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: “ДОСЛІДЖЕННЯ ПРАКТИК ЩОДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ”

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

_____ Іван ШЕВЧУК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Іван ШЕВЧУК
Ім’я, ПРІЗВИЩЕ

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

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

Шевчуку Івану Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Дослідження практик щодо побудови системи управління інформаційною безпекою на підприємстві”,
керівник кваліфікаційної роботи ЯКИМЕНКО Юрій, к.в.н., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “__“ березня 2024 р. №__.

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

3. Вихідні дані до кваліфікаційної роботи *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, міжнародні стандарти інформаційної безпеки, аналіз ризиків, наукова та технічна література*.

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати теоретичні аспекти управління інформаційною безпекою.
4.2. Дослідити основні практики щодо побудови системи управління інформаціною безпекою на підприємстві.
4.3. Визначити підходи щодо побудови системи управління інформаційною безпекою і розробити рекомендації по їх вдосконаленню для обраного прикладу.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних аспектів управління інформаційною безпекою	08.04.2024	
4.	Дослідження основних практик щодо побудови системи управління інформаціною безпекою на підприємстві.	22.04.2024	
5.	Визначення підходів щодо побудови системи управління інформаційною безпекою і розробка рекомендацій по їх вдосконаленню (для обраного прикладу)	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Іван ШЕВЧУК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Шевчук І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Дослідження практик щодо побудови системи управління інформаційною безпекою на підприємстві"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач Іван ШЕВЧУК у кваліфікаційній роботі проаналізував теоретичні аспекти управління інформаційною безпекою, дослідив основні практики щодо побудови системи управління інформаційною безпекою на підприємстві, визначив підходи щодо побудови системи управління інформаційною безпекою для обраного прикладу та розробив практичні рекомендації за темою дослідження..

ШЕВЧУК Іван 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 двох конференціях..

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

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

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Шевчук І.В. 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 ШЕВЧУКА Івана
на тему "Дослідження практик щодо побудови системи управління інформаційною безпекою на підприємстві"

Актуальність.

З розвитком і поширенням інформаційно-комунікаційних технологій гострої значимості набувають питання забезпечення інформаційної безпеки підприємств, що визнано однією із складових задач в їх повсягденної діяльності . Проблеми створення ефективної системи інформаційної безпеки на підприємствах намагаються вирішити у своїх наукових пошуках багато вчених. Побудова таких систем є комплексним завданням, що включає в себе оцінку сучасних загроз і ризиків, реагування на інциденти і відновлення стану після них, забезпечення безперервної готовності до виконання планових виробничих завдань. Дослідження існуючих практик щодо побудови системи управління інформаційною безпекою на підприємстві є надзвичайно актуальною і важливою науковою задачею.

Позитивні сторони.

1. У роботі досліджено основні аспекти побудови системи управління інформаційною безпекою на підприємстві, включаючи методи та моделі управління та сучасні практики їх проектування і впровадження.

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

3. Автор опрацював значну джерельну базу: близько 50 публікацій, у тому числі англомовних.

4. За результатами дослідження запропоновано практичні рекомендації по вдосконаленню підходів щодо побудови та впровадженню системи управління інформаційною безпекою на підприємстві.

Недоліки.

Доцільно було б приділити більше уваги розгляду особливостям побудови інших основних систем в сфері безпеки, таким як управлінню безперевностью бізнесом. Однак, це зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ __Галина ГАЙДУР _

д.т.н., професор *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню практик щодо побудови системи управління інформаційною безпекою на підприємстві. Робота складається зі вступу, трьох розділів, що містять 10 рисунків, висновків і списку використаних джерел із 48 найменувань. Загальний обсяг роботи становить 66 аркуші, з яких 7 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження практик щодо побудови системи управління інформаційною безпекою на підприємстві.

Об'єктом дослідження є системи управління інформаційною безпекою на підприємствах.

Предмет дослідження – практики та методи побудови систем управління інформаційною безпекою на підприємствах.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Як результат у роботі проаналізовано особливості управління інформаційною безпекою підприємства, досліджено основні характеристики практик побудови системи управління інформаційною безпекою; визначено інструменти та методи впровадження системи управління інформаційною безпекою, розроблено практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані в практичній діяльності при плануванні побудови та реалізації системи управління інформаційною безпекою підприємства у контексті забезпечення захисту інформаційних активів.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, УПРАВЛІННЯ РИЗИКАМИ, ПРАКТИКИ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ.

ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 10 figures, conclusions and the list of references containing 48 items. The total volume of the work is 66 pages, of which 7 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is study practices for building an information security management system at an enterprise.

The object the study is information security management systems at enterprises.

The subject of the study is the the practices and methods of building information security management systems at enterprises.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to information security management were used in the work.

As a result, the work analyzed the features of enterprise information security management, examines the main characteristics of practices for building an information security management system; examines the tools and methods for implementing an information security management system, and develops practical recommendations.

Field of application. The developed approaches can be used in the planning and implementation of an enterprise information security management system in the context of ensuring the protection of information assets.

Keywords: INFORMATION SECURITY OF THE ENTERPRISE, INFORMATION SECURITY MANAGEMENT SYSTEM, RISK MANAGEMENT, PRACTICES OF BUILDING MANAGEMENT SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

GDPR	Закони про захист даних в ЄС
IT-системи	Інформаційно-технологічні системи
ACL	Списки контролю доступу
NIST	Національний інститут стандартів і технологій
СМІБ	Система менеджменту ІБ
СУІБ	Система управління ІБ
IDS/IPS	Системи виявлення та попередження вторгнень
ISIMF	Комплексні системи управління інцидентами ІБ
СУВІБ	Системи управління вразливостями
ISM	The Corporate Information Security Management
CISO	Служби інформаційної безпеки
KPI	Ключові показники ефективності
ISMS.online	Платформа - включає шаблони і керівництва, які відповідають кращим практикам і міжнародним стандартам

ВСТУП

Актуальність теми. У світі, де держави, компанії та навіть окремі користувачі є об'єктом кібератак, забезпечення інформаційної безпеки підприємств є важливим, як ніколи. В сучасних умовах зростають інформаційні ризики і загрози інформаційної безпеки. Все більше виникає необхідність в пошуку ефективних методичних і інших організаційних підходів у боротьбі з ризиками і загрозами інформаційної безпеки.

Ефективне управління інформаційною безпекою є критично важливим процесом, який дозволяє своєчасно виявляти, аналізувати ризики, реагувати на загрози та відновлюватися від інцидентів.

Дослідження існуючих практик щодо побудови системи управління інформаційною безпекою на підприємстві є надзвичайно актуальною і важливою науковою задачею.

***Мета роботи*:** дослідження практик щодо побудови системи управління інформаційною безпекою на підприємстві.

***Об'єкт дослідження* –** системи управління інформаційною безпекою на підприємствах.

Предмет дослідження – практики та методи побудови систем управління інформаційною безпекою на підприємствах.

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

1. Проаналізувати особливості управління інформаційною безпекою підприємства.

2. Дослідити основні характеристики технологій формування обізнаності й навчання персоналу.

