем, можливі штрафи за невиконання зобов'язань перед клієнтами	Відповідальність за недотримання вимог з кібербезпеки, можливі розслідування регуляторних органів	Втрата репутації серед клієнтів та партнерів, негативне висвітлення у ЗМІ, шкода іміджу.	Зараження системи вірусом, що призвело до втрати даних
Внутрішні загрози (інсайдери)	Прямі фінансові втрати через розкрадання коштів, витрати на розслідування та зміцнення безпеки	Юридичні наслідки для організації, судові позови	Погіршення репутації серед співробітників та клієнтів, негативні відгуки у ЗМІ	Співробітник розголосив службову інформацію конкуренту за винагороду
НСД	Витрати на відновлення систем, компенсації клієнтам, витрати на підвищення рівня безпеки	Судові позови від постраждалих клієнтів, юридичні наслідки за недотримання вимог безпеки	Втрата довіри клієнтів та партнерів, негативне висвітлення у ЗМІ	Хакери отримали доступ до системи компанії та вкрали важливу інформацію
Неналежне управління даними	Витрати на виправлення помилок, компенсації клієнтам, штрафи за недотримання регуляторних вимог	Юридичні наслідки за порушення регуляторних вимог, судові позови від клієнтів	Зниження репутації серед клієнтів та партнерів, негативне висвітлення у ЗМІ	Неправильне зберігання даних клієнтів, що призвело до їх втрати

Надійний план забезпечення безперервності бізнесу визначає процедури для підтримки основних процесів, функцій, захисту даних і забезпечення швидкого відновлення після збоїв. Ключові концепції безперервності бізнесу представлені в табл. 1.2.

Таблиця 1.2.

Ключові концепції безперервності бізнесу

Концепція	Опис
Управління ризиками	Ідентифікація, оцінка та управління ризиками, які можуть вплинути на безперервність бізнесу, включаючи як внутрішні, так і зовнішні загрози.
Оцінка впливу на бізнес (BIA)	Визначення критичних бізнес-функцій та процесів, а також аналіз потенційних наслідків переривання цих процесів для організації.
Планування безперервності бізнесу (BCP)	Розробка та впровадження планів, що забезпечують безперервність критичних бізнес-функцій під час кризових ситуацій.
Відновлення після аварій (DRP)	Плани та заходи, спрямовані на відновлення IT-систем та інфраструктури після інцидентів, які викликають їх переривання.
Кризове управління	Стратегії та процеси для управління надзвичайними ситуаціями, включаючи координацію дій, комунікацію та прийняття рішень під час кризи.
Управління інцидентами	Виявлення, реагування та вирішення інцидентів, які можуть вплинути на безперервність бізнесу, з мінімізацією їх впливу на операції.
Навчання та підготовка персоналу	Проведення регулярних тренувань і симуляцій для підготовки співробітників до дій у кризових ситуаціях і перевірки ефективності BCP.
Моніторинг та тестування	Регулярне тестування BCP та відновлення після аварій для забезпечення їх актуальності та ефективності.
Управління змінами	Забезпечення того, що плани безперервності бізнесу та відновлення після аварій адаптуються до змін у бізнес-процесах, технологіях та зовнішньому середовищі.
Інтеграція з бізнес-стратегією	Інтеграція заходів з безперервності бізнесу у загальну бізнес-стратегію для забезпечення узгодженості дій та прийняття рішень на всіх рівнях організації.

Впровадження надійного контролю доступу та шифрування є ключовим компонентом систем ІБ, які не тільки забезпечують конфіденційність даних, але й сприяють безперервності бізнесу. Ці заходи запобігають НСД до даних і витоку інформації, які можуть привести до серйозних збоїв в роботі організації. Використовуючи надійні засоби контролю доступу, такі як системи аутентифікації та авторизації, а також шифрування даних, організації можуть звести до мінімуму ризик втрати даних і забезпечити їх цілісність.

Регулярне тестування та оновлення BCP можуть допомогти виявити можливі слабкі місця в системі та своєчасно усунути їх, підтвердивши ефективність заходів ІБ за допомогою ще одного важливого тесту для забезпечення стійкості бізнес-систем в умовах сучасних кіберзагроз. Оновлення BCP допомагає підтримувати ефективність заходів захисту на актуальному рівні у відповідь на кіберзагрози та швидкі зміни в технологіях. Такий підхід допоможе забезпечити стабільність бізнесу і захистити бізнес від потенційних

кібератак. Ключові принципи безперервності бізнесу представлені в табл. 1.3.

Таблиця 1.3.

Ключові принципи безперервності бізнесу

Принцип	Опис
Стійкість (кіберстійкість)	Забезпечення здатності організації протистояти та адаптуватися до кібератак, технічних збоїв та інших загроз, з мінімізацією їх впливу на бізнес-процеси.
Резервування (дублювання)	Впровадження резервних систем і ресурсів, які можуть бути використані в разі відмови основних систем, включаючи дублювання критичних компонентів інфраструктури.
Швидке відновлення	Розробка процедур для швидкого відновлення критичних бізнес-функцій і IT-систем після інцидентів, що забезпечує мінімізацію часу простою та зниження втрат.
Засоби забезпечення ІБ	Інтеграція заходів з ІБ в плани безперервності бізнесу для захисту даних і систем від кібератак та інших загроз.
Системний підхід до управління ризиками	Ідентифікація, оцінка та управління ризиками на всіх рівнях організації, що забезпечує цілісність і стійкість бізнес-процесів.
Інтеграція з бізнес-стратегією	Узгодження BCP з загальною бізнес-стратегією для забезпечення послідовності дій та пріоритетів.
Регулярне тестування та оновлення	Проведення регулярних тестувань BCP та відновлення після аварій для перевірки їх ефективності та актуальності, а також їх оновлення за необхідності.
Навчання та підготовка персоналу	Проведення регулярних навчань і тренувань для співробітників, щоб забезпечити їх готовність до дій в умовах кризи та ефективного виконання BCP.
Ефективна комунікація	Створення та підтримка систем комунікацій для швидкого та точного інформування співробітників, клієнтів, постачальників та інших зацікавлених сторін під час кризових ситуацій.
Безперервний моніторинг та управління	Постійний моніторинг бізнес-процесів і навколишнього середовища для своєчасного виявлення потенційних загроз і забезпечення відповідного реагування.

Впровадження безперервності бізнесу у сфері ІБ викликає низку проблем, з якими організації зіштовхуються в сучасному цифровому середовищі.

По-перше, швидкий розвиток кіберзагроз створює постійну необхідність адаптації та удосконалення заходів безпеки. Кіберзлочинці постійно вдосконалюють свої техніки, щоб обійти захист, що означає, що організаціям потрібно бути постійно на варті і оновлювати свої заходи безпеки.

Друга проблема полягає у обмеженості ресурсів. Впровадження ефективних заходів безперервності бізнесу вимагає значних фінансових та людських ресурсів. Це може бути особливо складно для малих та середніх підприємств, які можуть мати обмежений бюджет та персонал.

Третя проблема пов'язана з складною інтеграцією різних ІТ-систем. Багато підприємств мають різноманітні ІТ-системи та програми, які можуть бути складно інтегрувати в єдину систему безпеки та безперервності. Це може призвести до проблем з управлінням та координацією заходів безпеки та відновлення в разі інцидентів.

Четверта проблема пов’язана з відсутністю свідомості та підтримки вищого керівництва. Безперервність бізнесу та ІБ можуть не бути пріоритетними для вищого керівництва організації. Це може призвести до недостатньої підтримки та виділення ресурсів на важливі ініціативи.

П’ята проблема пов’язана зі змінами в законодавстві та регуляторних вимогах, зокрема у сфері захисту даних, які можуть вимагати постійного оновлення та адаптації стратегій безперервності бізнесу, щоб відповідати вимогам законодавства (табл. 1.4).

Врахування цих проблем дозволить організаціям більш ефективно планувати та впроваджувати стратегії безперервності бізнесу у сфері ІБ. Для цього необхідно розробляти гнучкі та адаптивні стратегії, а також забезпечувати постійне оновлення та навчання персоналу з питань кібербезпеки.

Таблиця 1.4.

Основні стандарти, пов'язані з безперервністю бізнесу

Стандарти	**Опис**
ISO 22301	Встановлює вимоги до BCMS. Надає рамки для розробки, реалізації, вдосконалення та підтримки системи управління.
ISO/IEC 27002	Містить набір контрольних заходів безпеки інформації. Включає вимоги щодо резервування засобів захисту та рекомендації з управління ІБ.
ISO/IEC 27035	Надає керівництво щодо управління інцидентами в області ІБ. Описує процеси та процедури виявлення, аналізу та реагування на інциденти.
GDPR	Регламент, що стосується захисту та обробки ПД громадян ЄС. Включає вимоги до безпеки даних та управління інцидентами безпеки даних.

Останнім часом спостерігається збільшення загроз, що стоять перед фінансовими установами. Деякі з цих загроз можуть мати суттєвий негативний вплив на організацію, який навіть може призвести до припинення її діяльності. Тому установам, банкам, організаціям необхідно впровадити політику

безперервності бізнесу, щоб визначити критичні процеси та ресурси, а також вжити необхідних заходів з їх захисту в разі серйозних загроз.

У відповідності до підходу безперервності ведення бізнесу, організація приймає контрзаходи, щоб прямо протистояти ризикам, які можуть спричинити значні збої критичних бізнес-процесів. Організації заздалегідь планують, як реагувати на ті чи інші несприятливі кризові явища, та впроваджує відповідну систему у свої щоденні операції, задля швидкого реагування на кризову ситуацію. Таким чином, організація може продовжувати свою бізнес-діяльність, не завдаючи незручностей клієнтам, партнерам, та втрачаючи мінімум доходу та ресурсів.

Безперервність бізнесу включає в себе планування та підготовку, для забезпечення можливості організації продовжувати працювати, у випадку серйозних інцидентів або катастроф та здатності відновитись до нормального стану протягом досить короткого періоду [1].

Управління безперервністю бізнесу визначене в стандарті ISO 22301:2021, як «процес виявлення потенційних загроз бізнес діяльності організації» та «який забезпечує структуру для побудови стійкості організації зі спроможністю ефективного реагування, яке захищає інтереси ключових акціонерів, репутацію, рейтинг компанії та діяльність зі створення цінностей».

Управління безперервністю бізнесу повине мати всебічний підхід в управлінні організацією, а не зосереджений в одному напрямці. Необхідно передбачати негативний вплив на організацію при розробці процесу та враховувати таку можливість для розуміння можливостей організації та прихованих резервів.

Особливу увагу до управлінню безперервністю бізнесу на практиці приділяють ІТ-компанії, банки та великі корпорації, а також усі фінансові установи. Для організацій в сфері фінансів – це просто невід’ємна частина управління, бо вони контролюється національними та міжнародними регуляторами.

Окремим напрямком управління безперервністю бізнесу є кризове управління. Управління безперервністю бізнесу та кризове управління не є одним й тим самим, хоча й чітку різницю також важко помітити. Антикризове управління засноване на плані антикризового управління і направлено на забезпечення стабільного функціонування всіх важливих процесів і роботи організації в цілому. План антикризового управління є універсальним і не включає конкретних покрокових дій у разі виникнення кризи, а лише описує загальну схему реагування та ескалації проблеми. Антикризове управління зосереджено не на критично важливих бізнес-процесах, а на кризових явищах, які загрожують всій організації (стихійні лиха, технологічні кризи, конфронтації, організаційні помилки, насильство на робочому місці, чутки, тероризм).

Забезпечення безперервності бізнесу та антикризове управління – це два взаємопов'язані процеси, спрямовані на захист організації як від природних, так і від антропогенних загроз. Повинна бути забезпечена наявність відповідної інформації для чіткого визначення відповідальних, які повинні займатися цією справою.

Останнім елементом BCMS має бути постійне тестування та перегляд існуючих планів та політик. План тестування вибирається залежно від типу компанії та її цілей.

Управління безперервністю бізнесу забезпечує комплексну інтеграцію всіх заходів, що застосовуються до організації, в реальний вагомий керований комплекс, який дозволяє організації безперервно надавати послуги, уникати впливу надзвичайних ситуацій на операційну діяльність і мінімізувати можливий збиток.

Щоб забезпечити безперервну роботу організації, необхідно застосовувати заходи з підтримки безперервності бізнесу. Це полягає в розробці плану, що дозволяє організації функціонувати в умовах ліквідації або скорочення діяльності. BCP повинен допомагати організаціям відновлювати діяльність без значних затримок.

Щоб розробити BCP, необхідно визначити ризики, які можуть призвести до припинення діяльності організації. Також потрібно визначити пріоритетність того, наскільки важливою є безперервність для різних видів операцій, які здійснює організація. Далі потрібно виявити та проаналізувати другий набір потенційних ризиків, що можуть призвести до перерви в діяльності організації. Наприклад, бізнес може потрапити в передачі власності, або можуть виникнути проблеми з постачанням послуг або матеріалів. Подальший аналіз дає можливість виявити ризики та прорахувати їхню вагу, а також прийняти заходи для їх належної обробки.

Для досягнення безперервності бізнесу потрібно розробити план відновлення послуг та дотримуватися його. План має містити програму дій, яка дасть можливість організації відновити свою діяльність після здійснення критичних дій для вирішення проблеми. План має містити такі дані, як перелік місць, де можуть бути потрібні послуги відновлення, контактні дані для підтримки, критерії оцінки ризиків та план дій для відновлення діяльності.

Застосування BCP є необхідним для забезпечення надійної роботи організації і забезпечення безперервності послуг та продуктів. Розробка та застосування плану допоможе організації боротися з потенційними ризиками та отримати конкурентні переваги.

1.2 Аналіз регуляторного середовища у сфері забезпечення безперервності бізнесу

Першим стандартом, що використовується у сфері забезпеченні безперервності бізнесу, є міжнародний стандарт ISO/IEC 27002, який містить кращі практики щодо розробки та впровадження в організації СУІБ в контексті вибору, впровадження та управління заходами захисту, заснованими на оцінці ризиків. Він містить більш повний опис і рекомендації щодо впровадження заходів забезпечення ІБ в порівнянні з міжнародним стандартом ISO/IEC 27001 та призначений для використання організаціями, які:

- обирають інструмент управління для ефективного функціонування заходів захисту на основі вимог стандарту ISO/IEC 27001;
- впроваджують інструменти управління ІБ;
- розробляють власні принципи управління ІБ.

Положення цього міжнародного стандарту можуть стати основою для вибору організацією заходів захисту відповідно до вимог стандарту ISO/IEC 27001, відповідних інструментів управління ІБ та їх застосування до окремих бізнес-процесів.

Такі заходи захисту можуть включати політику, процеси, процедури, організаційні структури та можливості програмного та апаратного забезпечення, і повинні створюватися, впроваджуватися, контролюватися, переглядатися і вдосконалюватися в міру необхідності, щоб забезпечити відповідність конкретних цілей ІБ бізнес-цілям організації.

ISO/IEC 27002 — це міжнародний стандарт, який містить вказівки для організацій, які прагнуть створити, запровадити та вдосконалити систему управління інформаційною безпекою (ISMS), орієнтовану на кібербезпеку [2].

Стандарт ISO/IEC 27002 показує, що організації можуть використовувати як інструменти управління, представлені в IT, так і інші джерела. З іншого боку, задовольняючи конкретні потреби і, за необхідності, організація може самостійно розробляти нові інструменти управління ІБ.

Дуже важливим моментом є вибір власних інструментів управління організацією і вимог до безпеки. В цілому існує 3 джерела для їх визначення:

- вибір, заснований на оцінці ризиків ІБ, узгодженій з бізнес-стратегією та цілями організації;
- юридичні, нормативні, договірні або статутні вимоги;
- принципи, цілі та бізнес-вимоги, що пред'являються до обробки, зберігання, передачі та архівування інформації.

Вибір інструментів управління також залежить від рівня прийнятності ризиків, варіантів обробки ризиків та організаційних рішень, що приймаються на

основі визначення загального підходу до управління ризиками відповідно до національних та міжнародних стандартів.

Оскільки належні практики управління інцидентами ІБ є вагомою складовою процесів забезпечення безперервності бізнесу, доцільно розглянути міжнародний стандарт ISO/IEC 27035, який містить найкращі практики та рекомендації щодо впровадження стратегічних планів управління інцидентами та підготовки до реагування на інциденти. Даний стандарт містить основні принципи безпеки для запобігання інцидентів ІБ та ефективного реагування на них. Крім того, стандарт включає спеціальний процес управління інцидентами, подіями та потенційними вразливостями в області ІБ.

Організації, які використовують систему управління інцидентами ІБ, можуть управляти бізнес-ризиками. Аналогічним чином, стандарт ISO/IEC 27035 є ключовим елементом структури безпеки організації для ефективного управління ІБ, запобігання інцидентів і створення стійких бізнес-процесів.

ISO/IEC 27035 є найефективнішим способом захисту організацій від інцидентів у сфері ІБ та зменшення фінансових наслідків для їхнього бізнесу, якщо вони зацікавлені в безпеці ІТ.

Впровадження належної системи управління інцидентами відповідно до вимог ISO/IEC 27035 дозволяє організаціям:

- зрозуміти концепції, підходи та інструменти для ефективного управління інцидентами ІБ;
- проаналізувати сучасні методи ефективного реагування на інциденти;
- отримати знання, необхідні для створення команди з управління інцидентами в області ІБ та управління нею;
- зменшити ймовірність збоїв і негативного впливу на бізнес-операції;
- покращити навички управління ІБ та аналіз інцидентів;
- отримати знання про найкращі практики управління ІБ.