3. Вивчити інструменти та методи формування обізнаності й навчання персоналу з інформаційної безпеки, розробити практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління

інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і інструментів формування обізнаності й навчання персоналу як важливого елемента управління інформаційною безпекою відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

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

Розділ 1 ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Управління інформаційною безпекою є важливою складовою сучасних інформаційних систем, що має за мету забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Теоретичні аспекти цієї дисципліни охоплюють широкий спектр концепцій, методологій та інструментів, що спрямовані на захист інформаційних активів від різноманітних загроз.

Основою управління інформаційною безпекою є ризик-орієнтований підхід, що передбачає ідентифікацію, оцінку та управління ризиками, пов’язаними з інформаційними ресурсами. Це включає визначення активів, вразливостей, потенційних загроз та ймовірних наслідків реалізації цих загроз. Використання кількісних і якісних методів оцінки ризиків дозволяє розробляти адекватні стратегії захисту та оптимізувати витрати на забезпечення безпеки.

Іншим важливим теоретичним аспектом є розробка та впровадження політик безпеки. Політики безпеки визначають правила, процедури та контролі, необхідні для захисту інформаційних ресурсів. Вони включають як технічні заходи, такі як шифрування, автентифікація та контроль доступу, так і організаційні заходи, такі як навчання персоналу та управління інцидентами.

Моделі загроз та вразливостей є ще одним ключовим елементом теорії управління інформаційною безпекою. Моделювання загроз дозволяє визначити потенційні джерела атак, їхні можливості та мотиви, а також шляхи, якими можуть бути здійснені атаки. Вразливості системи визначаються як слабкі місця, що можуть бути використані для реалізації загроз. Знання про загрози та вразливості дозволяє розробляти ефективні контрзаходи.

Управління інформаційною безпекою також включає аспекти відповідності нормативним вимогам та стандартам. Існує ряд міжнародних стандартів, таких як ISO/IEC 27001, які визначають вимоги до систем управління інформаційною безпекою. Відповідність цим стандартам допомагає

організаціям забезпечити систематичний підхід до захисту інформаційних ресурсів та продемонструвати свою надійність партнерам і клієнтам.

Загалом, теоретичні аспекти управління інформаційною безпекою включають комплексний підхід до захисту інформаційних систем, що поєднує методи оцінки ризиків, розробку політик безпеки, моделювання загроз та вразливостей, а також дотримання нормативних вимог. Цей підхід дозволяє забезпечити високий рівень захищеності інформаційних активів у сучасному цифровому середовищі.

1.1 Основні поняття інформаційної безпеки

Інформаційна безпека є ключовим елементом забезпечення стабільного функціонування сучасних інформаційних систем та захисту інформаційних активів від різноманітних загроз. В умовах стрімкого розвитку інформаційних технологій та зростаючої залежності суспільства від цифрових даних, питання інформаційної безпеки набувають особливого значення. Основні поняття інформаційної безпеки формують фундаментальні принципи та підходи, на яких базуються всі подальші заходи щодо захисту інформаційних ресурсів. Вони визначають методи та механізми захисту інформації, що дозволяють забезпечити її конфіденційність, цілісність та доступність, а також автентичність, відповідальність, контроль доступу, аудит та управління ризиками.

Розуміння та інтеграція цих основних понять в рамках інформаційної безпеки дозволяє організаціям ефективно протистояти кіберзагрозам, запобігати втратам інформації та забезпечувати безперервність бізнес-процесів. Оскільки інформація стала одним з найцінніших активів у сучасному світі, захист цієї інформації стає пріоритетом для державних установ, приватних компаній та інших організацій [1].

Основні поняття інформаційної безпеки охоплюють різні аспекти захисту інформації: від технічних рішень до організаційних заходів. Вони забезпечують

комплексний підхід до управління безпекою, який включає не тільки впровадження технічних засобів захисту, але й розробку політик безпеки, навчання персоналу та постійний моніторинг і аудит інформаційних систем.

Розгляд ключових понять, які є основою для побудови ефективної системи інформаційної безпеки, дозволяє сформувати цілісне уявлення про принципи захисту інформації та методи їх реалізації на практиці. Вивчення та впровадження цих понять є необхідною умовою для створення надійної системи захисту інформаційних активів, яка здатна протистояти сучасним викликам та загрозам.

Основні поняття інформаційної безпеки становлять фундамент для розуміння та ефективного управління захистом інформаційних систем. Ці поняття включають конфіденційність, цілісність, доступність, автентичність, відповідальність, контроль доступу, аудит та управління ризиками (рис. 1.1).

Рис. 1.1 Основні поняття інформаційної безпеки

Конфіденційність визначається як властивість, що забезпечує доступ до інформації лише тим суб’єктам, які мають на це право. Це означає, що несанкціоновані особи не можуть отримати доступ до конфіденційної

інформації. Методи забезпечення конфіденційності включають шифрування даних, контроль доступу та використання захищених каналів зв'язку [2].

Конфіденційність визначається як право контролювати доступ до особистої інформації. Це означає, що особи мають право вирішувати, хто має доступ до їхньої інформації, як вона використовується та з якою метою.

Існує багато загроз конфіденційності в сфері ІБ, до яких належать:

- **несанкціонований доступ:** зловмисники можуть отримати доступ до особистої інформації через кібератаки, крадіжки даних або соціальну інженерію;
- **несанкціоноване використання:** особиста інформація може бути використана без згоди власника для таких цілей, як маркетинг, шахрайство або дискримінація;
- **розголошення:** особиста інформація може бути випадково або навмисно розголошена неавторизованим особам.

Існує ряд методів захисту конфіденційності в сфері ІБ, до яких належать:

- **контроль доступу:** обмеження доступу до особистої інформації лише авторизованим особам;
- **шифрування:** захист особистої інформації від несанкціонованого доступу за допомогою шифрування;
- **анонімність:** знеособлення особистої інформації, щоб захистити ідентичність власника;
- **псевдонімізація:** заміна особистої інформації псевдонімами, щоб захистити ідентичність власника.

Існує ряд правових та етичних аспектів конфіденційності в сфері ІБ. Закони про захист даних, такі як GDPR в ЄС, встановлюють правила збору, використання та розголошення особистої інформації. Етичні принципи, такі як принцип справедливості та інформаційної самовизначення, також відіграють важливу роль у захисті конфіденційності.

Конфіденційність є важливою складовою інформаційної безпеки. Захист конфіденційності особистої інформації необхідний для захисту прав та свобод людей у цифровому світі.

Цілісність відноситься до захисту інформації від несанкціонованих змін або знищення. Це означає, що дані повинні залишатися непошкодженими та достовірними. Забезпечення цілісності включає методи контролю версій, хешування, цифрові підписи та механізми виявлення змін [3].

Цілісність даних є одним з трьох основних принципів інформаційної безпеки, поряд з конфіденційністю та доступністю. Вона гарантує, що дані не були змінені несанкціоновано, випадково або внаслідок збою системи. Збереження цілісності даних є критичним для багатьох організацій, адже воно забезпечує:

- **точність та надійність даних:** дані, що використовуються для прийняття рішень, мають бути точними та неупередженими;
- **відповідність нормативним вимогам:** багато галузей, таких як фінанси та охорона здоров'я, мають суворі нормативні вимоги щодо захисту даних;
- **захист від шахрайства та кіберзлочинів:** зміна даних може призвести до фінансових втрат, крадіжки особистих даних та інших серйозних наслідків.