Найпоширенішим стандартом для забезпечення безперервності бізнесу є ISO 22301:2021 – міжнародний стандарт системи управління безперервністю

бізнесу (BCMS), що дозволяє компанії або організації залишатися конкурентоспроможною в сучасному бізнес-середовищі.

Цей стандарт базується на структурах високого рівня (HLS), таких як система управління якістю (ISO 9001), система управління навколишнім середовищем (ISO 14001) та СУІБ (ISO/IEC 27001) [3].

У разі надзвичайної ситуації багато компаній та організацій повинні мати можливість зменшити втрати та продовжувати працювати. Стандарт ISO 22301 розроблений для того, щоб допомогти організаціям запобігати, належно готуватися, реагувати і усувати непередбачені і руйнівні інциденти. Для цього стандарт забезпечує практичну основу для створення ефективної системи забезпечення безперервності бізнесу та управління нею. Стандарт ISO 22301 спрямований на захист організацій від широкого спектру потенційних загроз і збоїв. Цей стандарт допомагає показати зацікавленим сторонам, що організації можуть швидко подолати збої в роботі та надавати постійні та ефективні послуги.

У багатьох країнах світу діють закони, що визначають відповідальність організації за планування дій у надзвичайних ситуаціях. Ці обов'язки часто включають впровадження системи управління безперервністю бізнесу. Як результат, організації, які повинні легально брати участь у плануванні надзвичайних ситуацій, таких як громадські роботи, транспорт та медичне обслуговування, повинні бути сертифіковані за стандартом ISO 22301:2021. Незалежно від того, чи потрібно організації впроваджувати стандарти відповідно до галузевих стандартів чи ні, отримання відповідного сертифіката – це рекомендований спосіб підвищити кіберстійкість та вдосконалити процеси управління ризиками.

Основною метою BCMS є підготовка, впровадження та підтримка інструментів та можливостей управління, які допомагають організаціям керувати своєю загальною здатністю продовжувати свою діяльність під час збоїв. До основних переваг ефективно впровадженої та функціонуючої BCMS можна віднести:

- впровадження та сертифікація BCMS може створити додаткову конкурентну перевагу, захистити та зміцнити репутацію та авторитет, сприяти досягненню стратегічних цілей та сприяти сталому розвитку організації;
- ефективна BCMS дозволяє організаціям захистити активи та знизити ризик подальших втрат, зберігаючи при цьому доходи після інцидентів ІБ, стихійних лих тощо;
- BCMS допомагає організаціям підтримувати рівень обслуговування, який вони надають своїм клієнтам. Це також допомагає оцінити потенційний вплив збоїв у роботі, швидко приймати доцільні рішення, своєчасно вживати ефективних заходів реагування та мінімізувати загальний вплив;
- сертифікована BCMS є корисним інструментом для впровадження чітко визначеної системи реагування на інциденти та звітності;
- оскільки сертифікація включає регулярні перевірки та внутрішні аудити, вона забезпечує, що організація має відповідні процеси управління ризиками і забезпечує рівень безпеки, необхідний для захисту своїх продуктів і послуг;
- з точки зору внутрішніх процесів, у організації є можливість підтримувати ефективність у разі збою, демонструвати управління ризиками і підвищувати здатність своєчасно усувати всі операційні уразливості.

Таким чином, цей стандарт визначає вимоги до впровадження, підтримки та вдосконалення BCMS для зниження ймовірності, готовності, реагування та відновлення після збою. Вимоги стандарту ISO 22301 є загальними і призначені для використання всіма організаціями або їх підрозділами, незалежно від типу, розміру або характеру організації, якщо вони:

- бажають впроваджувати, підтримувати та вдосконалювати BCMS;
- намагаються забезпечити відповідність заявленій політиці забезпечення безперервності бізнесу;
- бажають мати можливість виробляти продукцію і продовжувати надавати послуги з певною продуктивністю, прийнятною в разі збою;

- намагаються підвищити стабільність за рахунок ефективного використання BCM.

Ступінь застосовності вимог залежить від виробничого середовища і складності організації.

ISO/IEC 27005 – один з провідних міжнародних стандартів в області управління ІБ, який містить докладні рекомендації з управління ризиками ІБ. Стандарт доповнює ISO/IEC 27001, пропонуючи більш глибокий і структурований підхід до управління ризиками, що дозволяє організаціям більш ефективно захищати інформаційні активи.

Управління ризиками є важливим аспектом загальноорганізаційної стратегії ІБ. Стандарт ISO/IEC 27005 визначає контекст і межі процесу управління ризиками, включаючи розуміння як внутрішніх, так і зовнішніх факторів, які можуть вплинути на ІБ.

Після виявлення ризиків проводиться їх аналіз, включаючи оцінку потенційних можливостей і впливу виявлених загроз. Це дозволяє зрозуміти, які ризики є найважливішими та потребують негайного втручання. Оцінка ризиків, проведена після аналізу, допомагає визначити прийнятність ризику з точки зору організації та встановити пріоритети для подальшого управління ризиками.

Одним із ключових аспектів стандарту ISO/IEC 27005 є управління ризиками, яке передбачає вибір належних заходів щодо пом'якшення, запобігання, передачі або прийняття ризиків. Розробляючи та впроваджуючи плани управління ризиками, організації можуть мінімізувати негативний вплив ризиків на свою діяльність. Також важливо постійно відстежувати і аналізувати ризики, оцінювати ефективність вжитих заходів і забезпечувати актуальність і результативність процесу управління ризиками.

Документування процесу управління ризиками є ще одним важливим аспектом стандарту ISO/IEC 27005. Ведення чіткої документації по виявленню, аналізу, оцінці та обробці ризиків забезпечує прозорість і можливість перегляду прийнятих рішень. Це також допомагає підвищити обізнаність та залучення всіх зацікавлених сторін, включаючи вище керівництво та персонал організації.

Стандарт ISO/IEC 27005 підкреслює важливість чіткого визначення ролей та обов'язків для тих, хто бере участь у процесі управління ризиками. Це допомагає гарантувати, що кожен працівник усвідомлює свої обов'язки та готовий реагувати на потенційні інциденти. Ефективна комунікація між усіма зацікавленими сторонами також є важливим аспектом, що сприяє успішній реалізації процесу управління ризиками.

Завдяки стандарту ISO/IEC 27005 організації мають системний підхід до управління ризиками ІБ, який допомагає забезпечити захист критично важливої інформації та підвищити загальну стійкість до загроз. Цей стандарт допомагає підвищити рівень безпеки інформаційних ресурсів, підвищити обізнаність і готовність персоналу, а також забезпечити об'єктивність і прозорість процесу управління ризиками. Завдяки постійному вдосконаленню та адаптації до нових загроз і змін в організаційному середовищі, стандарт ISO/IEC27005 ідеально підходить для сучасних організацій, які прагнуть забезпечити надійну ІБ.

1.3 Визначення основних компонентів системи управління безперервністю бізнесу

BCMS складається з різних компонентів, які спільно допомагають організації відновлювати свою діяльність після кризових ситуацій та забезпечувати продовження операцій. До основних компонентів BCMS відносять стратегічне планування, розробку BCP, проведення тестувань та виправлення проблем, управління ризиками, розробку комунікаційних зв’язків, розробку та впровадження УВІТ, управління персоналом, управління інцидентами, а також моніторинг та оцінку впроваджених заходів (рис. 1.1).

Рис. 1.1. Основні компоненти BCMS

Чітке визначення ролей та відповідальності, а також комплексна оцінка ризиків дозволяють створити ефективну BCMS, яка забезпечить стійкість організації до кризових ситуацій. Систематичний підхід до цього процесу забезпечує не лише готовність до можливих загроз, але й підвищує загальну ефективність та стійкість організації, що є ключовими факторами успішного розвитку в сучасному бізнес-середовищі. Крім перерахованих вище дій, необхідно визначити потребу в проєкті. Для деяких компаній забезпечення безперервності бізнесу – це забезпечення ефективності критично важливих бізнес-функцій і демонстрація клієнтам стійкості їх бізнесу. З іншого боку, варто враховувати національне та міжнародне законодавство та вимоги регуляторних органів щодо безперервності бізнесу.

Розробка документованих BCP та процедур, які дозволяють організації відновити свою діяльність після кризових ситуацій. З власником процесу проводиться співбесіда, щоб визначити тип впливу на бізнес і залежність

процесу від IT і зовнішніх сервісів. Потім визначається максимально допустимий час простою (Maximum Allowable Outage).

Максимально допустиме відключення (МАО) – це максимальний проміжок часу, протягом якого система може бути недоступною, перш ніж її втрата поставить під загрозу цілі організації або виживання [4].

Після того, як власник процесу/функції визначився з МАО, IT-відділ на основі МАО визначає показники RTO, RPO та SDO:

- RTO (Recovery Time Objective) – це проміжок часу, протягом якого програма може не працювати, не завдаючи значної шкоди бізнесу, а також час, потрібний для переходу системи від втрати до відновлення. [5];
- RPO (Recovery Point Objective) – це максимально прийнятний обсяг втрати даних після незапланованої втрати даних, виражений у вигляді часу [6];
- цілі надання послуг (SDO) – рівень доступності послуг у певний момент часу.

Детальна схема RTO зображена на рис. 1.2 [7].

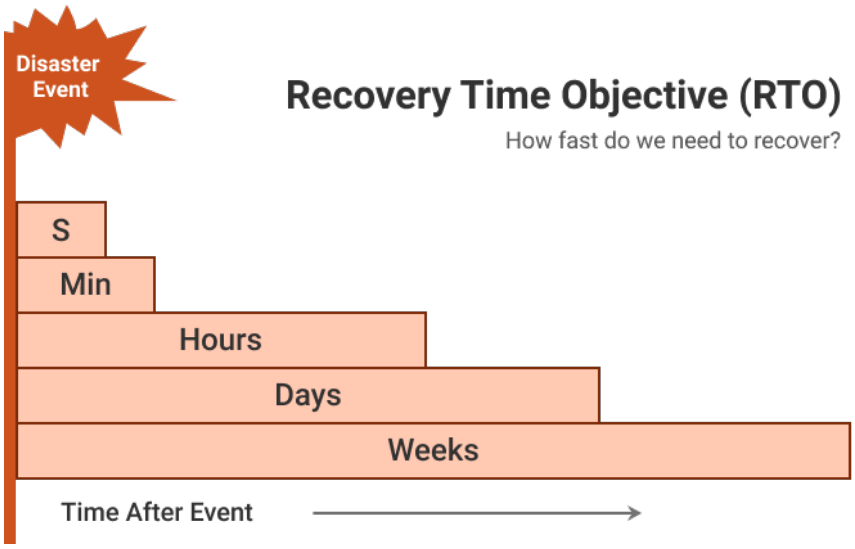

Рис. 1.2. Схема RTO

Як видно за схемою, RTO враховує кроки, які співробітники повинні виконати для повернення організації до робочого стану. Детальна схема RPO зображена на рис. 1.3 [8].

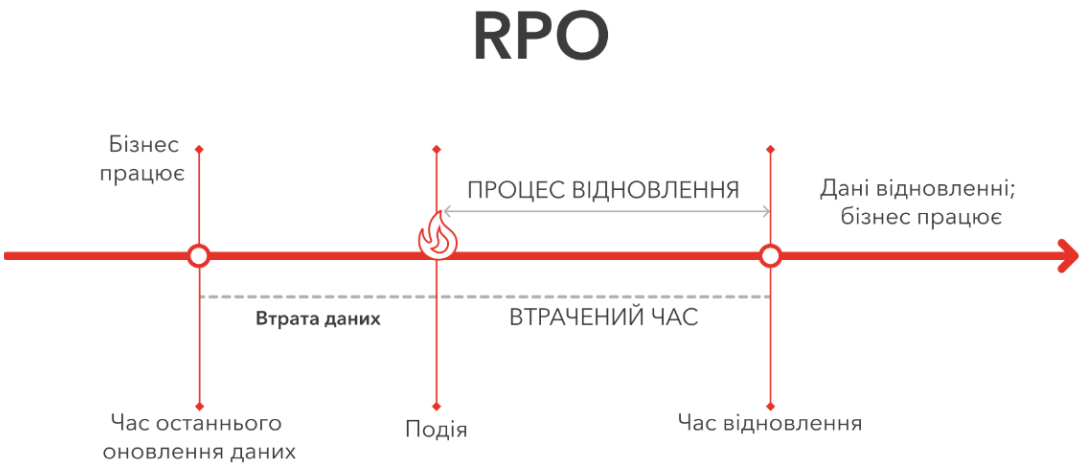

Рис. 1.3. Схема RPO

Як видно на схемі, якщо параметр становить, наприклад, 30 хвилин то у випадок інценденту організація відновить дані, які були створені не більше ніж півгодини до інценденту.

Нижче наведені результати аналізу впливу на бізнес:

- список пріоритетних важливих процесів і пов'язаних з ними взаємозалежностей;
- зареєстровані економічні та виробничі наслідки, спричинені порушенням важливих процесів;
- додаткові ресурси, необхідні для певних критичних процесів;
- можливі простої і відновлення критично важливих процесів і взаємопов'язаних IT.

Дуже часто власники бізнес-процесів навмисно або несвідомо завищують цільове значення критеріїв відновлення, що сприяє спотворенню результатів аналізу і супроводжується необґрунтованими витратами. Щоб обійти цю проблему, потрібно спільно з проєктною командою та зацікавленими сторонами розглянути цінність бізнес-функцій у контексті подій, які вплинули на всю компанію. Такий підхід дозволяє об'єктивно визначити критерії відновлення.

Проведення регулярних вправ та симуляцій для перевірки ефективності BCP та тренування персоналу на випадок кризових ситуацій. Ці заходи дозволяють перевірити наявні плани на практиці, а й забезпечують підготовку

персоналу до дій у реальних кризових ситуаціях. Важливою умовою успіху є систематичний підхід до розробки та реалізації вправ, залучення всіх рівнів організації та детальний аналіз результатів. Завдяки цьому організація може бути впевненою у своїй здатності ефективно реагувати на кризи та забезпечувати безперервність бізнесу за будь-яких умов.

Заходи зменшення ризиків спрямовані на мінімізацію ймовірності виникнення ризиків та їхніх наслідків, тоді як передача ризиків дозволяє знизити негативний вплив за рахунок використання зовнішніх механізмів. Метою оцінки ризиків у рамках управління безперервністю бізнесу є визначення подій, які можуть призвести до порушення діяльності компанії, а також їх наслідків (збитків). Оцінка ризиків забезпечує:

- розуміння потенційних небезпек та впливу їх наслідків на досягнення встановлених цілей компанії;
- розуміння загроз та їх джерел;
- ідентифікацію ключових факторів, що формують ризик; вразливих місць компанії та її систем;
- вибір способів обробки ризику;
- відповідність вимогам стандартів.

Процес оцінки ризиків складається з трьох компонентів (рис. 1.4).

Рис. 1.4. Оцінка ризику

Далі представлено короткий опис кожного кроку:

- ідентифікація ризиків – визначення ймовірних подій, які впливатимуть на здатність установи виконувати завдання і функції для досягнення встановлених мети (місії) та цілей [9]. Метою ідентифікації ризиків є створення списку причин ризиків і загроз, які можуть вплинути на досягнення кожної з встановлених цілей компанії;
- аналіз ризиків – це практика оцінки невизначеностей та управління ними, щоб зменшити їх потенційний вплив на проект [10]. Аналіз ризиків забезпечує вхідні дані для загального процесу оцінки ризиків, прийняття рішень про необхідність управління ризиками, а також визначення відповідних стратегій і методів обробки;
- порівняльна оцінка ризику – це зіставлення рівня ризику з критеріями ризику [11]. Тобто він використовується для визначення типу ризику й його важливості та порівняння його рівня з критеріями, встановленими при визначенні обсягу управління ризиками.

Оцінка майбутніх ризиків дозволить раціонально розробити стратегію забезпечення безперервності бізнесу, а також допоможе визначити оптимальний сценарій її реалізації.

Розробка системи комунікацій для ефективного спілкування зі співробітниками, клієнтами, постачальниками та іншими зацікавленими сторонами під час кризових ситуацій. Вона включає визначення цілей та принципів комунікації, ідентифікацію ключових контактів та ролей, вибір відповідних каналів комунікації, розробку плану комунікацій, а також тренування та тестування. Ефективна комунікація дозволяє знизити рівень паніки, забезпечити узгодженість дій, підтримати довіру зацікавлених сторін та зберегти репутацію компанії.

Розробка та впровадження стратегій відновлення та захисту ІТ підприємства. Вони включають оцінку поточного стану ІТ-систем, розробку превентивних заходів та планів реагування на інциденти, створення планів відновлення після збоїв, навчання персоналу та постійний моніторинг і

вдосконалення. Ефективна реалізація цих стратегій допомагає організації швидко реагувати на кризи, мінімізувати втрати та забезпечити стійкість до різноманітних загроз.