Існує багато загроз цілісності даних, як навмисних, так і ненавмисних. До *навмисних загроз* належать:

- **несанкціонований доступ:** зловмисники можуть отримати доступ до даних та змінити їх;
- **втручання:** зловмисники можуть втручатися в процес передачі даних та змінювати їх;
- **відмова в обслуговуванні:** зловмисники можуть блокувати доступ до даних або видаляти їх.

До *ненавмисних загроз* належать:

- **людська помилка:** співробітники можуть випадково змінити або видалити дані;
- **збої апаратного та програмного забезпечення:** збої можуть призвести до пошкодження даних;
- **стихійні лиха:** пожежі, повені та інші стихійні лиха можуть призвести до втрати даних.

Існує багато методів захисту цілісності даних, як програмних, так і апаратних. До ***програмних методів*** належать:

- контроль доступу.
- шифрування.
- електронні цифрові підписи.

До ***апаратних методів*** належать:

- системи резервного копіювання.
- системи стійкості до збоїв.
- системи виявлення та запобігання вторгненням.

Цілісність даних є критично важливою для будь-якої організації, яка використовує дані. Забезпечення цілісності даних допомагає захистити організацію від фінансових втрат, шкоди репутації та інших серйозних наслідків.

Цілісність даних є складним питанням, яке потребує комплексного підходу. Організації повинні використовувати різні методи для захисту цілісності своїх даних, як програмні, так і апаратні. Важливо також мати чітку політику та процедури щодо захисту даних та регулярно проводити навчання співробітників з питань інформаційної безпеки.

Доступність полягає в забезпеченні своєчасного та надійного доступу до інформації та ресурсів для авторизованих користувачів. Це означає, що системи повинні функціонувати без збоїв і бути доступними тоді, коли це необхідно. Засоби забезпечення доступності включають резервне копіювання, відновлення після збоїв, захист від відмов у обслуговуванні (DoS) та балансування навантаження.

Доступність є одним із трьох основних принципів інформаційної безпеки поряд з конфіденційністю та цілісністю. Вона гарантує, що авторизовані користувачі мають своєчасний та надійний доступ до інформаційних ресурсів та систем, коли їм це необхідно [4].

У сучасному цифровому світі доступність є критично важливою для багатьох організацій. Відсутність доступу до даних та систем може призвести до значних фінансових втрат, шкоди репутації та перешкод у виконанні важливих операцій.

Існує багато загроз доступності, які можуть спричинити перебої в роботі систем, такі як:

- **кібератаки:** зловмисники можуть використовувати різні методи, такі як ddos-атаки, викрадення програмного забезпечення та шкідливі програми, щоб порушити доступність систем;
- **відмови обладнання та програмного забезпечення:** навіть найнадійніші системи можуть вийти з ладу через збої обладнання, програмні помилки або людські помилки;
- **стихійні лиха:** природні катаклізми, такі як повені, землетруси та урагани, можуть пошкодити або знищити іт-інфраструктуру;
- **людські помилки:** ненавмисні дії користувачів, такі як видалення даних або скидання налаштувань, також можуть призвести до перебоїв у роботі.

Організації можуть вживати різних заходів для захисту доступності своїх інформаційних ресурсів, таких як:

- **резервне копіювання та відновлення:** регулярне резервне копіювання даних та систем гарантує, що їх можна швидко відновити у разі збою;
- **плани аварійного відновлення:** план аварійного відновлення описує дії, які необхідно вжити для відновлення систем та операцій у разі серйозного збою;

- **захист від кіберзагроз:** впровадження комплексних заходів кібербезпеки, таких як брандмауери, антивірусне програмне забезпечення та системи виявлення вторгнень, може допомогти захистити системи від кібератак;
- **підвищення стійкості до відмов:** використання надійного обладнання та програмного забезпечення, а також розміщення систем у дата-центрах з резервним живленням та охолодженням, може допомогти підвищити стійкість до відмов;
- **контроль доступу:** впровадження чітких правил контролю доступу може допомогти запобігти несанкціонованому доступу до систем та даних;
- **підготовка персоналу:** навчання персоналу основам іб та процедурам реагування на інциденти може допомогти мінімізувати ризик людських помилок.

Доступність є важливою складовою інформаційної безпеки. Організації повинні вживати комплексних заходів для захисту своїх інформаційних ресурсів від загроз доступності, щоб гарантувати, що авторизовані користувачі матимуть своєчасний та надійний доступ до них.

Автентичність забезпечує перевірку справжності користувачів та джерел даних. Це означає, що кожен суб’єкт чи ресурс, що взаємодіє з системою, має бути точно ідентифікований. Методи забезпечення автентичності включають паролі, біометричні дані, смарт-карти та криптографічні методи [5].

У сфері інформаційної безпеки автентичність позначає впевненість у тому, що те, чим воно здається, дійсно таким є. Це стосується користувачів, систем, даних та повідомлень.

Автентичність є фундаментальним принципом інформаційної безпеки, оскільки вона:

- **захищає від несанкціонованого доступу:** переконайтеся, що лише легітимні користувачі мають доступ до систем та даних;

- **запобігає шахрайству:** захищає від створення або маніпулювання даними з метою обману;
- **підтримує невідмовність:** гарантує, що користувачі не можуть заперечувати свої дії;
- **забезпечує конфіденційність:** дозволяє захищати конфіденційну інформацію від несанкціонованого розголошення.

Існує багато методів автентифікації, які можна використовувати для досягнення автентичності, включаючи:

- фактори знань.
- фактори володіння.
- фактори присутності.

Для забезпечення автентичності в системах інформаційної безпеки важливо використовувати надійні методи автентифікації та впроваджувати найкращі практики, такі як:

- **багатофакторна автентифікація:** використання декількох факторів автентифікації для підвищення рівня безпеки;
- **сильні паролі:** використання складних та унікальних паролів для всіх облікових записів;
- **регулярна зміна паролів:** періодична зміна паролів для зниження ризику їх компрометації;
- **захист факторів автентифікації:** захист факторів автентифікації, таких як фізичні токени, від втрати або крадіжки;
- **контроль доступу:** надання користувачам доступу лише до тих ресурсів, які їм необхідні для виконання своїх завдань;
- **моніторинг та реагування на інциденти:** постійний моніторинг систем на наявність підозрілих дій та швидке реагування на інциденти.

Автентичність є критично важливим аспектом інформаційної безпеки. Використання надійних методів автентифікації та впровадження найкращих практик може допомогти захистити системи та дані від несанкціонованого доступу, шахрайства та інших загроз [6].

Відповідальність визначається як можливість простежити дії користувачів та систем до їхніх джерел. Це забезпечує можливість визначення, хто, коли і які дії здійснював у системі. Відповідальність забезпечується за допомогою журналів аудиту, контрольних точок та протоколів обліку дій.

У сучасному цифровому світі інформаційна безпека (ІБ) стає дедалі більш критичною. Зростання кіберзагроз, таких як хакерські атаки, витоки даних та кібершпіонаж, робить захист інформаційних активів життєво важливим для як приватних осіб, так і організацій.