Розробка планів та процедур для забезпечення безперервності роботи персоналу підприємства під час кризових ситуацій. Вони включають оцінку критичних функцій та ролей, розробку планів резервування та гнучких графіків роботи, забезпечення охорони здоров'я та безпеки, розробку процедур реагування на кризи, навчання та підготовку персоналу, а також постійний моніторинг та вдосконалення. Після аналізу вимог до безперервності необхідно вибрати та обґрунтувати можливі технічні та організаційні рішення. У процесі вибору рішення необхідно детально розглянути можливі дії щодо об'єктів, технологій, інформаційних активів, підрядників і партнерів. Ці рішення зазвичай вибираються для наступних цілей:

- захист пріоритетних видів діяльності підприємства;
- ефективне відновлення;
- пом'якшення наслідків інциденту, розробка відповідних і превентивних заходів.

Вибір рішення повинен базуватися на вартості відновлення та вартості простою. До таких рішень відносяться: Дзеркальний, гарячий, "теплий", "холодний", платформа динамічного балансування навантаження, аутсорсинг, мобільна платформа.

Основна відмінність між перерахованими вище рішеннями полягає у вартості, а також терміні відновлення діяльності компанії. Ці рішення допоможуть реалізувати ефективну стратегію забезпечення безперервності бізнесу. Однак для того, щоб визначити найкращий варіант, необхідно вибрати стратегічне рішення, засноване на результатах аналізу впливу на бізнес і оцінки ризиків

Відповідно до найкращих практик, план управління безперервністю повинен складатися з трьох компонентів:

1. Реагування на надзвичайні ситуації – визначає набір дій, які необхідно вжити при виявленні інциденту;

2. Управління інцидентами – визначає, яким чином необхідно скоротити кількість подій;

3. Відновлення активності – визначає набір дій, які необхідно виконати для відновлення служби на певному рівні.

На практиці найчастіше використовуються наступні типи планів:

- план реагування на інциденти – цей тип плану може включати план реагування на кіберінциденти, який є планом реагування на надзвичайні ситуації для ІС. Цей план допоможе зменшити масштаби стихійного лиха і зменшити його наслідки, заощадивши час і отримавши додаткові переваги при використанні інших видів планування;
- план дій персоналу в надзвичайних ситуаціях – закон "Про захист населення і території від надзвичайних ситуацій природного і техногенного характеру" - система організаційних, технічних, медико-біологічних, фінансово-економічних та інших заходів щодо запобігання та реагування на надзвичайні ситуації техногенного та природного характеру і ліквідації їх наслідків [12]. Та другий закон "Про пожежну безпеку"- Цей закон визначає загальні правові, економічні та соціальні основи забезпечення пожежної безпеки на території України, регулює відносини державних органів, юридичних і фізичних осіб у цій галузі незалежно від виду їх діяльності та форм власності [13];
- план аварійного відновлення – орієнтований на відновлення критично важливих ІС. Цей тип планування призначений для підтримки планування безперервності бізнесу та відновлення зручності використання окремих систем та додатків;
- планування безперервності бізнесу – фокусується на підтримці бізнес-процесів в надзвичайних ситуаціях, гарантуючи, що компанія продовжує виконувати найважливіші види діяльності на встановленому прийнятному рівні;
- антикризовий комунікаційний план – цей план допоможе зберегти репутацію компанії в кризових ситуаціях. У ньому прописані процедури

взаємодії зі ЗМІ, правоохоронними органами, Міністерством з надзвичайних ситуацій і т.д.

Встановлення систем моніторингу та оцінки ефективності BCMS та реагування на виявлені відхилення. Ця система повинна включати чітко визначені цілі та показники ефективності, інструменти та процедури моніторингу, процеси збору та аналізу даних, а також механізми реагування на виявлені відхилення. Постійне вдосконалення системи на основі отриманих даних та зворотного зв'язку дозволить організації підтримувати високу ефективність та готовність до кризових ситуацій, забезпечуючи стійкість та довгостроковий успіх.

Стратегічне планування відіграє чималу роль у забезпеченні стійкості організацій у сучасному світі, де загрози для безпеки даних, фінансових ресурсів та репутації постійно зростають. Передбачення потенційних ризиків та розробка стратегій для їх усунення є дуже важливим етапом, який допомагає бізнесу ефективно функціонувати та залишатися конкурентоспроможним у випадку інцидентів або катастроф. Завдяки цьому організації краще можуть захищати свої активи, забезпечувати безпеку своїх клієнтів та партнерів, а також зберігати свою репутацію та конкурентоспроможність у цифровому світі.

Головна функція – це ідентифікація загроз та слабких місць у системі безпеки підприємства. Це може включати в себе аналіз існуючих систем захисту даних, оцінку стійкості до кібератак та інші аспекти, які можуть бути використані зловмисниками для атаки на організацію. Під час цього етапу аудитори зазвичай звертають увагу на відповідність організації регуляторним вимогам та стандартам безпеки, таким як GDPR, HIPAA, PCI DSS тощо.

Далі важливо розробити стратегії та заходи для запобігання цим загрозам. Це може включати в себе впровадження нових технологій захисту, оновлення політик безпеки, навчання персоналу щодо кібербезпеки та інші заходи, спрямовані на зменшення ризиків. Важливо також розробити план відновлення після кібератаки або інциденту безпеки, щоб мінімізувати можливі збитки та відновити нормальне функціонування організації якнайшвидше.

Крім того, стратегічне планування в аудиті безпеки бізнесу також включає в себе постійний моніторинг та оновлення заходів безпеки. Це важливо з урахуванням того, що загрози постійно змінюються, а також з урахуванням того, що технології та підходи до захисту можуть застаріти з часом. Такий підхід дозволяє організації залишатися на шляху до вдосконалення своєї стратегії безпеки та ефективно реагувати на нові виклики.

Плани безперервності бізнесу є важливою складовою аудиту безперервності бізнесу, оскільки вони допомагають організаціям готуватися до та відновлюватися після різних видів кризових ситуацій. Ці плани включають в себе стратегії, процедури та ресурси, необхідні для забезпечення безперервності операцій у випадку непередбачених обставин, таких як природні катастрофи, технічні неполадки, кібератаки та різноманітні інциденти безпеки. Їх розробка та впровадження відображають зобов'язання організації до захисту своїх операцій, ресурсів та стійкості в обличчі можливих загроз.

Першим кроком у розробці BCP є ідентифікація потенційних ризиків, які можуть призвести до збоїв у діяльності організації. Це може включати в себе аналіз історії попередніх подій, оцінку вразливостей систем та інфраструктури, а також оцінку здатності персоналу ефективно реагувати на надзвичайні ситуації.

Після ідентифікації ризиків необхідно розробити конкретні плани дій для реагування на них. Це включає в себе прийняття заходів для забезпечення безпеки персоналу, захисту даних та ІС, забезпечення доступу до необхідних ресурсів, комунікаційні стратегії та інші аспекти, які можуть бути важливими в кризовій ситуації.

Крім того, важливо випробувати та оновлювати плани безперервності бізнесу на регулярній основі. Це дозволяє переконатися, що плани ефективні та відповідають поточним потребам організації, а також дозволяє персоналу підтримувати навички та знання щодо виконання планів у надзвичайних ситуаціях.

Тестування та тренінги в аудиті безпеки бізнесу відіграють важливу роль у забезпеченні ефективності та стійкості організації в обличчі різноманітних загроз та викликів. Ці інструменти дозволяють не лише ідентифікувати потенційні ризики та вразливості, але й навчати персонал ефективно реагувати на них. Тестування та тренінги в аудиті безпеки бізнесу доповнюють один одного, створюючи комплексний підхід до забезпечення безпеки організації.

Тестування безпеки – комплекс досліджень програмного продукту, спрямований на пошук і виявлення дефектів, пов’язаних із збереженням даних користувача [14]. Це може включати в себе тестування на проникнення (пентести), імітацію кібератак, аналіз коду, аудит безпеки мережі та інші методи. Результати такого тестування надають організації можливість виправити виявлені проблеми та посилити свої заходи безпеки.

Тренінги з кібербезпеки, з свого боку, мають на меті навчити персонал ефективно реагувати на потенційні загрози та кібератаки. Це може включати в себе навчання співробітників, як виявляти підозрілу активність, як виконувати процедури безпеки, як реагувати на інциденти та як забезпечити безпеку під час виконання своїх обов'язків. Такі тренінги допомагають збільшити обізнаність персоналу щодо кібербезпеки та знизити ризик ненавмисних порушень безпеки.

Усі ці заходи важливі для ефективної аудиторської діяльності в галузі безпеки бізнесу. Тестування допомагає виявляти ізольовані проблеми та вразливості, а тренінги надають персоналу знання та навички, необхідні для реагування на загрози. Разом вони створюють надійний механізм захисту, який дозволяє організаціям залишатися стійкими та функціонувати ефективно в умовах постійно змінюючогося цифрового середовища.

УВІТ в аудиті безпеки бізнесу є важливою складовою стратегії забезпечення безперервності операцій та стійкості організації в обличчі потенційних загроз та інцидентів.

УВІТ включає в себе плани та процедури для відновлення ІТ та систем після катастрофи або інших непередбачених обставин. Це може включати відновлення даних, відновлення роботи систем та ПЗ, а також відновлення

доступу до мережі та інтернету. УВІТ спрямоване на мінімізацію збоїв у роботі організації та максимізацію відновлення нормального функціонування після інцидентів. Плани відновлення, тестування та постійне оновлення є ключовими елементами успішної програми УВІТ, яка допомагає організаціям залишатися стійкими та надійними в обличчі непередбачених обставин.

Першим кроком у УВІТ є розробка плану відновлення, який включає в себе процедури та вказівки щодо дій персоналу організації у разі інциденту. Це може включати в себе призначення відповідальних осіб, ідентифікацію критичних систем та даних, оцінку термінів відновлення та інші аспекти, необхідні для успішного відновлення.

Другим важливим аспектом УВІТ є тестування та випробування планів відновлення. Це дозволяє переконатися, що плани ефективні та готові до використання у реальних умовах. Тестування може включати в себе симуляції кризових ситуацій, практичні вправи з відновлення та перевірку реагування персоналу на сценарії надзвичайних ситуацій.

Крім того, УВІТ вимагає постійного оновлення та вдосконалення планів відновлення на основі змін у технологічному середовищі та нових загрозах. Це може включати в себе аналіз нових технологій та методів відновлення, внесення змін у процедури та підвищення кваліфікації персоналу.

Моніторинг та оцінка в аудиті безперервності бізнесу є інструментами для забезпечення ефективності, стійкості та безпеки організації в умовах постійно змінюючогося середовища. Ці процеси дозволяють виявляти потенційні ризики, оцінювати ефективність заходів безпеки та реагувати на зміни в обставинах. Ретельний моніторинг та оцінка є ключем до успішного управління безперервністю бізнесу і забезпечують стабільність та безпеку в умовах постійної зміни.

По-перше, моніторинг – це автоматизований процес збору та аналізу показників потенційних загроз безпеці, а потім сортування цих загроз із відповідними діями [15]. Він може включати в себе моніторинг мережевої активності, інцидентів безпеки, використання ресурсів та інших показників, які

вказують на загрози або ризики. Постійний моніторинг дозволяє підприємствам реагувати на потенційні проблеми та ідентифікувати області для покращень.

По-друге, оцінка – це епізодичний аналіз досягнень, пов'язаних із реалізованою програмою або проектом [16]. Він включає в себе оцінку ефективності існуючих стратегій безпеки, ідентифікацію нових ризиків та оцінку їхнього впливу на діяльність підприємства. Оцінка також може включати аналіз реакції на інциденти, ефективність планів відновлення та інші аспекти безпеки.

По-третє, моніторинг та оцінка в аудиті безперервності бізнесу вимагають відповідних інструментів та методів аналізу. Це може включати в себе використання програмних засобів для моніторингу мережі та систем, аналізу даних з різних джерел, проведення аудитів безпеки та інші методи. Важливо мати систематичні та цільові підходи до моніторингу та оцінки, щоб забезпечити повноту та точність аналізу.

Висновки до розділу 1

В розділі було проаналізовано основні принципи безперервності бізнесу в контексті ІБ, а саме: забезпечення кіберстійкості, дублювання (резервування) засобів забезпечення ІБ, мінімізація часу відновлення після інциденту ІБ, системний підхід до управління ризиками, інтеграція з бізнес-стратегією, регулярне тестування та оновлення, навчання та підготовка персоналу, ефективна комунікація, безперервний моніторинг та управління.

Було досліджено переваги впровадження BCMS та виклики, з якими стикаються організації при впровадженні даної системи.

Було проаналізовано нормативну базу та стандарти, які застосовуються у сфері забезпечення безперервності бізнесу, серед яких: ISO 22301, який описує вимоги до впровадження та функціонування BCMS, ISO/IEC 27035, який описує підхід до налаштування процесів управління інцидентами ІБ, які є вагомою частиною забезпечення безперервності бізнесу, ISO/IEC 27005, який пропонує детальні рекомендації щодо управління ризиками ІБ, ISO/IEC 27001, який

встановлює вимоги СУІБ та ISO/IEC 27002, який надає набір рекомендацій та кращих практик управління ІБ.

Було визначено основні компоненти системи забезпечення безперервності бізнесу, а саме: ефективні процеси управління ризиками, управління інцидентами, управління та навчання персоналу, моніторинг, розробка та впровадження УВІТ, проведення тестувань, розробка BCP.

Розділ 2 ДОСЛІДЖЕННЯ МЕТОДИКИ АУДИТУ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

Для досягнення мети дослідження необхідно провести аналіз кроків алгоритму проведення аудиту, визначити критерії, показники, інструменти та техніки, які при цьому застосовуються.

2.1 Аналіз алгоритму аудиту заходів із забезпечення безперервності бізнесу

Аудит заходів із забезпечення безперервності бізнесу передбачає систематичне оцінювання плану забезпечення безперервності бізнесу організації та його ефективності у забезпеченні операційної стійкості. Цей процес має вирішальне значення для виявлення прогалин, забезпечення відповідності стандартам і підвищення загальної готовності організації до збоїв. Методології аудиту забезпечують структурований підхід до оцінки того, чи є впроваджені заходи адекватними і чи функціонують вони за призначенням. У цьому підрозділі розглядаються методики, що використовуються для аудиту заходів з забезпечення безперервності діяльності, з акцентом на їхніх цілях, ключових компонентах та найкращих практиках.

Основними цілями аудиту заходів з забезпечення безперервності діяльності є забезпечення адекватності, ефективності та відповідності BCP. Адекватність передбачає оцінку того, чи охоплює план усі критичні бізнес-функції та потенційні загрози. Ефективність полягає в оцінці того, наскільки добре план працює в реальних умовах, включаючи час реагування та результати відновлення. Відповідність забезпечує узгодженість BCP з відповідними нормативними актами, стандартами та найкращими практиками. Досягаючи цих цілей, аудит допомагає організаціям виявити вразливі місця та сфери для вдосконалення, забезпечуючи надійне управління безперервністю бізнесу.

Аудит безперервності бізнесу зазвичай складається з кількох ключових

компонентів: планування, оцінка, тестування, звітність та подальший моніторинг (рис. 2.1.).

Рис. 2.1. Алгоритм аудиту

Планування передбачає визначення обсягу, цілей та критеріїв аудиту, а також формування команди аудиторів. Етап оцінки включає аналіз документації, проведення інтерв'ю та оцінку існуючих заходів безперервності. Тестування передбачає моделювання різних сценаріїв збоїв для оцінки ефективності роботи BCP. Звітування передбачає документування результатів, висвітлення сильних і слабких сторін та надання рекомендацій (табл. 2.1). Подальші дії забезпечують вирішення виявлених проблем та впровадження коригувальних заходів.

Таблиця 2.1.

Сильні та слабкі сторони аудиту окремих компонентів

Компонент	Сильні сторони	Слабкі сторони
Процеси реагування на інциденти ІБ	Швидка ідентифікація та нейтралізація загроз. Захист даних та збереження конфіденційності.	Можливість пропуску нетипових інцидентів. Висока залежність від швидкості реакції команди.
Процеси оцінки ризиків ІБ	Виявлення потенційних загроз та їх впливу на бізнес. Пріоритизація ризиків для ефективного розподілу ресурсів.	Складність виявлення всіх можливих ризиків. Можливість суб'єктивної оцінки ризиків. Необхідність регулярного оновлення даних про загрози
Процеси управління активами ІБ	Визначення та класифікація важливих активів. Збереження цілісності та конфіденційності даних. Підвищення контролю над ресурсами	Висока складність управління великою кількістю активів. Високі витрати на підтримку та захист активів. Ризик неврахування нових активів Високі витрати на постійне навчання персоналу. Необхідність регулярного оновлення навчальних програм. Ризик недостатньої мотивації персоналу

Продовження таблиці 2.1.

Компонент	Сильні сторони	Слабкі сторони
Процеси навчання та підвищення кваліфікації	Підвищення обізнаності персоналу про загрози ІБ. Покращення реакції на інциденти та зниження ризиків. Формування культури безпеки в організації	Високі витрати на постійне навчання персоналу. Необхідність регулярного оновлення навчальних програм. Ризик недостатньої мотивації персоналу
Процеси моніторингу та виявлення загроз	Рання ідентифікація загроз та попередження інцидентів. Постійний контроль стану безпеки. Можливість швидкого реагування на підозрілі активності	Високі витрати на впровадження та підтримку систем моніторингу. Можливість помилкових спрацьовувань. Необхідність постійного аналізу отриманих даних
Процеси відновлення після інцидентів ІБ	Швидке відновлення критичних процесів. Зниження впливу інцидентів на бізнес. Підтримка довіри клієнтів та партнерів	Висока складність розробки та підтримки планів відновлення. Необхідність регулярного тестування планів. Ризик неврахування всіх можливих інцидентів

Розробка методики проведення аудиту заходів з забезпечення безперервності бізнесу є ключовим етапом для забезпечення ефективності та надійності бізнес-процесів у разі кризових ситуацій. Методики проведення аудиту заходів з забезпечення безперервності бізнесу повинні містити як мінімум шість основниї етапів.