Відповідальність за ІБ лежить на всіх учасниках інформаційного середовища, від розробників програмного забезпечення та власників даних до окремих користувачів. Її можна розділити на декілька категорій:

1. Юридична відповідальність:

- **нормативно-правова база:** на національному та міжнародному рівні існує розгалужена система законодавчих актів та нормативних документів, що регулюють питання ІБ. ці акти визначають суб'єктів відповідальності за захист інформації, категорії даних, що потребують захисту, та санкції за порушення;
- **цивільно-правова відповідальність:** фізичні та юридичні особи несуть відповідальність за шкоду, завдану внаслідок порушення ІБ. це може включати відшкодування збитків, втрачені доходи та шкоду репутації;
- **кримінальна відповідальність:** у деяких випадках серйозні порушення ІБ можуть тягнути за собою кримінальну відповідальність, включаючи тюремне ув'язнення.

2. Операційна відповідальність:

- **впровадження політик та процедур:** організації повинні мати чітко визначені політики та процедури ІБ, що регламентують захист інформаційних активів. ці політики мають охоплювати аспекти контролю доступу, шифрування даних, резервного копіювання та реагування на інциденти;
- **навчання та обізнаність:** персонал має володіти базовими знаннями у сфері ІБ та розуміти свою роль у захисті інформаційних активів. це може

включати навчання з питань кібергігієни, розпізнавання фішингових атак та безпечного використання IT-систем [7];

- **впровадження технічних заходів:** організації повинні впроваджувати технічні заходи для захисту інформаційних активів, такі як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення.

3. Етична відповідальність:

- **захист конфіденційності:** організації та особи мають етичну відповідальність за захист конфіденційності даних. це означає, що дані повинні збиратися, використовуватися та розкриватися лише законним і етичним способом;
- **відповідальне розкриття інформації:** у деяких випадках може бути етично виправданим розкриття інформації, навіть якщо це суперечить закону або політиці організації. це може бути зроблено, наприклад, для захисту людей від шкоди або для викриття корупції.

4. Соціальна відповідальність:

- **захист критичної інфраструктури:** кібератаки на критичну інфраструктуру, таку як електромережі та транспортні системи, можуть мати руйнівні наслідки для суспільства. тому організації, які володіють або експлуатують критичну інфраструктуру, несуть особливу відповідальність за її захист;
- **підвищення обізнаності про кібербезпеку:** організації та особи можуть відігравати важливу роль у підвищенні обізнаності про кібербезпеку в суспільстві. це може бути зроблено шляхом проведення освітніх кампаній, підтримки досліджень у галузі іб та співпраці з правоохоронними органами.

Контроль доступу охоплює методи та механізми, що обмежують доступ до ресурсів системи тільки авторизованим користувачам. Це включає механізми автентифікації та авторизації, рольові моделі доступу, списки контролю доступу (ACL) та політики безпеки.

Контроль доступу є одним з фундаментальних принципів інформаційної безпеки, що ґрунтується на обмеженні доступу до інформаційних ресурсів

лише авторизованим користувачам. Його мета – захистити конфіденційність, цілісність та доступність інформації, запобігаючи несанкціонованому доступу, використанню, розголошенню, зміні або знищенню даних.

Основні концепції контролю доступу:

- **суб'єкт:** користувач або процес, який ініціює запит на доступ до інформаційного ресурсу;
- **об'єкт:** інформаційний ресурс, до якого запитується доступ, наприклад, файл, база даних або мережевий пристрій;
- **суб'єкт-об'єктне відношення:** відношення між суб'єктом та об'єктом, яке визначає, чи має суб'єкт доступ до об'єкта та який рівень доступу йому надається;
- **механізм:** засіб, що використовується для реалізації політики, наприклад, списки контролю доступу, брандмауери або системи автентифікації;
- **політика:** набір правил, які визначають, хто має доступ до яких інформаційних ресурсів та який рівень доступу їм надається.

Зростання нових технологій, таких як хмарні обчислення, Інтернет речей та штучний інтелект, створює нові виклики для контролю доступу.

Аудит включає систематичний процес збору та аналізу даних про дії користувачів та систем. Мета аудиту полягає у виявленні порушень політик безпеки, забезпеченні відповідності нормативним вимогам та оцінці ефективності заходів безпеки. Аудит включає моніторинг систем, аналіз журналів та звітність [8].

Аудит інформаційної безпеки - це комплексний процес системного аналізу та оцінки інформаційної системи з метою виявлення та оцінки ризиків ІБ, а також їх впливу на конфіденційність,

Аудит є важливим інструментом для забезпечення ІБ організації. Він дозволяє виявити та усунути потенційні загрози, перш ніж вони призведуть до серйозних наслідків. Регулярний аудит ІБ може допомогти організаціям захистити свої інформаційні активи, підвищити рівень довіри клієнтів та партнерів, а також зберегти свою репутацію.

Управління ризиками є процесом ідентифікації, оцінки та контролю ризиків, що можуть вплинути на інформаційні активи. Це включає аналіз вразливостей, оцінку ймовірностей реалізації загроз та розробку стратегій для мінімізації ризиків. Управління ризиками включає методи кількісної та якісної оцінки, а також планування та впровадження контрзаходів.

У сучасному цифровому середовищі, де інформація стає активом першочергової ваги, управління ризиками в сфері інформаційної безпеки набуває критичного значення. Зростання кіберзагроз, таких як хакерські атаки, витоки даних та кібершпіонаж, робить захист інформаційних активів життєво необхідним для як приватних осіб, так і організацій [9].

Управління ризиками – це системний процес, спрямований на виявлення, аналіз, оцінку та пріоритезацію ризиків для інформаційних активів, а також на розробку та впровадження заходів з їх мінімізації. Цей процес ґрунтується на наукових методах та принципах, що дозволяє приймати обґрунтовані та ефективні рішення щодо захисту інформації.

Ключові етапи управління ризиками ІБ:

- **ідентифікація ризиків:** на цьому етапі визначаються всі потенційні загрози для інформаційних активів, такі як зловмисні дії, технічні збої, людські помилки та стихійні лиха;
- **аналіз ризиків:** проводиться оцінка ймовірності виникнення кожного ризику та його потенційного впливу на інформаційні активи;
- **оцінка ризиків:** визначається загальний рівень ризику для кожного інформаційного активу, ґрунтуючись на ймовірності та впливі ризиків.
- **обробка ризиків:** розробляються та впроваджуються заходи з мінімізації ризиків, такі як технічні заходи, організаційні заходи та процедури, навчання персоналу;
- **моніторинг та контроль:** постійно здійснюється моніторинг ризиків та ефективності вжитих заходів з їх мінімізації. за потреби проводяться корективи в процесі управління ризиками.

Розгляд основних понять інформаційної безпеки дозволяють підсумувати важливі аспекти, що формують фундамент цієї дисципліни та визначають підходи до забезпечення захисту інформаційних систем.

Конфіденційність, цілісність та доступність інформації є базовими принципами, що лежать в основі будь-якої стратегії інформаційної безпеки. Ці поняття забезпечують захист від несанкціонованого доступу, модифікації та порушення доступності даних. Конфіденційність гарантує, що інформація доступна лише авторизованим суб'єктам, цілісність забезпечує збереження даних у незмінному стані, а доступність гарантує своєчасний доступ до ресурсів для авторизованих користувачів.

Автентичність та відповідальність є важливими аспектами, що забезпечують контроль над доступом та відслідковуванням дій користувачів. Автентичність дозволяє ідентифікувати та перевіряти справжність суб'єктів, що взаємодіють з системою, що є критично важливим для запобігання несанкціонованому доступу. Відповідальність, у свою чергу, забезпечує можливість простежити дії користувачів та систем до їхніх джерел, що є ключовим для розслідування інцидентів та забезпечення дотримання політик безпеки.

Контроль доступу є фундаментальним механізмом, що обмежує доступ до ресурсів системи лише авторизованим суб'єктам. Реалізація ефективного контролю доступу включає політики доступу, автентифікацію та авторизацію користувачів, що забезпечує захист від несанкціонованих дій та збереження конфіденційності та цілісності даних.

Аудит та управління ризиками є важливими елементами, що дозволяють оцінювати та контролювати стан інформаційної безпеки. Аудит забезпечує моніторинг та аналіз дій у системі, дозволяючи виявляти порушення та оцінювати ефективність заходів безпеки. Управління ризиками включає ідентифікацію, оцінку та контроль ризиків, що дозволяє організаціям розробляти адекватні стратегії захисту та оптимізувати витрати на безпеку [10].

Розуміння та впровадження основних понять інформаційної безпеки є критично важливими для створення надійної системи захисту інформаційних активів. Ці поняття забезпечують комплексний підхід до захисту, що включає технічні, організаційні та процедурні заходи. Інтеграція цих принципів у практику управління інформаційною безпекою дозволяє організаціям ефективно протистояти сучасним загрозам, забезпечувати безперервність бізнес-процесів та дотримання нормативних вимог.

1.2 Методи та моделі управління інформаційною безпекою

Управління інформаційною безпекою– це комплексна задача, що потребує застосування різноманітних методів та моделей для ефективного захисту інформаційних активів. Ці методи та моделі ґрунтуються на наукових принципах та практиках, що дозволяють приймати обґрунтовані та дієві рішення щодо захисту інформації.

Класифікація методів та моделей управління ІБ:

1. За цілями:

- методи аналізу ризиків.
- методи оцінки ефективності.
- методи аудиту.
- методи планування та впровадження.

2. За сферою застосування:

- методи захисту інформаційних систем.
- методи захисту даних.
- методи управління доступом.
- методи захисту інформаційних активів.

3. За підходом:

- кількісні методи.
- якісні методи.
- комбіновані методи.

Приклади методів та моделей управління ІБ:

- метод концентричних кіл.
- модель cobit.
- метод nist sp 800-30.
- метод diip-н 08-01:2016.

Наукові основи методів та моделей управління ІБ:

- теорія інформаційної безпеки.
- кількісний аналіз ризиків.
- теорія прийняття рішень.
- системний аналіз.

Вибір методів та моделей управління ІБ залежить від багатьох факторів, таких як розмір та складність організації, тип інформаційних активів, бюджет та рівень ризику. Важливо, щоб методи та моделі відповідали потребам та можливостям організації.

Методи та моделі управління ІБ – це важливі інструменти для захисту інформаційних активів. Науковий підхід до вибору та застосування цих методів та моделей дозволяє приймати обґрунтовані та дієві рішення щодо захисту інформації, ґрунтуючись на даних та фактах [11].

1.3 Стандарти в галузі інформаційної безпеки

У сучасному цифровому середовищі, де інформація стає активом першочергової ваги, стандарти в галузі інформаційної безпеки відіграють критичну роль у захисті інформаційних активів від кіберзагроз. Ці стандарти визначають набір правил, рекомендацій та найкращих практик, які допомагають організаціям та приватним особам впроваджувати ефективні системи ІБ.

Види стандартів ІБ:

- міжнародні стандарти: розробляються міжнародними організаціями, такими як ISO/IEC (міжнародна організація зі стандартизації та міжнародна

електротехнічна комісія) та ITU (міжнародний союз електрозв'язку). Ці стандарти мають глобальне значення та слугують основою для національних стандартів та законодавства [12].

- національні стандарти: розробляються національними організаціями зі стандартизації та адаптуються до специфічних потреб країни.
- галузеві стандарти: розробляються профільними організаціями та застосовуються до певної галузі або сфери діяльності.
- внутрішні стандарти: розробляються окремими організаціями для регулювання їх внутрішньої інформаційної безпеки.

Приклади ключових стандартів ІБ:

- **ISO/IEC 27001:2013:** цей міжнародний стандарт визначає вимоги до систем менеджменту інформаційної безпеки (СМІБ). СМІБ допомагає організаціям систематично керувати ризиками ІБ та забезпечувати відповідність найкращим практикам
- **NIST SP 800-53:** цей стандарт Національного інституту стандартів і технологій (NIST) США містить рекомендації щодо управління ризиками ІБ. Він описує процес виявлення, аналізу, оцінки та обробки ризиків ІБ.
- **ISO/IEC 27002:2022:** цей міжнародний стандарт наводить кодекс найкращих практик з управління ІБ. Він містить 14 категорій контролів ІБ, які охоплюють широкий спектр аспектів, таких як контроль доступу, шифрування даних, резервне копіювання та реагування на інциденти.
- **ДСТУ 28001:2004:** цей національний стандарт України визначає вимоги до СМІБ. Він ґрунтується на ISO/IEC 27001:2005 та адаптований до потреб України.

Переваги використання стандартів ІБ:

- підвищення рівня ІБ: стандарти забезпечують чітку структуру та методику для управління ризиками ІБ та впровадження ефективних заходів захисту.

- зменшення кількості кіберінцидентів: дотримання стандартів ІБ може допомогти зменшити ймовірність виникнення кіберінцидентів та пом'якшити їх наслідки.
- підвищення довіри: відповідність стандартам іб може підвищити довіру клієнтів, партнерів та інших зацікавлених сторін до організації.
- покращення економії коштів: запобігання кіберінцидентам та зменшення їх наслідків може допомогти організаціям заощадити кошти.
- гармонізація з законодавством: багато стандартів іб ґрунтуються на законодавчих вимогах або відповідають їм, що допомагає організаціям дотримуватися законів.

З розвитком нових технологій та зростанням кіберзагроз стандарти ІБ повинні постійно оновлюватися та адаптуватися. Очікується, що в майбутньому стандарти ІБ стануть більш динамічними та гнучкими, а також більше орієнтованими на кіберстійкість та управління ризиками [13].

Стандарти в галузі інформаційної безпеки відіграють важливу роль у захисті інформаційних активів від кіберзагроз. Вони надають організаціям та приватним особам чітку структуру та методику для управління ризиками ІБ та впровадження ефективних заходів захисту. Незважаючи на деякі виклики, впровадження та підтримка стандартів ІБ є важливою інвестицією, яка може допомогти організаціям підвищити рівень ІБ, зменшити кількість кіберінцидентів та заощадити кошти.

Висновки до розділу 1

Інформаційна безпека – це багатогранна сфера, що охоплює комплекс заходів, спрямованих на захист інформаційних активів від несанкціонованого доступу, використання, розкриття, зміни, знищення або порушення їх цілісності.

Забезпечення того, щоб інформація доступна лише авторизованим особам, захист інформації від несанкціонованих змін, забезпечення того, щоб авторизовані особи мали доступ до інформації, коли це необхідно, забезпечення того, щоб не можна було заперечити факт виконання транзакції або події, забезпечення того, щоб дії з інформацією можна було відстежити та за них можна було нести відповідальність – все це включають в себе ключові поняття ІБ.

Для управління ІБ використовується широкий спектр методів та моделей, що дозволяють організаціям та приватним особам систематично та ефективно захищати свої інформаційні активи.