1. Перший етап – планування аудиту, який включає в себе декілька задач: встановлення цілей аудиту, визначення обсягу аудиту та часових рамок.

Встановлення цілей аудиту передбачає опис того, що має бути визначено або перевірено під час аудиту безперервності бізнесу. Прикладами цілей аудиту можуть бути:

- оцінка відповідності стандарту (шляхом перевірки планів та заходів безперервності бізнесу, що до вимог стандарту та нормативних актів);
- ідентифікація та оцінка ризиків (виявляються основні ризики, що загрожують безперервності бізнесу, а також перевіряється ефективність механізмів управління ризиками та заходи мінімізації цих ризиків);
- перевірка готовності та реагування (оцінюється готовність організації та її співробітників до кризових ситуацій чи інциндентів);
- оцінка ефективності BCP (перевірка актуальності BCP та оцінка його ефективності шляхом перевірки результатів навчань персоналу та симуляцій кризових ситуацій);

- аналіз ресурсів та інфраструктури (перевіряється достатність людських ресурсів, технологічних ресурсів та фінансових ресурсів для забезпечення безперервності бізнесу, а також оцінюється стан інфраструктури та IT-систем, які підтримують критичні процеси бізнесу);
- визначення областей для вдосконалення (проводиться пошук слабких місць та областей до яких необхідно привернути увагу та провести їх вдосконалення, а також надаються рекомендації щодо вже впроваджених планів та процедур);
- оцінка системи моніторингу та звітності (проводиться перевірка, як саме здійснюється моніторинг та реалізуються плани безперервності бізнесу, а також оцінюється система звітності та управління інциндентів);
- безперервність ланцюгів постачання (перевіряється чи враховується в планах безперервності ризики з постачальниками або підрядниками).

Визначення обсягу аудиту має на меті розглянути, які процеси, системи та ресурси будуть охоплені аудитом, а також які аспекти безперервності бізнесу будуть перевірені. Це можуть бути процеси, від яких залежить життєдіяльність організації, такі як IT, виробничі потужності, логістика і ланцюги постачання. Визначення обсягу аудиту дозволяє сфокусувати увагу на ключових елементах, що забезпечують безперервність бізнесу, та уникнути надмірного розподілу ресурсів.

Визначення часових рамок аудиту має на меті визначити чіткий проміжок часу, протягом якого буде проведений аудит. Визначений час проведення аудиту дозволяє організувати його процес таким чином, щоб він був ефективним та при цьому не затягувався.

2. Другий етап – збір і аналіз інформації, що стосується BCMS, вимагається стандартами, чи визнана організацією такою, що необхідна для належного функціонування BCMS.

Збір вихідних даних передбачає збір інформації про поточні стратегії, процедури та технології, що використовуються для забезпечення безперервності бізнесу, а у подальшому це допомагає організаціям підготуватися до

непередбачуваних подій та мінімізувати ризики, пов’язаних з надзвичайними ситуаціями.

Також в рамках цього етапу проводиться аналіз документальної бази, який починається з детального вивчення BCP. Аудитори повинні перевірити, чи відповідають ці плани встановленим стандартам та внутрішнім політикам організації. Важливо, щоб плани були актуальними, повними та добре структурованими. Це включає чітко визначені ролі співробітників та їх обов’язки, процедури реагування на різні типи кризових ситуацій, а також інструкції щодо відновлення критичних бізнес-процесів. До цього пункту можна додати необхідність проводити моніторинг та ведення звітності. Вони включають в себе оцінку регулярних звітів про наявний стан BCMS, результати моніторингу виконання планів, а також аналіз інцидентів, що відбулися. Такий аналіз дозволяє зрозуміти, наскільки ефективно здійснюється моніторинг і управління ризиками в організації, та виявити області, де необхідне вдосконалення. Наприклад, регулярний моніторинг може виявити проблеми в системах резервного копіювання даних або недоліки в процедурах відновлення після інцидентів. Після чього необхідно зібрати всі дані та підготувати для аналізу.

Також в рамках даного етапу може бути проведено аналіз ризиків та оцінка потенційних загроз, які можуть виникнути внаслідок кризових ситуацій та непередбачуваних подій.

3. Третій етап – перевірка відповідності та ефективності впроваджених заходів.

Перевірка відповідності дозволяє переконатися, що існуючі заходи забезпечення безперервності відповідають вимогам законодавства, стандартів та внутрішніх політик організації, а також оцінює, наскільки добре організація підготовлена до кризових ситуацій.

Додатково оцінюється ефективність заходів безперервності бізнесу у відновленні операцій після інцидентів та в минулих кризових ситуаціях. Аудитори повинні ретельно вивчити плани безперервності бізнесу, політики,

процедури та інші нормативні документи. Зазвичай для оцінки відповідності використовується стандарт ISO 22301, який встановлює вимоги до BCMS. Відповідність цьому стандарту свідчить про те, що організація має структурований та систематичий підхід до забезпечення безперервності бізнесу.

Також оцінка ефективності включає в себе аналіз результатів навчань та інцидентів, які вже відбувалися в організації. Аудитори повинні вивчити звіти про проведені навчання і симуляції, а також інциденти, з якими стикалася організація. Це дозволяє визначити, наскільки ефективно організація реагує на кризові ситуації, а також виявити, які саме висновки були винесені з попередніх інцидентів та як вони вплинули на вдосконалення заходів з забезпечення безперервності бізнесу.

Також оцінку ефективності можна провести завдяки проведенню інтерв'ю з відповідальним персоналом. Інтерв'ю дозволить отримати уявлення про фактичний стан готовності співробітників та організації до кризових ситуацій, виявити потенційні проблеми та недоліки в поточних процедурах.

Варто також зазначити, що організація повинна мати чітко визначені угоди з постачальниками та партнерами, які включають вимоги щодо безперервності їх діяльності у разі виникнення кризових ситуацій. Аудитори повинні оцінити рівень готовності постачальників до кризових ситуацій та різні аспекти взаємодії з ними у разі виникнення кризових ситуацій.

Також в рамках цього етапу аудитори повинні перевірити, як здійснюється моніторинг систем та реалізується BCP, які характеристики використовуються для оцінки їх ефективності, та як саме організація підготовлена до різноманітних кризових ситуацій. Це включає в себе оцінку регулярних звітів, результатів моніторингу та аналізу інцидентів.

4. Четвертий етап – проведення аудиту та формування висновків.

На цьому етапі проводиться аудит на базі розробленого плану аудиту, використовуючи різні методи дослідження, включаючи огляд документів, інтерв'ю із зацікавленими сторонами та тестування систем та процедур. Проведений аудит дозволяє організаціям оцінити свою готовність до кризових

ситуацій і забезпечити безперебійну роботу у випадку їх виникнення. Обсяг аудиту визначає, які аспекти безперервності бізнесу будуть оцінюватися, наприклад, готовність IT-систем, управління ризиками, взаємодія з постачальниками та партнерами. Планування також включає визначення критеріїв оцінки, таких як відповідність стандартам ISO 22301, а також внутрішнім політикам і процедурам організації.

Після проведення аудиту аудитори повинні зібрати всю необхідну інформацію, проаналізувати отримані дані для оцінки BCMS та сформувати висновки на базі наявних аудиторських доказів. Висновки повинні бути чіткими, обґрунтованими, та можуть включати оцінку загального рівня готовності організації до виявлених слабких місць, або конкретні проблеми, що потребують вирішення.

5. П’ятий етап – розробка рекомендацій та планів вдосконалення (опціонально).

Розробка рекомендацій має на меті підвищити готовність організації до кризових ситуацій та забезпечити безперервне функціонування організації. Шляхом встановлення конкретних рекомендацій щодо покращення систем безпеки та забезпечення безперервності бізнесу. Перед тим, як організації нададуть рекомендації, неохідно провести ретельний аналіз результатів аудиту. Аудиторам необхідно оцінити ефективність вже впроваджених заходів з забезпечення безперервності бізнесу. Наприклад, аналіз може виявити, що організація недостатньо готова до відновлення після кібератак, кіберінцендентів чи природних катастроф, або що існуючі процедури резервного копіювання даних є недостатньо ефективними.

План вдосконалення повинен містити чітко визначені кроки, терміни, власників і необхідні ресурси. Важливо, що план має бути реалістичним і враховувати існуючі можливості організації. Наприклад, впровадження нової технології резервного копіювання даних може потребувати значних фінансових витрат і часу, тому важливо передбачити етапи впровадження та забезпечити необхідні ресурси. Наприклад, для оцінки ефективності впроваджених змін

можна розробити періодичні звіти про виконання програми, проміжні аудити або залучення зовнішніх експертів.

6. Шостий етап – впровадження рекомендацій та моніторинг їх впровадження та підтримки.

Цей етап починається з розробки детального плану дій, який включає конкретні кроки, такі як: терміни виконання, відповідальні особи та ресурси, які будуть необхідні під час виконання цього плану. План повинен враховувати фізичні можливості організації. Наприклад, якщо аудит виявив, що системи резервного копіювання є застарілими, план може включати закупівлю нового обладнання, налаштування нових процесів резервного копіювання та навчання персоналу.

Моніторинг впровадження рекомендацій є критично важливим для забезпечення їх успішної реалізації. Це включає регулярний перегляд прогресу виконання плану, виявлення проблем і коригування дій за необхідності. Для ефективного моніторингу можуть бути використані різні інструменти, такі як звіти про виконання, регулярні наради, контрольні списки і системи управління проєктами.

Розробка методики для проведення аудиту заходів з забезпечення безперервності бізнесу є дуже складним та відповідальним процесом, при цьому це дуже важлива складова стратегії забезпечення ефективності та стійкості бізнесу в умовах непередбачуваних обставин.

2.2 Аналіз методів оцінки ефективності заходів та процедур забезпечення безперервності бізнесу

Оцінка ефективності є важливою частиною управління безперервністю бізнесу. Завдяки їй організації можуть переконатися в тому, що плани і стратегії забезпечення безперервності актуальні, ефективні і готові до реалізації в разі виникнення кризової ситуації. До основних вигод організації від проведеної

оцінки ефективності планів забезпечення безперервності бізнесу можна віднести такі:

- оцінка ефективності допомагає визначити, наскільки плани та стратегії організації підготовлені до можливих кризових ситуацій;
- періодичні оцінки можуть допомогти виявити слабкі сторони та потенційні прогалини в плані безперервності, які потребують вдосконалення;
- оцінка ефективності забезпечує підвищення стійкості організації за рахунок регулярного оновлення та вдосконалення плану забезпечення безперервності;
- оцінка ефективності допомагає забезпечити відповідність внутрішнім політикам організації, галузевим стандартам і нормативним вимогам;
- оцінка ефективності дозволяє зрозуміти, наскільки добре працівники розуміють свої ролі та обов'язки у разі кризи, а також рівень професійної підготовки;
- оцінка ефективності допомагає обґрунтувати необхідність інвестицій у системи безперервності бізнесу та інші відповідні ресурси.

Ключові показники для оцінки ефективсності заходів із забезпечення безперервності бізнесу в конексті ІБ:

MTTR (середній час до ремонту) — це показник, що визначає середній час, необхідний для ремонту пристрою, машини чи системи після відмови [17]. Вираховується за формулою 2.1 [18].

$$MTTR = \frac{\sum t}{n} \tag{2.1}$$

де t – загальний час простою;

n – кількість інцендентів.

Середній час реагування на інциденти ІБ – середній час, необхідний для початку реагування на інцидент після його виявлення. Вираховується за формулою 2.2.

$$t_{avg\_response} = \frac{\sum_{i=1}^{n} t_{i\_response}}{n}, \quad (2.2)$$

де $t_{avg\_response}$ – середній час реагування на інциденти ІБ,

$t_{i\_response}$ – час реагування на i-й інцидент,

n – загальна кількість інцидентів.

Відсоток завершених тестів – процент успішно завершених тестів BCP. Вираховується за формулою 2.3.

$$X = \frac{t}{n} \times 100\% \quad (2.3)$$

де X – відсоток завершених тестів,

t – кількість успішних тестів,

n – загальна кількість тестів.

Оцінка ефективності включає в себе встановлення критеріїв оцінки, аналіз впроваджених заходів, виявлення сильних та слабких сторін і надання рекомендацій для подальшого вдосконалення.

Перед тим. як провести оцінку впроваджених заходів та програм безперервності бізнесу необхідно встановити чіткі критерії оцінки. Критерії повинні бути конкретними, вимірюваними і пов'язаними з цілями безперервності бізнесу. Основні критерії, за якими зазвичай проводять оцінки:

- час відновлення критичних бізнес-процесів (RTO);
- точка відновлення даних (RPO);
- рівень готовності персоналу до кризових ситуацій;
- ефективність комунікаційних процедур під час кризи;
- відповідність нормативним вимогам та стандартам (ISO 22301).

Критерії оцінки слугують орієнтиром для аудиторів, допомагаючи структурувати процес оцінки та забезпечити об'єктивність і точність результатів. Вони дозволяють визначити, наскільки ефективно впроваджені заходи

забезпечують безперервність бізнесу, виявити сильні та слабкі сторони та розробити рекомендації для вдосконалення.

Другим етапом є аналіз впроваджених заходів, який дозволяє визначити сильні та слабкі місця в системі забезпечення безперервності бізнесу. При цьому він допомагає організації оцінити свою готовність до кризових ситуацій, виявити потенційні ризики та розробити рекомендації для їх мінімізації. В результаті аналізу впроваджених заходів можна підвищити ефективність існуючих планів та процесів, забезпечити відповідність нормативним вимогам і досягти кращої підготовленості до можливих криз. Для оцінки ефективності впроваджених заходів необхідно провести всебічний аналіз, що включає в себе перевірку документів та політик, оцінку технічної інфраструктури, проведення тестів та ситуацій, оцінка підготовки персоналу, перевірку відповідності нормативним вимогам:

- перевірка документів та політик включає в себе огляд BCP, процедур відновлення після катастроф, політик резервного копіювання та відновлення даних, а також інструкцій для персоналу на випадок надзвичайних ситуацій. Важливо перевірити, чи відповідають ці документи встановленим стандартам, таким як ISO 22301, та чи є вони актуальними і чи відображають поточні умови бізнесу;
- оцінка технічної інфраструктури включає в себе перевірку систем резервного копіювання, відмовостійкості серверів, мережевої інфраструктури, систем захисту даних тощо;
- проведення тестів та симуляцій надзвичайних ситуацій, які включають в себе тести на відмовостійкість IT-систем, симуляції кібератак та інші сценарії, які зображені в табл. 2.2;
- оцінка підготовки персоналу включає аналіз програм навчання та тренінгів, оцінку знань і навичок співробітників щодо дій у кризових ситуаціях;
- перевірка відповідності нормативним вимогам включає проведення внутрішніх та зовнішніх аудитів для перевірки відповідності встановленим стандартам та вимогам законодавства.

Таблиця 2.2.

Сценарії інцидентів

Вид	Сценарій	Наслідки
Кібератака	Хакери отримали НСД до ІС компанії та поширюють шкідливе ПЗ.	Втрата конфіденційної інформації, зупинка роботи важливих систем, порушення роботи бізнес-процесів.
Природна катастрофа	Регіон компанії став жертвою природної катастрофи, такої як землетрус, повінь або ураган.	Пошкодження фізичних приміщень, переривання постачання електроенергії та інтернету, втрата доступу до даних та обладнання.
Втрата ключового персоналу	Ключовий керівник або спеціалісти компанії несподівано залишають організацію.	Втрата знань і досвіду, збільшення ризику невиконання завдань, нестабільність в роботі бізнес-процесів.
Втрата постачальника	Ключовий постачальник продуктів або послуг банкрутує або припиняє свою діяльність.	Зупинка постачання необхідних ресурсів або матеріалів, затримки в виробництві, втрата довіри клієнтів.
Внутрішній інцидент	Співробітник компанії випадково видалив важливі дані або пошкодив ІС.	Втрата даних, перерва у роботі, ризик втрати довіри клієнтів.

Персонал є ключовим ресурсом будь-якої організації, а його підготовка до дій в критичних ситуаціях має вирішальне значення для забезпечення безперервності бізнесу, оскільки добре підготовлений персонал здатний швидко реагувати на надзвичайні ситуації, що довзоляє мінімізувати збитки та забезпечити швидке відновлення нормальної діяльності організації. Оцінка рівня підготовки дозволяє виявити прогалини в знаннях та навичках співробітників, визначити ефективність навчальних програм та розробити рекомендації для їх вдосконалення. Така оцінка проводиться в декілька етапів:

- аналіз існуючих навчальних програм;
- проведення симуляцій та навчальних тренінгів;
- аналіз комунікаційних процедур;
- оцінка психологічної готовності.

Види тестувань, за якими можна провести перевірку (табл. 2.3):

- табличні вправи (Tabletop Exercises) – симуляція сценарію у вигляді обговорення серед ключових осіб організації;
- симуляційні навчання (Simulation Exercises) – відтворення конкретного інциденту для перевірки плану у реальних умовах;

- повномасштабні тестування (Full-Scale Testing) – комплексне тестування, що включає всіх співробітників та системи організації;
- тестування на місці (On-Site Testing) – відтворення сценарію на конкретному об'єкті, де розміщені критичні системи.