Стандарти ІБ відіграють важливу роль у забезпеченні єдиного підходу до захисту інформаційних активів. Вони надають організаціям та приватним особам чітку структуру та методику для впровадження ефективних систем ІБ.

Розуміння основних понять ІБ - конфіденційності, цілісності, доступності, незаперечності та підзвітності - є ключовим для розробки та впровадження ефективних стратегій захисту інформаційних активів.

Використання методів та моделей управління ІБ - таких як аналіз ризиків, впровадження заходів захисту, контроль та моніторинг, навчання та обізнаність - дозволяє систематично та еф

Дотримання стандартів ІБ - ISO/IEC 27001, NIST SP 800-53, ISO/IEC 27002, ДСТУ 28001:2004 - надає організаціям та приватним особам чітку структуру та методику для впровадження ефективних систем ІБ.

Розділ 2 АНАЛІЗ ПРАКТИК ЩОДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ НІОРФМАЦІНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

2.1 Методичні підходи щодо побудови системи управління інформаційною безпекою і їх ефективності

У сучасному інформаційному суспільстві забезпечення надійного захисту інформаційних ресурсів є однією з ключових задач для будь-якої організації. Побудова ефективної системи управління інформаційною безпекою (СУІБ) вимагає комплексного підходу, що включає різноманітні методи та засоби для виявлення, оцінки та управління ризиками інформаційної безпеки. Відповідні методичні підходи повинні враховувати специфіку організації, її інформаційні потоки та можливі загрози. Ефективність таких систем визначається здатністю своєчасно реагувати на інциденти, мінімізувати ризики та забезпечувати безперервність бізнес-процесів.[47, 48]

Основними методичними підходами є ризик-орієнтований, нормативно-правовий, технічний, організаційний та проактивний (див. рис.2.1).

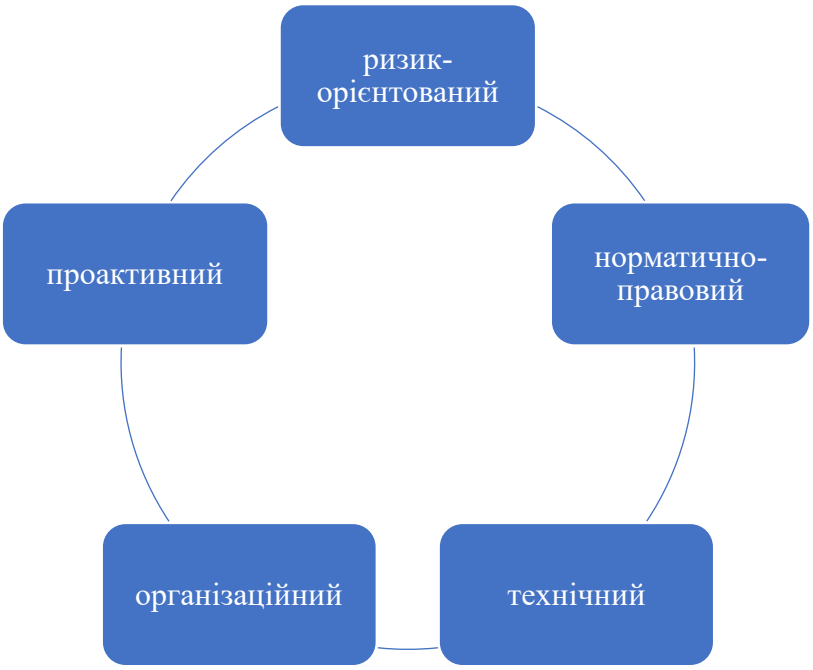

Рис. 2.1 Основні методичні підходи

Ризик-орієнтований підхід є фундаментальним у побудові СУІБ. Він передбачає ідентифікацію, аналіз та оцінку ризиків, пов'язаних з інформаційною безпекою, з метою визначення пріоритетних заходів захисту. Цей підхід дозволяє організаціям ефективно розподіляти ресурси, зосереджуючи їх на найбільш критичних зонах.

Дотримання нормативно-правових вимог є обов'язковою умовою для будь-якої системи управління інформаційною безпекою. Нормативно-правовий підхід передбачає врахування міжнародних стандартів, таких як ISO/IEC 27001, а також національних законодавчих актів, що регулюють питання захисту інформації [14].

Технічний підхід включає використання спеціалізованого програмного та апаратного забезпечення для забезпечення інформаційної безпеки. Це можуть бути системи виявлення та попередження вторгнень (IDS/IPS), антивірусні програми, засоби шифрування та інші технологічні рішення.

Організаційний підхід передбачає розробку та впровадження політик, процедур та регламентів, що регулюють процеси управління інформаційною безпекою. Важливою складовою є навчання та підвищення кваліфікації персоналу, а також створення культури інформаційної безпеки в організації.

Проактивний підхід спрямований на попередження інцидентів інформаційної безпеки шляхом регулярного моніторингу, аналізу вразливостей та проведення аудиту безпеки. Це дозволяє виявляти потенційні загрози на ранніх стадіях та вживати необхідних заходів для їх нейтралізації.

Особливості побудови системи управління ризиками. Побудова системи управління ризиками є однією з ключових складових забезпечення стабільного та безпечного функціонування організації. В умовах сучасної економіки та високої динаміки змін у зовнішньому середовищі, ефективне управління ризиками дозволяє ідентифікувати, оцінювати та управляти потенційними загрозами, які можуть впливати на досягнення стратегічних

цілей організації. Цей процес вимагає системного підходу, який враховує специфіку діяльності організації та передбачає інтеграцію управління ризиками в усі бізнес-процеси. Процес побудови системи управління ризиками представлений на рис.2.2.

Рис. 2.2 Процес побудови системи управління ризиками [15]

Побудова системи управління ризиками вимагає системного підходу, що включає кілька ключових етапів. Перший етап – це визначення контексту, в якому функціонує організація. Він передбачає аналіз внутрішнього та зовнішнього середовища, виявлення факторів, що можуть впливати на діяльність, а також визначення ключових зацікавлених сторін та їхніх очікувань. Це дозволяє встановити межі та рамки для подальшого управління ризиками. Наступний важливий етап – ідентифікація ризиків, яка полягає у виявленні всіх потенційних загроз, що можуть вплинути на досягнення цілей організації. Для цього використовуються методи, такі як мозковий штурм, аналіз сценаріїв, SWOT-аналіз та консультації з експертами. Важливо залучати до цього процесу представників усіх підрозділів організації, щоб забезпечити всебічний погляд на можливі ризики.

Після ідентифікації ризиків необхідно провести їх оцінку. Оцінка включає визначення ймовірності виникнення кожного ризику та його потенційного впливу на організацію, що дозволяє пріоритезувати ризики та виділити найбільш критичні з них. Для цього можуть використовуватися як

кількісні, так і якісні методи, такі як аналіз чутливості, аналіз впливу, моделювання та симуляції. На основі результатів оцінки ризиків розробляються стратегії управління, які можуть включати уникнення ризиків, зменшення їхнього впливу, передавання ризиків або їх прийняття. Вибір стратегії залежить від характеру ризику, його ймовірності, можливих наслідків та ресурсів, які організація готова витратити на управління цим ризиком [16].

Впровадження заходів з управління ризиками включає реалізацію обраних стратегій та контроль їхньої ефективності. Це передбачає розробку конкретних планів дій, призначення відповідальних осіб та встановлення строків виконання. Важливо, щоб заходи з управління ризиками були інтегровані в повсякденну діяльність організації та підтримувалися на всіх рівнях. Завершальним етапом процесу управління ризиками є моніторинг та перегляд. Це включає постійний контроль за змінами у зовнішньому та внутрішньому середовищі, перегляд і оцінку ефективності реалізованих заходів та коригування стратегій за необхідності. Регулярний моніторинг дозволяє своєчасно виявляти нові ризики та оперативно реагувати на них.

Таким чином, побудова ефективної системи управління ризиками є складним процесом, що вимагає інтеграції в усі аспекти діяльності організації. Визначення контексту, ідентифікація та оцінка ризиків, розробка та впровадження стратегій управління ризиками, а також постійний моніторинг і перегляд є ключовими етапами цього процесу. Ефективне управління ризиками дозволяє організації знижувати невизначеність, забезпечувати стійкість до зовнішніх та внутрішніх загроз та досягати стратегічних цілей у динамічному та конкурентному середовищі.

Представлена на рис. 2.3. схема моделі управління ризиками на підприємстві доповнює попередній опис методів, висвітлюючи ключові етапи цього процесу. Модель охоплює етапи планування і забезпечення, функціонування та оцінки результатів, що дозволяє систематично підходити до ідентифікації, аналізу та управління ризиками. Важливими аспектами є оцінка життєвого циклу підприємства, цільових показників діяльності, контексту

підприємства, управління політикою ризиків, ресурсів та компетенцій персоналу. Таким чином, інтеграція теоретичних підходів з практичними аспектами, зображеними на схемі, сприяє побудові ефективної системи управління ризиками, що забезпечує стійкість та безпеку підприємства.

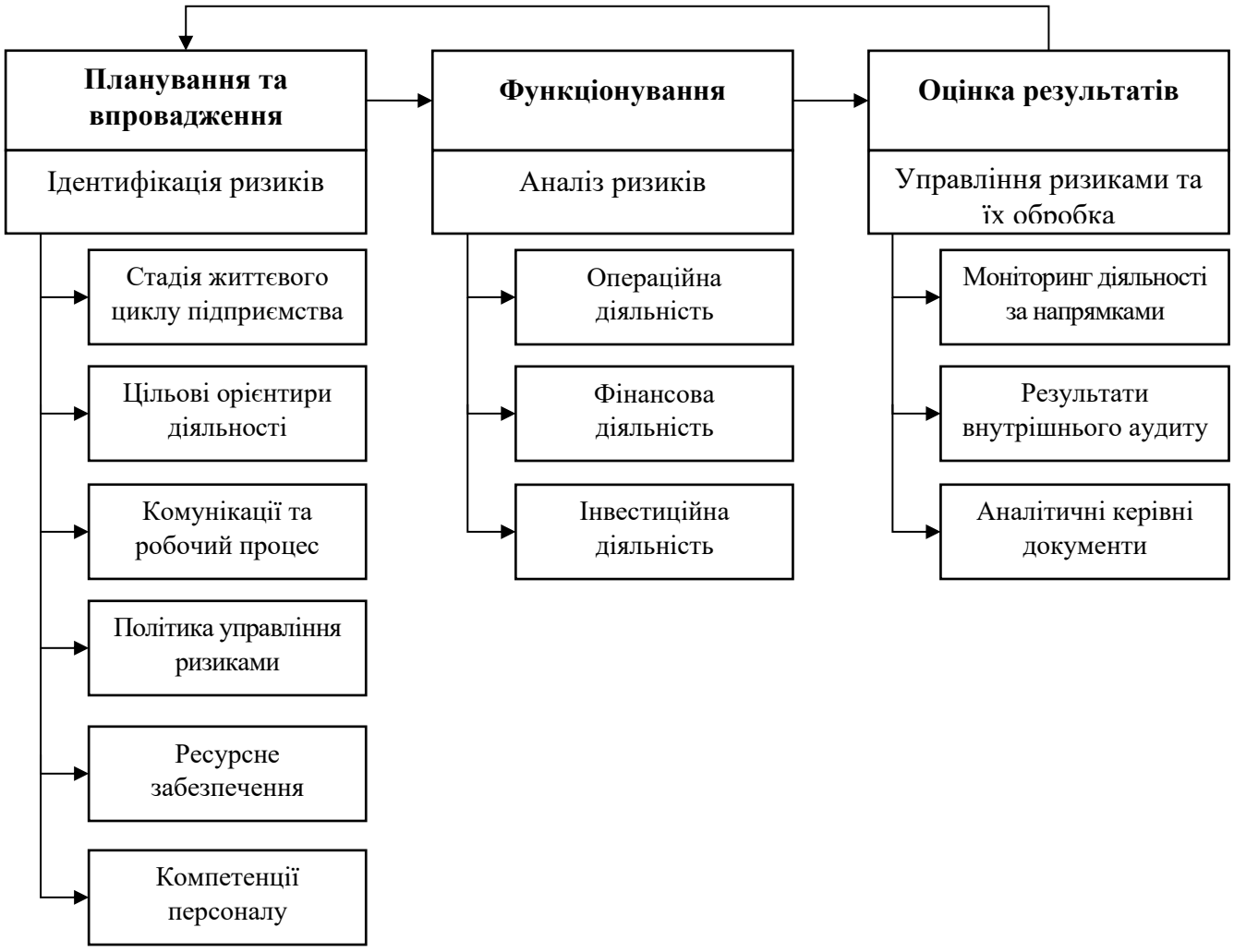

Рис. 2.3 Схема моделі управління ризиками на підприємстві [17]

Схема моделі управління ризиками на підприємстві складається з трьох основних етапів: планування та забезпечення, функціонування, а також оцінки результатів. На першому етапі, що стосується планування та забезпечення, відбувається ідентифікація ризиків, що включає визначення стадії життєвого циклу підприємства, цільових показників діяльності, контексту підприємства (включаючи комунікації та робочі процеси), політики управління ризиками, ресурсів та компетенцій персоналу. Цей етап є критичним для створення

основи для подальшого управління ризиками, забезпечуючи розуміння внутрішніх і зовнішніх чинників, які можуть вплинути на діяльність підприємства.

Другий етап, функціонування, охоплює аналіз ризиків, зосереджений на операційній, фінансовій та інвестиційній діяльності підприємства. Аналіз ризиків на цьому етапі передбачає детальне вивчення кожного аспекту діяльності підприємства для виявлення потенційних загроз та оцінки їхнього впливу на різні бізнес-процеси. Операційна діяльність охоплює повсякденні бізнес-процеси, тоді як фінансова діяльність включає управління фінансовими ресурсами та зобов'язаннями. Інвестиційна діяльність, у свою чергу, пов'язана з управлінням інвестиційними проектами та оцінкою їхніх ризиків. Аналіз ризиків на цьому етапі дозволяє виявити слабкі місця в різних сферах діяльності підприємства та розробити стратегії для їхнього мінімізації [18].