Таблиця 2.3.

Основні методи та їх характеристика

Назва	**Мета**	**Процес**	**Переваги**	**Недоліки**
Табличні вправи	Перевірка теоретичних знань та обговорення дій у разі кризи.	Учасники збираються для обговорення сценаріїв кризових ситуацій, проходять план дій крок за кроком.	Можливість виявити теоретичні недоліки без реальних витрат ресурсів.	Обмежена практична перевірка, учасники можуть недооцінювати реальність ситуації.
Функціональні вправи	Перевірка конкретних аспектів BCP, таких як IT-відновлення або евакуація.	Виконання практичних завдань, що симулюють окремі компоненти кризової ситуації.	Практична оцінка окремих елементів плану.	Може не охоплювати всі аспекти безперервності бізнесу.
Повномаштабні симуляції	Комплексна перевірка всієї системи безперервності бізнесу.	Повномасштабне моделювання кризової ситуації з участю всіх підрозділів і систем.	Виявлення всіх можливих недоліків у реальних умовах.	Високі витрати часу та ресурсів, можливий вплив на реальні бізнес-процеси.

Моніторинг та звітність також є важиливими складовими процесу оцінки ефективності впроваджених заходів забезпечення безперервності. Моніторинг забезпечує безперервне спостереження за виконанням заходів безперервності бізнесу, дозволяючи своєчасно виявляти потенційні проблеми та реагувати на них. Звітність, в свою чергу, надає керівництву об’єктивну інформацію про стан програм та BCP, про ефективність впроваджених заходів та прогрес у досягненні стратегічних цілей. Разом вони забезпечують прозорість процесів, підвищують відповідальність і сприяють постійному вдосконаленню організації.

Для ефективного моніторингу насамперед необхідно встановити ключові показники ефективності (KPIs), які відображають успішність заходів безперервності бізнесу. KPIs повинні бути конкретними, вимірюваними, досяжними та обмеженими в часі.

Так само моніторинг передбачає регулярний збір даних про виконання заходів безперервності. Він може включати дані про функціонування IT-систем, результати тестів та симуляцій, зворотній зв'язок від співробітників, інформацію про інциденти та відхилення від планів. Регулярний збір даних допомагає отримати актуальну інформацію про стан систем та своєчасно виявляти проблеми.

Зібрані дані потребують ретельного аналізу для виявлення трендів, відхилень та можливих проблем. Вони включають в себе порівняння фактичних результатів з встановленими KPIs, проведення аналізу причин відхилень та оцінку впливу інцидентів на безперервність бізнесу. Аналіз дозволяє зрозуміти, наскільки ефективні впроваджені заходи та де саме необхідні покращення.

Звітність є ключовим інструментом для інформування керівництва про результати моніторингу та аналізу. Звіти повинні бути чіткими, структурованими та містити всю необхідну інформацію для прийняття оптимальних рішень. Вони можуть включати в себе інформацію про стан виконання BCP, результати пройдех тестів, виявлені проблеми, рекомендації для вдосконалення та інші важливі аспекти.

На основі отриманих результатів моніторингу та звітів необхідно впроваджувати рекомендації для вдосконалення програм безперервності бізнесу. Рекомендації можуть включати в себе: оновлення планів, проведення додаткових тренінгів, впровадження нових технологій або зміну процедур. Дуже важливо зазначити, що всі рекомендації повинні бути враховані та реалізовані вчасно.

Після впровадження рекомендацій необхідно оцінити їх ефективність. Оцінка ефективності включає проведення повторних тестів, аналіз їх результатів та порівняння їх з попередніми даними. Оцінка ефективності дозволяє

визначити, наскільки впроваджені заходи сприяли вдосконалення безперервності бізнесу та чи досягнуто поставлених цілей.

Моніторинг та звітність повинні бути безперервним процесом, спрямованим на постійне вдосконалення, та повинен включати в себе регулярний перегляд планів, аналіз нових ризиків, оновлення навчальних програм та впровадження нових технологій. Постійне вдосконалення забезпечує актуальність та ефективність програм безперервності бізнесу в довгостроковій перспективі.

Оцінка відповідності нормативним вимогам допомагає організаціям впевнитися в тому, що їхні плани, процедури та політики відповідають чинним законодавчим та регуляторним вимогам. Відповідність нормативним вимогам забезпечує додатковий рівень надійності та правомірності впроваджених заходів, знижує ризики правових наслідків та покращує загальну репутацію організації. Крім того, відповідність стандартам допомагає організаціям досягти високих рівнів ефективності та готовності до кризових ситуацій.

Ще одним методом оцінки ефективності заходів та планів забезпечення безперервності бізнесу є проведення внутрішніх і зовнішніх аудитів для перевірки відповідності програм безперервності бізнесу встановленим стандартам. Внутрішні аудити можуть проводитися внутрішнім відділом аудиту або залученими спеціалістами та дозволяють проводити регулярну перевірку процесів та процедур, виявляти відхилення та розробляти коригуючі заходи. Результати внутрішніх аудитів допомагають вчасно виявляти проблеми та забезпечувати відповідність нормативним вимогам.

Зовнішні аудити надають об'єктивну оцінку та підтвердження відповідності встановленим стандартам. Результати зовнішніх аудитів можуть використовуватися для сертифікації організації за міжнародними стандартами, такими як ISO 22301, що підвищує репутацію організації та довіру з боку клієнтів й партнерів.

Результати внутрішніх та зовнішніх аудитів потребують ретельного аналізу, який включає в себе оцінку виявлених невідповідностей, аналіз причин

їх виникнення та розробку рекомендацій для їх усунення. Важливо визначити пріоритетні заходи для покращення та розробити план дій для забезпечення відповідності нормативним вимогам у майбутньому.

Необхідно також зазначити, що необхідний постійний моніторинг змін у законодавстві та нормативних актах, що стосуються безперервності бізнесу, і внесення необхідних корективів у відповідні політики та процедури.

Постійне вдосконалення спрямоване на безперервне підвищення ефективності процесів та процедур, що використовуються для забезпечення безперервності бізнесу. Воно дозволяє організаціям своєчасно виявляти та усувати слабкі місця, впроваджувати нові технології та методи управління ризиками, підвищувати кваліфікацію персоналу.

Як окремі рішення для забезпечення безперервності бізнесу слід виділити такі інструменті, як Enterprise Risk Management (ERM) Systems дозволяють компаніям оцінювати, контролювати та звітувати про ризики, пов'язані з безперервністю бізнесу, Business Continuity Management (BCM) Software допомагають компаніям розробляти, впроваджувати та керувати планами безперервності бізнесу, Incident Management Systems дозволяють компаніям реєструвати, відстежувати та керувати інцидентами, які можуть вплинути на безперервність їх бізнесу, Monitoring and Alerting Tools дозволяють компаніям встановлювати моніторингові точки в їхній інфраструктурі та програмному забезпеченні для виявлення аномальної активності або потенційних проблем, Reporting and Dashboarding Tools дозволяють компаніям візуалізувати дані про безперервність бізнесу через звіти, графіки та інші графічні елементи.

2.3 Дослідження особливостей застосування інструментів та технік аудиту

Аудит заходів забезпечення безперервності бізнесу передбачає використання різноманітних інструментів і методів для оцінки ефективності, результативності та відповідності плану забезпечення безперервності бізнесу

організації. Ці інструменти та методи допомагають аудиторам систематично оцінювати, чи можуть впроваджені заходи належним чином захистити від збоїв та забезпечити швидке відновлення. У цьому підрозділі розглядаються ключові інструменти та методи, що використовуються в процесі аудиту, а також висвітлюються особливості їх застосування та переваги.

Автоматизовані інструменти аудиту, програмні рішення для забезпечення безперервності бізнесу (спеціалізовані інструменти, призначені для підтримки планування, управління та аудиту заходів з безперервності бізнесу) часто включають такі функції, як модулі оцінки ризиків, інструменти аналізу впливу на бізнес (BIA) та можливості управління інцидентами. Прикладами можуть слугувати такі програмні продукти, як Fusion Risk Management, Archer Business Continuity Management та MetricStream. Ці інструменти допомагають аудиторам оцінити надійність планів забезпечення безперервності бізнесу, перевірити ефективність впроваджених заходів і забезпечити відповідність стандартам і вимогам регуляторів.

Існує 5 основних технік для оцінки та перевірки рівня готовності:

- аудит на основі чек-листів, який полягає в використанні стандартизованих чек-листів або шаблонів, які містять питання або критерії оцінки для перевірки різних аспектів системи безперервності бізнесу;
- інтерв’ю з ключовими працівниками та відповідальними особами організації, які дозволяють отримати інформацію про процеси, процедури та практики безперервності бізнесу;
- опитування, які в більшості випадків передбачають розсилку анкет або опитувальників працівникам організації для збору даних про їхнє розуміння процедур та практик безперервності бізнесу;
- моделювання, яке передбачає використання спеціалізованих програмних засобів для створення моделей або симуляцій сценаріїв кризових ситуацій для оцінки реакції організації та її готовності до таких подій;
- тестування, тобто проведення спеціальних вправ або симуляцій подій для перевірки ефективності BCP у реальних умовах.

Всі перераховані вище техніки поділяються на кількісні, якісні та перевірку документацій та політик:

- кількісні методи оцінки базуються на кількісних даних та числових показниках. Наприклад, кількість часу, яка потрібна для відновлення після перерви в роботі, або кількість системних збоїв протягом певного періоду. Головна перевага цих методів – це об’єктивність, але недолік –неможливість якісно зафіксуівти складні аспекти;
- якісні методи оцінки базуються на якісних характеристиках, таких як якість процесів, процедур та культури безпеки в організації, наприклад, оцінка ефективності комунікаційної системи під час кризових ситуацій. Перевага цього методу полягає в якісній оцінка складних аспектів бізнесу, недолік – у неможливості кількісної інтерпретації;
- перевірка документації включає аналіз документації (плани безперервності бізнесу, політики безпеки, звіти про тестування, результати внутрішніх аудитів тощо) і дозволяє оцінити відповідність вимогам та стандартім, але їм важко перевіряти великі обсяги документації.

Вимоги українських та міжнародних стандартів внутрішнього та зовньошнього аудиту передбачають під час проведення аудиту застосування різноманітних прийомів, методів та процедур, які аудитори обирають, опираючись на поставлене завдання. Їх вибір залежить від багатьох факторів, таких як: зазначені цілі, від самих об’єктів зовньошнього та внутрішнього аудиту, від навичок та стажу аудиторів, наявних даних тощо.

У методах міжнародних науковців велика увага приділяється дослідженню методів, прийомів і засобів аудиту. Однак не зважаючи на їхні зусилля на сьогоднішній день немає єдиного підходу до визначення понять методів, його головних елементів, прийомів аудиту та аудиторських процедур. Тому на практиці вітчизняні та міжнародні експерти часто не розрізняють методики аудиту від прийомів та засобів аудиту, вважаючи, що це одне й те саме.

Метод в аудиті це сукупність прийомів, за допомогою яких досліджується стан об'єкт аудиту (табл. 2.4).

Таблиця 2.4.

Назва та суть методів внутрішнього аудиту

Назва методу	Опис
Вивчення	Перевірка документів і записів про матеріальні активи. Це дозволяє отримувати докази різного ступеня достовірності ,яий залежить від їх характеру та джерел.
Спостереження	Візуально контролювати хід виконання операцій процедур, щоб визначити фактичний спосіб їх виконання. Він широко використовується внутрішніми аудиторами при вивченні систем внутрішнього контролю.
Опитування	Пошук офіційних та неофіційних доказів, як усних, так й письмових, від особи, відповідальної за діяльність. Це може бути зроблено шляхом проведення інтерв'ю та анкетування.
Підтвердження	Отримання аудитором письмової відповіді для підтвердження вже наявної інформації.
Підрахунок	Перевірка арифметичної точності записів.
Аналітичний огляд	Внутрішній аудит й вивчення важливих коефіцієнтів, тенденцій і інших даних, що характеризують стан об'єкта.

Проведення аудиту заходів безперервності бізнесу є важливим кроком у забезпеченні стійкості та надійності діяльності організації. Для цього використовуються різноманітні інструменти та техніки, які спрямовані на оцінку, аналіз та вдосконалення систем безпеки й безперервності бізнес-процесів. Зазвичай використовують шість основних методів: структуровані аудиторські питання, аналіз документації, тестування та симуляції, технічне аудитування, оцінка ризиків, оцінка відповідності.

1. Структуровані аудиторські питання, що передбачає розробку набору запитань, спрямованих на перевірку виконання процедур безпеки та безперервності, таких як наявність резервних копій даних, регулярне тестування планів відновлення, а також дотримання персоналом політик безпеки. Ці питання є інструментом для систематичної оцінки ефективності та відповідності бізнес-процесів і заходів, спрямованих на забезпечення безперервності діяльності організації, й допомагають аудиторам зібрати необхідну інформацію, оцінити поточний стан BCMS та виявити потенційні недоліки або області для вдосконалення. Вони можуть бути спрямовані на політики безперервності бізнесу, оцінку ризиків та аналіз впливу, BCP, персоналу (тренування, навчання), моніторинг тощо. Вони допомагають аудиторам зібрати детальну інформацію про поточний стан BCP, виявити потенційні недоліки та розробити рекомендації щодо їх усунення. Використання структурованих питань забезпечує високий

рівень точності та об'єктивності в оцінці ефективності BCMS, що є критично важливим для підтримання стабільності та стійкості організації в умовах кризових ситуацій.

2. Аналіз документації дозволяє оцінити відповідність і ефективність розроблених планів, політик та процедур з забезпечення безперервної діяльності організації. Він включає в себе систематичний перегляд, оцінку та верифікацію всіх наявних документів, що стосуються безперервності бізнесу, з метою виявлення можливих прогалин, недоліків та областей для вдосконалення. Проведений аналіз документації дозволяє:

- переконатися, що документи відповідають внутрішнім політикам організації, нормативним вимогам та галузевим стандартам;
- перевірити, чи містять документи всі необхідні елементи та чи є вони точними, актуальними та відповідними реальним умовам;
- виявити потенційні прогалини, недоліки або суперечності в документації, які можуть негативно вплинути на ефективність заходів безперервності бізнесу;
- на основі аналізу документів розробити рекомендації щодо їх покращення та оновлення.

Ключовими етапами аналізу документації є збір документів, перевірка їх цілісності, оцінка змісту, виявлення недоліків та розробка рекомендацій. Аналіз документації забезпечує об'єктивну оцінку відповідності та ефективності розроблених планів і процедур, допомагає виявити потенційні недоліки та розробити рекомендації для їх усунення. Систематичний та детальний підхід до аналізу документації дозволяє забезпечити високий рівень готовності організації до кризових ситуацій та підтримати її стабільну роботу в умовах невизначеності.

3. Тестування та симуляції в аудиті заходів безперервності бізнесу є важливими інструментами, що дозволяють перевірити ефективність та готовність планів і процедур, розроблених для забезпечення безперервності діяльності організації в умовах кризових ситуацій. Ці процеси забезпечують реалістичну оцінку можливостей компанії реагувати на надзвичайні ситуації та

відновити свою роботу в найкоротші терміни. Основні цілі тестування та симуляцій включають в себе такі:

- оцінка, наскільки добре плани безперервності бізнесу і плани відновлення після аварій здатні забезпечити безперервність бізнес-процесів;
- виявлення слабких місць в існуючих планах і процедурах, які можуть перешкоджати ефективному реагуванню на надзвичайну ситуацію;
- забезпечення підготовки персоналу до дій у надзвичайних ситуаціях, підвищення їхньої обізнаності та навичок;
- перевірка здатності різних відділів і команд ефективно взаємодіяти та координувати свої дії під час кризи;
- отримання даних для вдосконалення та оновлення планів і процедур на основі реальних результатів тестування.

4. Технічне аудитування включає всебічний аналіз і оцінку технологічних аспектів, які забезпечують безперервну роботу організації під час кризових ситуацій. Вона включає перевірку IT-систем, інфраструктури, безпеки даних, а також планів відновлення після аварій. Основна мета технічного аудитування – виявлення технічних недоліків і розробка рекомендацій щодо їх усунення, щоб забезпечити стабільну роботу критичних бізнес-процесів. Основні компоненти технічного аудитування включають в себе такі:

- IT-інфраструктура, тобто перевірка стану апаратного забезпечення, його надійності та відповідності вимогам безперервності бізнесу. Також сюди можна віднести аналіз мережевої інфраструктури для виявлення потенційних недоліків та вразливостей;
- системи зберігання та резервного копіювання даних, тобто перевірка регулярності, надійності та безпеки процедур резервного копіювання та перевірка здатності відновлення даних з резервних копій у передбачений час;
- плани відновлення після аварій, тобто перевірка того, чи розроблені та задокументовані плани відновлення після аварій для всіх критичних систем організації, а також проведення тестів і симуляцій для оцінки ефективності планів відновлення;

- IT-безпека, тобто оцінка наявності та ефективності засобів захисту інформації, таких як антивірусні програми, міжмережеві екрани та системи виявлення вторгнень, а також оцінка відповідності IT-систем і процесів стандартам безпеки, таким як ISO/IEC 27001;
- віртуалізація та хмарні технології, тобто перевірка ефективності та надійності використання віртуалізаційних технологій для забезпечення безперервності бізнесу, а також перевірка надійності та безпеки хмарних рішень, що використовуються для зберігання даних і додатків.

5. Оцінка ризиків дозволяє виявити, проаналізувати та оцінити потенційні ризики, які можуть вплинути на здатність організації підтримувати безперервну діяльність під час кризових ситуацій. Оцінка ризиків спрямована на виявлення слабких місць, загроз і вразливостей, а також на розробку стратегій для їх мінімізації або усунення (рис. 2.2).

Рис. 2.2. Основні етапи оцінки ризиків

Методи оцінки ризиків можна умовно розділити на три категорії:

- кількісні методи, що базуються на використанні математичних моделей для оцінки ймовірності виникнення ризиків та їхнього впливу. До цих методів також відноситься оцінка потенційних фінансових втрат від реалізації інцидентів;
- якісні методи, які базується на збірці думок та оцінок експертів щодо ймовірності та впливу ризиків. Ці методи часто використовуються для визначення сильних і слабких сторін організації, можливостей для вдосконалення і виявлення актуальних загроз;
- сценарний аналіз, який базується на моделювані можливих сценаріїв розвитку подій для оцінки потенційних наслідків реалізації різних сценаріїв.

6. Оцінка відповідності в аудиті заходів безперервності бізнесу стосується перевірки того, наскільки процеси, політики, процедури та практики організації відповідають встановленим стандартам, регуляторним вимогам, внутрішнім політикам та найкращим практикам. Цей процес є критично важливим для забезпечення того, що організація здатна ефективно реагувати на кризи та підтримувати безперервність бізнесу (рис. 2.3).

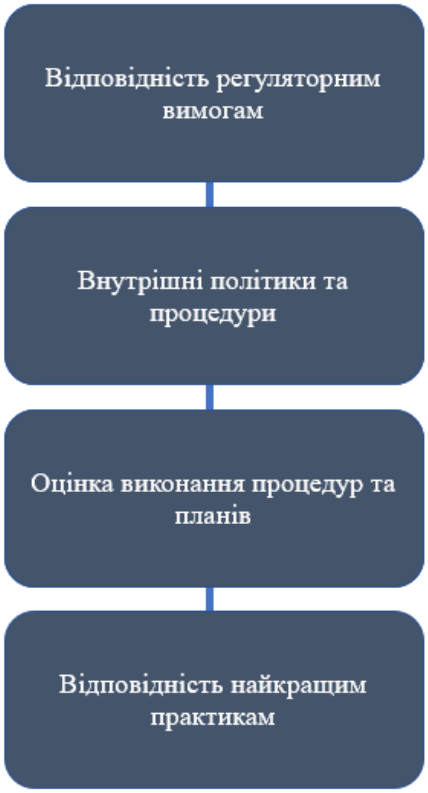

Рис. 2.3. Основні аспекти оцінки відповідності

Процес оцінки відповідності складається з п’яти основних етапів, вони продемонстровані на рис. 2.4.

Рис. 2.4. Процес оцінки відповідності

Проаналізовані інструменти та техніки допомагають аудиторам отримати об'єктивну інформацію про стан систем безперервності бізнесу, виявити можливі ризики та недоліки та розробити рекомендації для подальших покращень.

Комбінація різних підходів дозволяє забезпечити широкий та глибокий аналіз стійкості та надійності бізнесу у випадку непередбачуваних обставин.

Висновки до розділу 2

В розділі проаналізовано алгоритм проведення аудиту заходів з забезпечення безперервності бізнесу, який складається з таких етапів: планування, збір інформації, оцінка ризиків, проведення аудиту, виявлення недоліків, розробка рекомендацій, звітність, моніторинг та впровадження.

Проаналізовано перешкоди, які можуть виникнути при аудиті окремих компонентів BCMS, зокрема, для управління інцидентами ІБ, навчання персоналу, процесів реагування на інциденти ІБ, процесів оцінки ризиків ІБ, процесів управління активами ІБ, процесів навчання та підвищення кваліфікації, процесів моніторингу та виявлення загроз, процесів відновлення після інцидентів ІБ.

Проаналізовано методи оцінки ефективності заходів та планів забезпечення безперервності бізнесу, зокрема, досліджено такі показники ефективності в контексті ІБ, як MTTR (середній час відновлення), середній час реагування на інциденти ІБ, відсоток завершених тестів.

Досліджено інструменти, які використовуються організаціями для підтримки та оцінки процесів забезпечення безперервності бізнесу, зокрема, Enterprise Risk Management, Business Continuity Management, Incident Management Systems, Monitoring and Alerting Tools, Reporting and Dashboarding Tools.

Досліджено особливості застосування інструментів та технік аудиту, а саме: аудит на основі чек-листів, інтерв’ю з ключовими працівниками та відповідальними особами організації, опитування, моделювання, тестування, проаналізовано особливості проведення внутрішнього аудиту методами вивчення, спостереження, опитування, підтвердження, підрахунку, аналітичного огляду.

Розділ 3 ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АУДИТУ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

3.1 Аналіз поточного стану системи управління безперервністю бізнесу

Аналіз поточного стану BCMS дозволяє організації зрозуміти, наскільки вона готова до можливих збоїв та кризових ситуацій. Цей процес забезпечує комплексну оцінку наявних планів, процедур, ресурсів та готовності персоналу до реагування на непередбачені події. Результати аналізу допомагають виявити слабкі місця та розробити заходи для їх усунення, що підвищує загальну ефективність BCMS та знижує ризики для організації. Існує вісім основних етапів проведення аналізу поточного стану (рис. 3.1), але компанії можуть збільшити їх за потребою.

Рис. 3.1. Алгоритм проведення аналізу

Першим етапом аналізу є збір інформації про поточний стан BCMS. Це включає огляд наявних BCP, процедур відновлення після катастроф, політик резервного копіювання та відновлення даних, інструкцій для персоналу, а також

результати попередніх аудитів та тестів. Інформацію можна збирати шляхом опитувань, анкетування, інтерв'ю з ключовими співробітниками та аналізу документації.

Другим етапом аналізу є оцінка ризиків. Оцінка ризику – це процес, який використовується для визначення потенційних небезпек і аналізу того, що може статися, якщо станеться лихо чи небезпека [32]. Вона включає ідентифікацію можливих загроз для безперервності бізнесу, оцінку ймовірності їх виникнення та потенційного впливу на організацію. Це дозволяє визначити пріоритетні області для вдосконалення та розробити заходи для зменшення ризиків. Оцінка ризиків може включати аналіз внутрішніх і зовнішніх загроз, таких як технічні збої, природні катастрофи, кібератаки, людські помилки та інші.

Існує безліч небезпек, які необхідно враховувати, і кожна небезпека може мати безліч можливих сценаріїв розвитку.

Можна використовувати інструменти оцінки ризиків для завершення оцінки ризиків. За допомогою цього інструменту можна визначити небезпеки та ризики, які найімовірніше можуть призвести до серйозних травм або пошкоджень.

Проводячи оцінку ризику, зверніть увагу на вразливі місця, які можуть зробити ваш бізнес вразливим до шкоди від небезпечних факторів. Вразливі місця включають дефекти в конструкції, технічних системах, системах безпеки та програмах запобігання втратам. Вони сприяють збільшенню шкоди при виникненні інциденту.

Третім етапом є проведення детального аналізу існуючих планів та процедур безперервності бізнесу. Він включає в себе оцінку їхньої відповідності найкращим практикам та стандартам, таким як ISO 22301, а також їхньої здатності забезпечити ефективне реагування на кризові ситуації. Важливо оцінити, наскільки детально розроблені плани, чи охоплюють вони всі критичні процеси та ресурси, чи містять вони чіткі інструкції для персоналу та чи враховують можливі сценарії розвитку подій.

Четвертим етапом аналізу є перевірка готовністі персоналу до кризових ситуацій. Оцінка готовності включає аналіз навчальних програм, проведених тренінгів та симуляцій, рівня обізнаності співробітників про свої ролі та обов'язки в разі кризових ситуацій. У разі виникнення кризи організація повинна бути готова швидко і ефективно відреагувати, щоб звести її наслідки до мінімуму. Наявність надійного плану і протоколу антикризового управління важливо, але не можна недооцінювати роль залучення персоналу в антикризове управління. Для того, щоб співробітники були добре підготовлені і могли впевнено справлятися з кризовими ситуаціями, необхідно навчати співробітників практичним сценаріям кризових ситуацій за допомогою таких вправ, як тренінг із забезпечення готовності до надзвичайних ситуацій (ECP). Участь персоналу в навчаннях з антикризового управління допомагає підвищити обізнаність і розуміння потенційних криз, з якими може зіткнутися організація. Активно залучаючи співробітників до практичних сценаріїв, вони можуть зрозуміти типи криз, які можуть виникнути, їх потенційні наслідки та дії, необхідні для їх пом'якшення. Ці знання дозволяють працівникам розпізнавати попереджувальні знаки, адекватно реагувати та ефективно брати участь у кризових зусиллях. Наприклад, під час навчань ECP співробітники можуть змоделювати сценарій кібератаки. Активно беручи участь у тренінгу, ви дізнаєтеся про різні тактики, які можуть використовувати хакери, включаючи фішингові електронні листи та програми-вимагачі. Також необхідно моделювати кризові сценарії, завдяки ним організації можуть виявляти прогалини і слабкі сторони в плануванні і вносити необхідні поліпшення. Цей повторюваний процес гарантує, що план антикризового управління є надійним, оновлюється та узгоджується з цілями організації. Ці знання дозволяють працівникам виявляти підозрілі дії та повідомляти про них, мінімізуючи ризик успішної кібератаки. Бо дуже важливо оцінити, наскільки персонал підготовлений до швидкого та ефективного реагування на надзвичайні ситуації, чи є у нього необхідні навички та знання.

П’ятим етапом аналізу є проведення тестів та симуляцій. Проведення тестів та моделювання є важливим п'ятим етапом аналізу існуючих планів та

процедур безперервності бізнесу. На цьому етапі можна не тільки підтвердити практичну ефективність розробленого документа, а й підвищити готовність організації до можливих кризових ситуацій. Тестування та моделювання відіграють важливу роль у виявленні дефектів, які можуть бути пропущені при теоретичному аналізі.

Тестування BCP бізнесу включає в себе реалізацію контрольованих заходів, що імітують реальні кризові ситуації. Сюди входять різні сценарії, такі як відключення електроенергії, кібератаки, стихійні лиха та інші незвичайні події. Основна мета тестування-побачити, як організації можуть швидко та ефективно відновити критичні бізнес-процеси та мінімізувати втрати. Проводячи такі тести, ви можете оцінити, чи достатньо детальний план, чи містить він усі необхідні інструкції та чи здатний персонал їх зрозуміти.

Моделювання кризових ситуацій дозволяє створити найбільш реалістичні умови для перевірки готовності співробітників і їх здатності діяти відповідно до розроблених процедур. При моделюванні важливо задіяти різні підрозділи організації для оцінки взаємодії між ними і перевірки ефективності каналів комунікації. Це допоможе виявити слабкі місця в координації і забезпечити чітке розуміння всіма учасниками своїх ролей і обов'язків в кризових ситуаціях. Моделювання також допомагає підвищити обізнаність співробітників про можливі загрози та способи їх подолання. Це ключовий фактор підготовки вашої організації до реальних інцидентів.

Тестування і моделювання не обмежуються разовими заходами. Це повинен бути регулярний процес, що дозволяє адаптувати BCP до змін у внутрішньому і зовнішньому середовищі організації. Зміни в технології, бізнес-структурі, законодавстві чи ринкових умовах можуть вимагати коригування існуючих планів. Регулярне тестування забезпечує актуальність і ефективність плану, а також постійне вдосконалення процедури.

Результати тестування та моделювання повинні бути задокументовані та детально проаналізовані. Важливо не тільки фіксувати успіхи, а й виявляти проблемні точки і визначати причину можливих збоїв. Аналіз результатів

дозволяє не тільки розробити рекомендації щодо вдосконалення планування і процедур, а й поліпшити навчання персоналу. Важливо, щоб результати тестування обговорювалися на рівні керівництва організації, що допомагає приймати обґрунтовані рішення про подальші дії.

Крім того, результати тестування можуть бути використані для навчання персоналу. Проведення тренінгів на основі реальної ситуації, що сталася під час моделювання, може підвищити рівень підготовки співробітників і їх здатність реагувати на непередбачувані події. Це сприяє формуванню культури забезпечення безперервності бізнесу в організації і підвищує стійкість до кризових ситуацій.

Шостим етапом аналізу є перевірка результатів тестів та симуляцій оскільки вони потребують ретельного аналізу для виявлення слабких місць та недоліків у BCMS. Важливо оцінити, наскільки ефективно виконувалися плани та процедури, які проблеми виникали під час тестування, які заходи були успішними, а які потребують вдосконалення. Аналіз результатів дозволяє розробити конкретні рекомендації для покращення BCMS.

Кожне тестування та моделювання створюють унікальне середовище, де ви можете протестувати різні аспекти свого BCP. Після завершення цих заходів важливо ретельно проаналізувати всі дані, отримані в ході тестування. Це включає в себе збір відгуків від учасників, оцінку часу реагування на інциденти, виявлення затримок і проблем при виконанні процедур і аналіз ефективності взаємодії між різними підрозділами організації.

Одним з ключових аспектів перевірки результатів є виявлення слабких місць в плануванні і процедурах. Це можуть бути як технічні, так і організаційні питання. Наприклад, в тестах деякі інструкції недостатньо докладні, незрозумілі персоналу, певні ресурси недоступні в потрібний час, а аналіз також може свідчити про те, що канали зв'язку між різними підрозділами функціонують неефективно, що призводить до затримок в прийнятті рішень і здійсненні необхідних дій.

Перевірка результатів також може допомогти виявити недоліки в навчанні персоналу. Якщо працівник не знає своєї ролі або не знає, як діяти в кризовій ситуації, це буде виявлено під час тестування. Таке виявлення дає організації можливість провести додаткові навчання і тренінги для поліпшення підготовки персоналу до надзвичайних ситуацій.

Іншим важливим аспектом є оцінка ресурсів і технологій, що використовуються в BCP. Результати тестування можуть свідчити про те, що певні технічні рішення є ненадійними або недостатньо ефективними. Це може вимагати перегляду та оновлення технічної підтримки, впровадження нових інструментів або зміни підходу до управління ресурсами.

Після завершення перевірки результатів тестування та моделювання Вам слід створити детальний звіт із усіма виявленими проблемами та рекомендаціями щодо їх усунення. Цей звіт необхідно представити керівництву організації для прийняття обґрунтованих рішень щодо вдосконалення BCMS. Важливо, щоб процес аналізу результатів був прозорим і включав усі зацікавлені сторони, щоб забезпечити всебічне розуміння проблем та спільну розробку рішень.

Сьомим етапом аналізу є розробка рекомендацій для покращення BCMS на основі результатів аналізу. Вони можуть включати оновлення планів та процедур, впровадження нових технологій, проведення додаткових тренінгів для персоналу, зміну політик та процесів. Важливо, щоб рекомендації були конкретними, досяжними та враховували реальні можливості організації. При аналізі результатів тестів і симуляцій і перегляді BCP виявляються різні недоліки, недоліки і можливі шляхи поліпшення. На основі цих висновків були розроблені конкретні рекомендації, спрямовані на вдосконалення BCMS. Рекомендації включають в себе різні аспекти, такі як оновлення планів і процедур, вдосконалення каналів комунікації, підвищення обізнаності персоналу, поліпшення технічної підтримки, впровадження нових технологій і розширення охоплення критично важливих бізнес-процесів. Важливо, щоб рекомендації були конкретними, реалістичними та ретельно обґрунтованими. Вони повинні враховувати виявлені проблеми і відповідати потребам і можливостям конкретної

організації. Кожна рекомендація повинна мати чіткий план реалізації та визначати особу, відповідальну за її виконання. Після того, як рекомендації будуть складені, їх слід представити керівництву організації для обговорення та затвердження. Участь вищого керівництва є ключовим фактором успішного виконання рекомендацій, оскільки воно забезпечує підтримку та ресурси для здійснення необхідних змін. Після прийняття рішення про виконання рекомендацій необхідно розробити план дій і встановити відповідні терміни. Цей план повинен включати конкретні кроки, відповідальних осіб та ресурси, необхідні для виконання завдання. Регулярний моніторинг і оцінка виконання рекомендацій забезпечать їх успішне виконання і, при необхідності, своєчасне коригування стратегій.

Завершальним восьмим етапом аналізу є впровадження розроблених рекомендацій для поточного стану BCMS. Важливо забезпечити належну координацію та комунікацію між всіма залученими сторонами, а також проводити регулярний моніторинг виконання заходів. Це дозволяє забезпечити своєчасне усунення виявлених проблем та підтримання високого рівня готовності організації до кризових ситуацій. Після складання рекомендацій на попередньому етапі слід вжити конкретних заходів щодо їх реалізації. Це включає оновлення документів, впровадження нових процедур і політик, навчання персоналу, а також зміна організаційної структури та технічної підтримки. Одним з ключових аспектів реалізації рекомендацій є залучення всіх зацікавлених сторін. Керівникам організацій слід розставити пріоритети в підходах, спрямованих на активну підтримку процесу впровадження, надання необхідних ресурсів і забезпечення успіху. Крім того, співробітники повинні бути чітко поінформовані про зміни та їх вплив на роботу, а також отримувати навчання та підтримку, необхідні їм для успішної адаптації до нових умов. Процес виконання рекомендацій також вимагає належного керівництва та контролю. Важливо відстежувати хід виконання рекомендацій і створити систему моніторингу та оцінки, щоб можна було своєчасно виявляти і вирішувати проблеми, які можуть виникнути на цьому шляху. Крім того, важливо

враховувати динаміку змін у внутрішньому і зовнішньому середовищі організації. Рекомендації, можливо, доведеться коригувати або доповнювати з часом у міру зміни обставин та вимог. Тому важливо забезпечити гнучкість і адаптивність впроваджуваних змін.

3.2 Розробка рекомендацій щодо підвищення ефективності системи управління безперервністю бізнесу

План забезпечення безперервності бізнесу – це стратегічний посібник, створений для того, щоб допомогти організації підтримувати або швидко відновлювати бізнес-функції в умовах перебоїв, незалежно від того, спричинені вони стихійним лихом, громадськими заворушеннями, кібератакою чи будь-якою іншою загрозою бізнес-операціям [33]. Завжди існує ймовірність того, що критично важливий бізнес-процес організації зупиниться через вплив непередбаченої події, яка знаходиться поза контролем. Щоб впоратися з такими інцидентами, краще бути готовим до найгіршого. Організації повинні мати план відновлення, щоб забезпечити мінімальний вплив або порушення бізнес-операцій і обслуговування клієнтів. Однак лише створення BCP не захистить бізнес. Організації повинні мати надійну стратегію BCMS, яка не тільки добре сформульована, але й ефективна в реалізації. Отже, коли організація розробляє BCP, важливо перевірити його ефективність. Тестування плану перевіряє ефективність стратегії на місці та навчає відповідальний персонал для реального сценарію. Крім того, тестування допомагає визначити проблемні області, де план потрібно посилити.

Плани безперервної діяльності повинні включати:

- деталі дій, які будуть виконувати команди, щоб продовжувати або відновлювати пріоритетні дії протягом заданого періоду часу; контролювати вплив порушення (інциденту, аварії, катастрофи) та реакцію організації на нього;
- посилання на попередньо визначені пороги та процес активації відповіді;

- процедури, що дозволяють постачати продукти та послуги з узгодженою потужністю;
- деталі управління безпосередніми наслідками порушення, враховуючи:
  - добробут одиниць;
  - запобігання подальшої втрати або недоступності пріоритетних функцій/дій;
  - вплив на навколишнє середовище [34].

Виявлення недоліків та розробка рекомендацій щодо покращення BCMS дозволяє виявити слабкі місця, що можуть загрожувати безперервності операцій, та дозволяє розробити рекомендації для їх усунення, тим самим зміцнюючи загальну стійкість організації. Завдяки цьому організація отримає необхідною інформацією для підвищення її готовності до кризових ситуацій та зниження ризиків для бізнесу. Систематичний підхід до аналізу та впровадження рекомендацій дозволяє підтримувати високий рівень стійкості організації та забезпечувати її безперервну роботу в умовах непередбачуваних подій. Найпопулярніші рекомендації щодо покращення BCMS зображені на рис. 3.2.

Виявлення недоліків є дуже важливим етапом для будь-якої організації. Одними з основних недоліків у BCMS може бути недостатня оцінка ризиків. Часто організації обмежуються стандартними сценаріями, такими як природні катастрофи або технічні збої, не враховуючи нові та менш очевидні загрози, такі як кібератаки або пандемії й через це трапляються різні кризові ситуації.

До поширених недоліків можна віднести недостатню інтеграцію BCMS з повсякденною діяльністю компанії. У багатьох компаніях та організаціях BCP існують лише на папері і не впроваджуються у повсякденну роботу. Через це трапляються ситуації коли персонал не ознайомлений з планами та не готовий діяти за ними у разі кризових ситуацій й компанія несе значні збитки.

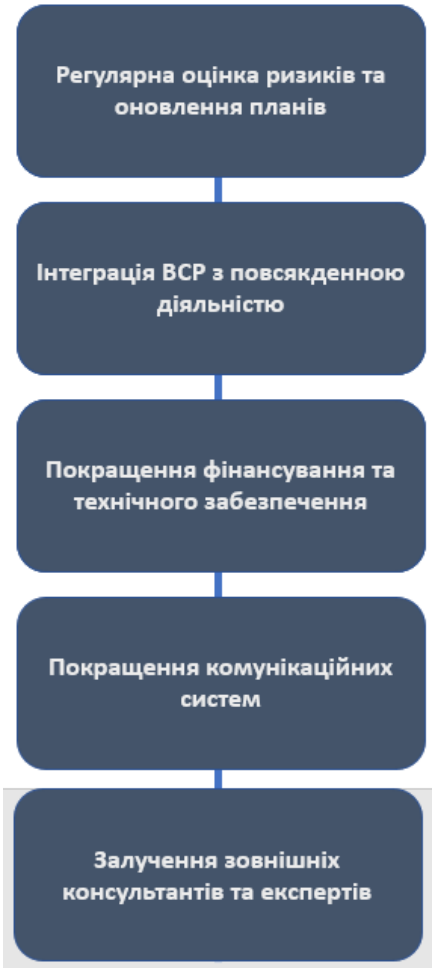

Рис. 3.2. Найпопулярніші рекомендації

Також до важливих недоліків можна віднести недостатнє фінансування і технічне забезпечення. Без належних ресурсів важко забезпечити ефективне резервне копіювання, автоматизацію процесів відновлення та надійну систему комунікацій. Через що дуже знижується здатність організації швидко реагувати на надзвичайні ситуації.

До головних методів, які допомагають виявити недоліки системи, можна віднести: регулярне проведення внутрішнього аудиту, залучення акредитованих органів для проведення зовнішнього аудиту, проведення стрес-тестів та симуляцій, аналіз попередніх інцидентів, оцінку відповідності стандартам та найкращим практикам, використання аналітичних інструментів та технологій, підвищення рівня обізнаності та навчання персоналу.

Внутрішній аудит є одним із найефективніших способів ідентифікації слабких місць у BCMS. Внутрішні аудитори мають глибоке розуміння процесів

та операцій організації, що дозволяє їм детально оцінити відповідність BCP поточним потребам. Вони аналізують документи, перевіряють процедури та інтерв'ють ключових співробітників, щоб оцінити їх готовність до виконання планів у разі надзвичайної ситуації. Це допомагає виявити прогалини у документації, нерозуміння працівниками своїх ролей або застарілість планів.

Залучення зовнішніх експертів та консультантів дозволяє отримати неупереджену оцінку BCMS. Зовнішні аудитори можуть мати досвід роботи з різними організаціями та галузями, що надає їм унікальну перспективу. Вони здатні виявити недоліки, які можуть бути непомітні для внутрішніх команд через відсутність об'єктивності. Зовнішні аудитори також можуть надати рекомендації щодо вдосконалення на основі найкращих практик у галузі.

Стрес-тести та симуляції кризових ситуацій є важливими інструментами для оцінки реальної ефективності BCMS. Моделювання різних сценаріїв, таких як природні катастрофи, кібератаки або технічні збої, дозволяє оцінити, як система функціонує під тиском. Важливо, щоб ці симуляції проводилися регулярно і охоплювали всі аспекти бізнесу. Аналіз реакції персоналу та ефективності процедур під час симуляцій дозволяє виявити слабкі місця у планах та підготовці.

Один із найкращих способів виявлення недоліків у BCMS – це аналіз попередніх кризових ситуацій. Організації повинні ретельно аналізувати, як вони вирішували минулі інциденти, щоб виявити слабкі місця та невідповідності у своїх планах. Докладний розбір випадків допомагає зрозуміти, які аспекти системи працювали добре, а які потребують вдосконалення. Збір зворотного зв'язку від працівників, які брали участь у вирішенні цих ситуацій, також є цінним джерелом інформації.

BCMS повинна відповідати міжнародним стандартам, таким як ISO 22301, так й іншим стандартам, впровадженим в організації. Порівняння поточних процедур та політик із вимогами цих стандартів дозволяє виявити недоліки та прогалини. Важливо також постійно стежити за змінами у стандартах та

найкращих практиках, щоб своєчасно оновлювати BCMS відповідно до нових вимог.

Сучасні аналітичні інструменти можуть значно спростити процес виявлення недоліків у BCMS. Автоматизовані системи моніторингу та управління подіями безпеки дозволяють виявляти потенційні загрози та відхилення у реальному часі. Системи управління ризиками допомагають ідентифікувати, оцінювати та управляти ризиками, що можуть вплинути на безперервність бізнесу. Використання цих технологій підвищує точність та швидкість виявлення недоліків.

Персонал організації відіграє ключову роль у забезпеченні безперервності бізнесу. Регулярні тренінги та навчання дозволяють підвищити рівень обізнаності працівників щодо їх ролей та обов’язків під час кризових ситуацій. Проведення тестів та оцінок знань допомагає виявити прогалини у знаннях та навичках, що можуть вплинути на ефективність BCP.

В умовах зростаючої складності та непередбачуваності бізнес-середовища ефективна BCMS стає життєво необхідною для забезпечення безперебійної роботи та мінімізації втрат під час кризових ситуацій. Однак, щоб ця система була дієвою, вона потребує постійного вдосконалення та розробки рекомендацій та їх адаптації. Перед тим, як перейти до розробки рекомендацій, потрібно виявити головні недоліки, а вже після цього впроваджувати ряд різних процедур, до яких можна віднести: регулярну оцінку ризиків, інтеграцію BCP з повсякденної діяльності, покращення фінансування, покращення комунікаційних систем, залучення зовнішніх консультантів та експертів, проведення регулярних симуляційних навчань та стрес-тестів.

Оцінка ризиків є однією з найголовніших рекомендацій, вона має бути постійним процесом, який включає аналіз як традиційних загроз, так і нових, які можуть виникнути у майбутньому. Мається на увазі, що вона не лише враховує природні катастрофи або технічні збої, але й кібератаки, соціально-економічні зміни, ризики, пов'язані з постачальниками тощо. На основі всіх результатів

оцінки ризиків слід регулярно оновлювати BCP, щоб вони відповідали актуальним викликам.

Для підвищення ефективності BCMS важливо інтегрувати її у повсякденну діяльність компанії. Необхідно, щоб вона включала в себе проведення регулярних тренінгів для персоналу, симуляцій кризових ситуацій та постійного моніторингу готовності систем. Оскільки співробітники повинні бути добре ознайомлені з BCP і знати свої ролі та обов'язки у разі надзвичайної ситуації, а за для більшої впевненості можна зробити розсилку: у разі кризової ситуації це допоможе забезпечити їх оперативне використання.

Також не слід забувати про регулярні симуляції кризових ситуацій та стрес-тестів, які допоможуть виявити вразливості BCMS та покращити координацію дій між співробітниками. У майбутньому це допоможе підвищити готовність організації до реальних кризових ситуацій та дозволить забезпечити швидке відновлення звичайної діяльності.

Ефективна BCMS потребує відповідних ресурсів. Збільшення інвестицій у сучасні технології резервного копіювання та відновлення даних, використання хмарних сервісів для підвищення гнучкості та надійності є критично важливими. Впровадження автоматизованих систем моніторингу та управління подіями безпеки (SIEM) дозволить швидко виявляти та реагувати на загрози. Організація повинна забезпечити належне фінансування для підтримки цих технологій та процесів. Гарним прикладом використання ресурсів є ефективна комунікація, яка під час кризових ситуацій допомагає скоординувати дії співробітників. Організація повинна встановити багатоканальні системи комунікації, що включають мобільні додатки, месенджери, електронну пошту та інші засоби зв'язку. Регулярне тестування цих систем забезпечить їх надійність та ефективність у реальних умовах. Крім того, важливо забезпечити доступність контактної інформації та каналів зв'язку для всіх співробітників, клієнтів та постачальників.

Інколи внутрішні аудитори можуть не помітити недоліки чи навіть навмисно не враховувати через людський фактор чи недостатню обізнаність.

Тому незалежна оцінка BCMS дозволить виявити вразливості чи приховані недоліки та впровадити найкращі практики. Залучення зовнішніх консультантів та експертів може допомогти отримати нові ідеї та рекомендації для вдосконалення BCMS. Регулярні консультації з фахівцями дозволять організації залишатися на передовій у питаннях управління ризиками та кризовими ситуаціями.

Управління інцидентами інформаційної безпеки – це процес, який використовується спеціалістами з кібербезпеки, DevOps та IT-фахівцями для виявлення інцидентів у їхніх організаціях і реагування на них [35]. Він є одним з найважливіших процесів, який дає організаціям можливість своєчасно виявляти інциденти і реагувати на них якомога швидше, використовуючи ретельно підібрані інструменти підтримки.

Управління ризиком – це процес реагування на події та зміни ризиків у процесі виконання проекту [36].

Таким чином, основні рекомендації щодо підвищення ефективності BCMS включають такі:

- проведення регулярних тестів та моделювання вони можуть допомогти перевірити ефективність планів та процедур та виявити слабкі місця. Після цього необхідно ретельно проаналізувати результати тестів і симуляцій, щоб виявити недоліки і дати рекомендації щодо їх усунення;
- на основі аналізу результатів розробляються конкретні рекомендації, які повинні бути реалізовані в рамках оновлених планів і процедур. Процес впровадження рекомендацій вимагає активної підтримки керівництва, ефективного управління та контролю;
- проведення оцінка ризиків, вона має бути постійним процесом, який включає аналіз як традиційних загроз, так і нових, які можуть виникнути у майбутньому;
- проведення регулярних симуляції кризових ситуацій та стрес-тестів, які допоможуть виявити вразливості BCMS та покращити координацію дій між співробітниками;

- інтегрування BCMS у повсякденну діяльність компанії. Оскільки співробітники повинні бути добре ознайомлені з BCP і знати свої ролі та обов'язки у разі надзвичайної ситуації;
- збільшення інвестицій у сучасні технології резервного копіювання та відновлення даних, використання хмарних сервісів для підвищення гнучкості та надійності.

3.3 Розробка рекомендацій щодо впровадження технологій ІБ для підвищення ефективності заходів із забезпечення безперервності бізнесу

У сучасному динамічному бізнес-середовищі забезпечення безперервності бізнесу стає все більш важливим для організацій будь-якого розміру та галузі. Впровадження нових методів та інструментів може значно підвищити ефективність BCMS, забезпечуючи її здатність швидко реагувати на кризи та мінімізувати їх вплив. Систематичний підхід до впровадження новітніх технологій та методів забезпечує високу стійкість організації та здатність швидко відновлюватися після збоїв, що є критично важливим у сучасному нестабільному бізнес-середовищі. До сучасних методів та інструментів можна віднести використання хмарних тегнологій для резервного копіювання та відновлення даних, впровадження SIEM, використання різноманітніх інструментів управління ризиками, проведення регулярних тренінгів та симуляцій кризових ситуацій, впровадження інструментів для віддаленої роботи.

Сучасні методи та інструменти зображені на рис. 3.3.

Рис. 3.3. Сучасні методи та інструменти

1. Використання хмарних технологій для резервного копіювання та відновлення даних. Захист даних є критично важливим аспектом BCP. Традиційні методи резервного копіювання, що базуються на локальних серверах або фізичних носіях, можуть бути ненадійними або неефективними в умовах серйозних криз. Хмарні технології забезпечують високий рівень доступності та безпеки даних, дозволяючи зберігати резервні копії у віддалених дата-центрах. Це забезпечує можливість швидкого відновлення даних у випадку втрати чи пошкодження. Використання хмарних рішень також знижує витрати на управління фізичними резервними копіями та забезпечує гнучкість у масштабуванні обсягів зберігання даних. Ключова перевага хмарного резервного копіювання полягає в тому, що ви можете створити резервну копію будь-якого обсягу даних. Сервіс хмарного резервного копіювання адаптуватиметься до ваших запитів у міру збільшення вимог до потужності [37].

2. Впровадження систем автоматизованого моніторингу та управління подіями. SIEM-системи надають організаціям можливість автоматично збирати, аналізувати та реагувати на інциденти безпеки в режимі реального часу. Впровадження таких систем дозволяє швидко виявляти потенційні загрози та забезпечувати своєчасне реагування, що є важливим для мінімізації ризиків і забезпечення безперервності бізнесу. SIEM-системи можуть автоматично генерувати звіти про інциденти, що полегшує процес аудиту та оцінки ефективності BCMS. Крім того, такі системи допомагають організаціям дотримуватись вимог нормативних актів щодо ІБ.

Система SIEM має надавати такі функції:

- збір інформації про події безпеки в режимі реального часу;
- аналіз даних і категоризація;
- реагування на інциденти, виявлення внутрішніх і зовнішніх загроз;
- моніторинг додатків;
- моніторинг доступу до даних і активності користувачів;
- масштабованість і гнучкість;
- ведення журналу, звітність;

- простота розгортання та підтримки [38].

3. Інтеграція інструментів управління ризиками забезпечує організаціям систематизований підхід до ідентифікації, оцінки та управління ризиками.

Інструменти для аналізу ризиків можуть включати SWOT-аналіз (аналіз сильних і слабких сторін, можливостей і загроз) – це система, яка використовується для оцінки конкурентної позиції компанії та розробки стратегічного планування [39], PESTLE-аналіз (оцінка політичних, економічних, соціальних, технологічних, правових та екологічних факторів) – аналіз PESTLE є системою управління та інструментом діагностики [40], сценарний аналіз, карта ризиків, планування та реагування на ризики, моніторинг ризиків, внутрішній аудит.

Використання таких інструментів дозволяє автоматизувати процес збору та аналізу даних про ризики, що сприяє більш швидкому та ефективному реагуванню на зміни в профілі ризиків організації, а також допомагає в розробці та впровадженні стратегій пом'якшення ризиків, що підвищує загальну стійкість бізнесу.

4. Проведення регулярних тренінгів та симуляцій кризових ситуацій є важливим заходом для підвищення готовності персоналу до дій у разі надзвичайних подій. Тренінги допомагають працівникам зрозуміти їхні ролі та обов'язки в рамках BCMS, що забезпечує більш ефективне реагування на інциденти. Симуляції дозволяють перевірити реальну ефективність BCP та виявити потенційні слабкі місця. Важливо, щоб такі тренінги та симуляції проводилися регулярно і охоплювали всі можливі сценарії кризових ситуацій. Це включає техногенні аварії, природні катастрофи, кібератаки та інші загрози.

5. Впровадження інструментів для віддаленої роботи в умовах зростання її популярності стає важливо, оскільки необхідно забезпечити можливість безперебійної роботи співробітників незалежно від їхнього місцезнаходження. Використання віртуальних приватних мереж (VPN), систем для спільної роботи та комунікаційних платформ дозволяє зберегти продуктивність бізнесу навіть у

разі фізичної недоступності офісів. Це особливо важливо під час природних катастроф, епідемій або інших ситуацій, що потребують тимчасової ізоляції.

У VPN є три основні види підключення:

- L2TP (Layer 2 Tunneling Protocol)
- PPTP (Point-to-point tunneling protocol)
- OpenVPN

L2TP – це розширення протоколу тунелювання «точка-точка» (PPTP), який використовується постачальниками послуг Інтернету (ISP) для створення віртуальних приватних мереж [41].

PPTP (Point-to-point tunneling protocol) – це тунельний протокол типу «точка-точка», який дозволяє комп'ютеру користувача встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеною мережі [42].

Різниця між L2TP і PPTP полягає в тому, що L2TP може використовувати різні засоби тунелювання, тоді як PPTP може бути тунельований лише через IP-мережу. L2TP також підтримує кілька тунелів між двома кінцевими точками. Протокол PPTP підтримує лише один тунель між двома кінцевими точками.

OpenVPN – це популярний протокол з відкритим кодом. OpenVPN використовує власний протокол безпеки, який базується на SSL та TLS, для обміну ключами, створення безпечних з'єднань типу "точка-точка" або "сайт-сайт" [43].

6. Впровадження технологій штучного інтелекту (ШІ) та машинного навчання може значно підвищити ефективність BCMS. Використання штучного інтелекту для аналізу великих обсягів даних дозволяє виявляти приховані патерни та передбачати можливі ризики.

Технології штучного інтелекту – галузь інформаційних технологій, яка займається створенням розумних машин, здатних виконувати завдання, які зазвичай вимагають людського інтелекту [44].

Машинне навчання – це галузь ШІ та інформатики, яка зосереджена на використанні даних і алгоритмів, щоб дозволити ШІ імітувати спосіб навчання людей, поступово підвищуючи його точність [45].

Наприклад, машинне навчання може використовуватись для прогнозування ймовірності виникнення кібератак або природних катастроф, що дозволяє організаціям заздалегідь готуватися до можливих загроз. ШІ також може використовуватися для автоматизації процесів моніторингу та реагування на інциденти, що підвищує швидкість та ефективність дій.

7. Розробка та впровадження політик кібербезпеки. Кібербезпека є невід'ємною частиною сучасної BCMS. Розробка та впровадження комплексних політик кібербезпеки допомагає захистити ІС та дані організації від загроз. Політики кібербезпеки повинні включати заходи з управління доступом, захисту мережі, шифрування даних та регулярного оновлення ПЗ. Крім того, важливо проводити регулярні оцінки кіберризиків та тренінги для працівників, щоб підвищити їх обізнаність про загрози та навички реагування на інциденти ІБ.

Висновки до розділу 3

У розділі було проаналізовано алгоритм для проведення оцінки поточного стану BCMS організації, етапи якого включають: збір інформації про поточний стан BCMS, оцінка ризиків, проведення детального аналізу існуючих планів та процедур безперервності бізнесу, перевірка готовності персоналу до кризових ситуацій, проведення тестів та симуляцій, перевірка результатів тестів та симуляцій, розробка рекомендацій для покращення BCMS на основі результатів аналізу, впровадження розроблених рекомендацій для поточного стану BCMS.

Було запропоновано рекомендації щодо впровадження організаційних заходів для підвищення ефективності функціонування BCMS, а саме:

- розробка чітких інструкцій та процедур для персоналу;
- навчання та тренінги для персоналу;
- проведення регулярних тестів та симуляцій;

- створення системи моніторингу та контролю;
- використання сучасних технологій та інструментів;
- постійне вдосконалення BCMS.

Було запропоновано рекомендації щодо впровадження технологій ІБ для підвищення ефективності заходів із забезпечення безперервності бізнесу, а саме:

- проведення регулярних тестів та моделювання;
- на основі аналізу результатів розробляються конкретні рекомендації;
- проведення оцінка ризиків;
- проведення регулярних симуляції кризових ситуацій та стрес-тестів;
- інтегрування BCMS у повсякденну діяльність компанії;
- збільшення інвестицій у сучасні технології резервного копіювання та відновлення даних.

ВИСНОВКИ

У кваліфікаційній роботі було детально розглянуто основні принципи забезпечення безперервності бізнесу в контексті ІБ. Зокрема, розглядалися аспекти кіберстійкості, резервування засобів ІБ, мінімізація часу відновлення після інциденту, системний підхід до управління ризиками, інтеграція планів безперервності з бізнес-стратегією, регулярне тестування та оновлення, навчання персоналу, ефективна комунікація та безперервний моніторинг.

Було досліджено переваги та виклики, які виникають при впровадженні BCMS відповідно до стандартів, таких як ISO 22301, ISO/IEC 27035, ISO/IEC 27005, ISO/IEC 27001 та ISO/IEC 27002. В цих стандартах надаються вимоги, різні підходи до налаштування та рекомендації щодо управління інцидентами, ризиками, навчання персоналу, моніторингу та розробки планів безперервності бізнесу.

Крім того, було приділено увагу до аналізу алгоритму проведення аудиту заходів із забезпечення безперервності бізнесу, який включає в себе етапи: планування, збору інформації, оцінки ризиків, проведення аудиту, виявлення недоліків, розробки рекомендацій, звітності, моніторингу та впровадження.

Було виявлено перешкоди, які можуть виникнути при аудиті окремих компонентів BCMS, таких як управління інцидентами ІБ, процеси оцінки ризиків, навчання персоналу та процеси відновлення після інцидентів.

Було проаналізовано методики оцінки ефективності заходів та планів забезпечення безперервності бізнесу та застосовні для них показники: середній час відновлення (MTTR), середній час реагування на інциденти ІБ, відсоток завершених тестів. Використання таких показників допомагає організаціям визначити рівень готовності до кризових ситуацій та вжити заходів для підвищення ефективності.

Було досліджено головні інструменти для підтримки та оцінки процесів забезпечення безперервності бізнесу, а саме: Enterprise Risk Management, Business Continuity Management, Incident Management Systems, Monitoring and

Alerting Tools, Reporting and Dashboarding Tools. Також було розглянуто різні техніки аудиту, включаючи чек-листи, інтерв'ю, опитування, моделювання та тестування.

Крім того, було запропоновано рекомендації для підвищення ефективності функціонування BCMS, включаючи розробку чітких інструкцій для персоналу, регулярне навчання та тренінги, проведення тестів та симуляцій, створення системи моніторингу та контролю, використання сучасних технологій та інструментів, а також постійне вдосконалення BCMS.

Впровадження комплексного підходу до забезпечення безперервності бізнесу з врахуванням розроблених рекомендації та запропонованої методики проведення аудиту заходів із забезпечення безперервності бізнесу дозволить організаціям підвищити свою стійкість до негативних впливів, забезпечити безперервну діяльність при кризових ситуацій та мати змогу підтримувати довіру клієнтів, партнерів та інших зацікавлених сторін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Б.М. Мушинський. Безперервність ведення бізнесу як концепція управління фінансовою установою URL: https://economics.net.ua/files/science/ek_kiber/2018/112.pdf.

2. ISO/IEC 27002:2022. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911 .

3. Стандарт ISO 22301. Безперервність бізнесу (BCMS) | TMS Academy. URL: https://academy.tms.ua/uk/sertificat-ua/standart-iso-22301-systema-menedzhmentu-bezperervnosti-biznesu-bcms/.

4. Maximum Acceptable Outage. Risky Thinking - On Risk Management, Business Continuity, and Security. URL: https://www.riskythinking.com/glossary/maximum_acceptable_outage#:~:text=The%20Maximum%20Acceptable%20Outage%20(MAO,Period%20of%20Disruption%20(MTPOD.

5. What is a Recovery Time Objective? URL: https://www.kyndryl.com/us/en/learn/rto

6. What is a Recovery Point Objective (RPO). URL: https://www.f5.com/glossary/recovery-point-objective-rpo

7. RTO and RPO: Disaster Recovery Strategy Essentials. Backup and IT management software. MSP360 Data Protection. URL: https://www.msp360.com/resources/blog/rto-vs-rpo-difference/

8. RTO і RPO: відмінності у показниках резервного копіювання. URL: https://gigacloud.ua/blog/navchannja/rto-i-rpo-vidminnosti-u-pokaznikah-rezervnogo-kopijuvannja

9. Міністерство фінансів україни. Методичний посібник щодо аспектів управління ризиками, як складової системи внутрішнього контролю у розпорядника бюджетних коштів. Київ, 2022. С. 22

10. Що таке аналіз ризику: визначення та інструменти | Повний посібник – рішення Visure. URL: https://visuresolutions.com/uk/блог/аналіз-

ризику/#:~:text=Аналіз%20ризиків%20–%20це%20практика%20оцінки,до%20бізнес-%20та%20інвестиційних%20рішень.

11. Менеджмент Ризику. URL: https://moodle.znu.edu.ua/pluginfile.php/875849/mod_resource/content/1/Тема%205%20МЕНЕДЖМЕНТ%20РИЗИКУ.%20МЕТОДИ%20ОЦІНКИ%20РИЗИКУ.pdf#:~:text=Порівняльна%20оцінка%20ризику%20–%20це%20зіставлення,ризик%2C%20отриману%20при%20аналізі%20ризику.

12. Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру. URL: https://zakon.rada.gov.ua/laws/show/1809-14#Text

13. Про пожежну безпеку : Закон України від 17.12.1993 р. № 3745-XII : станом на 1 лип. 2013 р. URL: https://zakon.rada.gov.ua/laws/show/3745-12#Text

14. Тестування безпеки. URL: https://qalight.ua/baza-znaniy/testuvannya-bezpeki/

15. What is Security Monitoring? URL: https://www.hpe.com/emea_europe/en/what-is/security-monitoring.html#:~:text=Security%20monitoring%20is%20the%20automated,these%20threats%20with%20appropriate%20action.

16. Моніторинг і оцінка: базові поняття. URL: http://multycourse.com.ua/ua/page/21/45

17. MTTR (середній час до ремонту) – ключовий показник продуктивності та як його розрахувати – програмне забезпечення для промисловості – автоматизація – ТЕХМАШ-УКРАЇНА. URL: https://metalloobrabotka.org.ua/article/mttr-srednee-vremya-do-remonta-klyuchevoj-pokazatel-proizvoditelnosti-i-kak-ego-rasschitat-programmnoe-obespechenie-dlya-promyshlennosti-avtomatizacziya/

18. Understanding Mean Time to Recover (MTTR): A Key Metric in Incident Management. URL: https://gartsolutions.medium.com/understanding-mean-time-to-recover-mttr-a-key-metric-in-incident-management-07d9fe015e49

19. RTO и RPO - UCloud. URL: https://ucloud.ua/rto-i-rpo/

20. Exercises | Ready.gov. URL: https://www.ready.gov/business/training/testing-exercise/exercises#:~:text=Tabletop%20exercises%20are%20discussion-based,of%20one%20or%20more%20scenarios

21. Conducting simulation exercises. URL: https://www.preventionweb.net/conducting-simulation-exercises#:~:text=Simulation%20exercises%20help%20prepare%20communities,are%20tested%20in%20these%20exercises.

22. Full-Scale Testing. URL: https://advintegrity.com/full-scale-testing#:~:text=Full-scale%20testing%20allows%20us,validating%20and%20calibrating%20numerical%20models

23. What is a Disaster Recovery Plan? URL: https://www.kyndryl.com/gb/en/learn/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DR,and%20any%20other%20disruptive%20events.

24. Резервне копіювання та відновлення – у чому різниця? URL: https://wiseit.com.ua/rezervne-kopiyuvannya-ta-vidnovlennya-u-chomu-riznyczya/#:~:text=Резервне%20копіювання%20(backup)%20означає%20створення,пошкоджених%20даних%20із%20резервних%20копій.

25. Cloud Solutions - стаття з розвитку бізнесу та інформаційних технологій на підприємстві | IT-Enterprise URL: https://www.it.ua/articles/cloud-solutions-

26. What Is Virtualization? Definition, Benefits & Examples. URL: https://www.forbes.com/advisor/business/software/what-is-virtualization/

27. Monitoring Automation. URL: https://docs.microfocus.com/OMi/10.62/Content/OMi/ConceptsGuide/getStarted/getStarted_concepts_MA.htm#:~:text=Monitoring%20Automation%20provides%20a%20complete,(CIs)%20comprising%20the%20application.

28. What are Management Tools? Meaning, Examples & Tips. URL: https://www.teamazing.com/management-tools-meaning/#:~:text=Management%20tools%20are%20tools%20used,%2C%20motivation%2C%20and%20conflict%20management.

29. 13 Top Business Communication Platforms to Work Faster. URL: https://www.nextiva.com/blog/communication-platforms.html#:~:text=A%20communication%20platform%20is%20software,task%20management%2C%20and%20team%20messaging.

30. What is a Crisis Management Plan? (Overview, Definition, and Examples). URL: https://www.onboardmeetings.com/blog/crisis-management-plan/

31. Business Impact Analysis | Ready.gov. URL: https://www.ready.gov/business/planning/impact-analysis#:~:text=A%20business%20impact%20analysis%20(BIA,identified%20during%20a%20risk%20assessment.

32. Risk Assessment | Ready.gov. URL: https://www.ready.gov/business/planning/risk-assessment#:~:text=A%20risk%20assessment%20is%20a,to%20complete%20your%20risk%20assessment.

33. How to create an effective business continuity plan. URL: https://www.cio.com/article/288554/best-practices-how-to-create-an-effective-business-continuity-plan.html#:~:text=A%20business%20continuity%20plan%20(BCP,other%20threat%20to%20business%20operations.

34. Планування безперервності бізнесу, частина 1. URL: https://ikmj.com/uk/планування-безперервності-бізнесу-ч/#:~:text=Що%20таке%20план%20безперервності%20бізнесу,її%20цілей%20забезпечення%20безперервності%20бізнесу.

35. Що таке управління інцидентами та які його переваги? URL: https://www.issp.training/post/shcho-take-upravlinnya-intsydentamy-ta-yaki-yoho-perevahy#:~:text=Управління%20інцидентами%20—%20це%20процес%2C%20який,організаціях%20і%20реагування%20на%20них.

36. Управління ризиками в проектах. URL: https://www.oa.edu.ua/download/Lektsija_8.pdf

37. Які переваги хмарного резервного копіювання? URL: https://experience.dropbox.com/uk-ua/resources/cloud-backup-advantages#:~:text=Ключова%20перевага%20хмарного%20резервного%20копіювання,за%20те%2C%20що%20вам%20потрібно.

38. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? URL: https://eska.global/blog/sho-take-upravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo

39. SWOT Analysis: How To With Table and Example. URL: https://www-investopedia-com.translate.goog/terms/s/swot.asp?_x_tr_sl=auto&_x_tr_tl=uk&_x_tr_hl=uk#:~:text=SWOT%20(strengths%2C%20weaknesses%2C%20opportunities,as%20current%20and%20future%20potential.

40. CIPD | PESTLE analysis. URL: https://www.cipd.org/en/knowledge/factsheets/pestle-analysis-factsheet/#:~:text=A%20PESTLE%20analysis%20studies%20the,managers%20in%20strategic%20decision%20making.

41. What is L2PT and how does it work? URL: https://www-techtarget-com.translate.goog/searchnetworking/definition/Layer-Two-Tunneling-Protocol-L2TP?_x_tr_sl=auto&_x_tr_tl=uk&_x_tr_hl=uk

42. Віртуальні приватні мережі (VPN). URL: https://compbest.com.ua/ua/virtualnye-chastnye-seti-vpn/

43. Що таке OpenVPN протокол? VPN Unlimited. URL: https://www.vpnunlimited.com/ua/help/vpn-protocols/open-vpn-protocol

44. Технології штучного інтелекту та машинного навчання у бізнесі MetinvestDigital. URL: https://metinvest.digital/ua/page/1017#:~:text=Технології%20штучного%20інтелекту%20(Artificial%20Intelligence,які%20зазвичай%20вимагають%20людського%20інтелекту.

45. What is machine learning (ML)? IBM. URL: https://www.ibm.com/topics/machine-learning