Третій етап, оцінка результатів, передбачає управління та обробку ризиків. Це включає моніторинг діяльності за напрямками, результати внутрішнього аудиту та підготовку аналітичних документів. Моніторинг діяльності забезпечує постійний контроль за виконанням заходів управління ризиками та своєчасне виявлення відхилень від запланованих показників. Внутрішній аудит дозволяє оцінити ефективність впроваджених заходів управління ризиками, виявити можливі недоліки та розробити рекомендації щодо їхнього усунення. Аналітичні документи, підготовлені на основі результатів моніторингу та аудиту, забезпечують керівництво підприємства інформацією для прийняття обґрунтованих рішень щодо подальшого управління ризиками.

Особливості побудови системи управління інцидентами інформаційної безпеки. Розробка комплексної системи управління інцидентами інформаційної безпеки (ISIMF) є критично важливим процесом, який гарантує, що організація може ефективно реагувати на інциденти безпеки та пом'якшувати їхній вплив. Цей процес охоплює кілька ключових етапів:

планування та підготовка, виявлення та звітування, оцінка та прийняття рішень, реагування та засвоєння уроків (рис.2.4). Кожна фаза покликана створити надійну систему управління інцидентами, від початкового планування та розробки політики до проактивного виявлення загроз, ефективної оцінки інциденту, ефективних стратегій реагування та постійного вдосконалення на основі минулого досвіду. Кінцевою метою є створення стійкої та адаптивної системи, яка підвищує здатність організації захищати свої інформаційні активи від кіберзагроз, що еволюціонують.

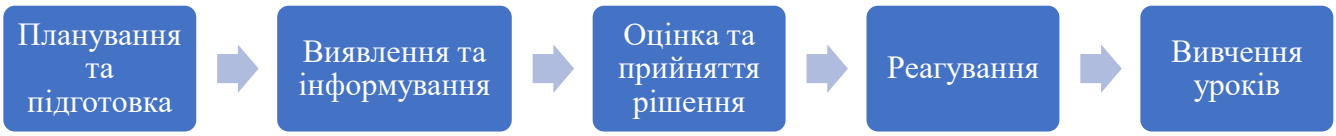

Рис. 2.4 Розробка комплексної системи управління інцидентами інформаційної безпеки [19]

Етап "Планування та підготовка" має вирішальне значення для створення ефективної системи управління інцидентами в організації. Цей етап передбачає визначення обсягу та контексту подій та інцидентів інформаційної безпеки за допомогою чітких визначень та критеріїв. Він передбачає встановлення порогових значень для розмежування подій та інцидентів, а також класифікацію інцидентів для оптимізації процесу реагування. Крім того, вона охоплює документування організаційних зобов'язань, включно з нормативними, правовими та контрактними вимогами. Політики розробляються для того, щоб сформулювати наміри та цілі організації, забезпечуючи узгодженість з більш широкими рамками управління ризиками. Потім ці політики доводяться до відома всіх зацікавлених сторін, щоб забезпечити єдине розуміння та впровадження в організації.

Крім того, на цьому етапі розробляється комплексний план впровадження, в якому визначаються ресурси і дії, необхідні для створення і

підтримки системи управління інцидентами. Цей план повинен отримати схвалення керівництва для забезпечення організаційної прихильності та підтримки. Для моніторингу ефективності системи визначаються показники результативності, що дозволяють проводити постійну оцінку та вдосконалення. Завдяки ретельному плануванню та підготовці організації можуть побудувати міцну основу для управління інцидентами інформаційної безпеки, що в кінцевому підсумку підвищить їхню стійкість до кіберзагроз. Цей етап гарантує, що всі необхідні компоненти, включаючи політики, процеси та ресурси, наявні та узгоджені із загальною стратегією управління ризиками організації.

Етап "Виявлення та інформування" має важливе значення для проактивного виявлення та повідомлення про загрози та вразливості в інформаційних системах організації. Цей етап включає проведення комплексного аналізу загроз і вразливостей для розуміння еволюції ландшафту загроз і виявлення потенційних прогалин у безпеці. Створюються системи моніторингу безпеки для забезпечення безперервного нагляду за мережевою діяльністю з використанням передових технологій для виявлення аномалій та підозрілої поведінки. Визначаються індикатори інцидентів для розпізнавання потенційних подій у сфері безпеки, а також встановлюються пороги тривоги для забезпечення своєчасного реагування. Такий системний підхід дозволяє виявляти інциденти безпеки на ранніх стадіях, що сприяє оперативному повідомленню про них та вжиттю заходів для їхнього усунення [20]. Створивши надійні механізми виявлення та звітування, організації можуть підвищити свою здатність ефективно реагувати на загрози, тим самим мінімізуючи вплив потенційних порушень безпеки. Постійний моніторинг та регулярні оцінки гарантують, що організація залишається пильною та адаптивною до нових загроз, підтримуючи стійку позицію безпеки.

Етап "Оцінка та прийняття рішення" має вирішальне значення для визначення належного реагування на події безпеки. На цьому етапі організації систематично оцінюють події безпеки, щоб визначити, чи є вони інцидентами,

які потребують втручання. Цей процес передбачає проведення сортування для визначення пріоритетності подій на основі їхньої серйозності та потенційного впливу. Своєчасна оцінка має вирішальне значення для забезпечення оперативного реагування, а інциденти класифікуються для оптимізації зусиль з реагування. Залучення профільних експертів має важливе значення для проведення поглибленого аналізу, який дає уявлення про характер і масштаби інцидентів. Точно оцінюючи та класифікуючи події безпеки, організації можуть ефективно розподіляти ресурси та впроваджувати цілеспрямовані стратегії реагування. Цей етап забезпечує структурований підхід до управління інцидентами, підвищуючи здатність організації зменшувати ризики та мінімізувати наслідки порушень безпеки. Безперервне оцінювання та вдосконалення процесів оцінювання ще більше посилюють можливості організації в управлінні інцидентами, забезпечуючи готовність до нових загроз.

Етап "Реагування" є ключовим у забезпеченні вжиття відповідних заходів для управління та пом'якшення наслідків інцидентів інформаційної безпеки. Цей етап охоплює низку заходів, спрямованих на ефективне реагування та вирішення інцидентів. Початкові кроки включають ретельне розслідування, щоб зрозуміти характер і масштаби інциденту, з подальшою передачею справи відповідним органам, якщо це необхідно. Впроваджуються стратегії локалізації для запобігання подальшої шкоди, які можуть включати ізоляцію уражених систем або мереж. Паралельно з цим ретельно збираються і зберігаються докази для підтримки потенційних судових позовів і криміналістичного аналізу [21].

Зусилля також спрямовані на усунення першопричини інциденту шляхом усунення вразливостей або недоліків у системі. Ініціюються процедури відновлення для відновлення нормальної роботи та мінімізації часу простою, забезпечуючи безперервність бізнесу. На цьому етапі важлива ефективна комунікація з усіма зацікавленими сторонами, включаючи внутрішні команди, зовнішніх партнерів і регуляторні органи, для підтримки прозорості та координації зусиль з реагування. Своєчасне вирішення інциденту є ключовим завданням, спрямованим на швидке відновлення порушених послуг та

пом'якшення будь-яких негативних наслідків для організації. Такий структурований підхід забезпечує комплексне реагування на інциденти безпеки, підвищуючи стійкість організації та її здатність протистояти майбутнім загрозам. Постійне вдосконалення та уточнення стратегій реагування є невід'ємною частиною цього етапу, забезпечуючи готовність до еволюції кіберзагроз.

Етап "Вивчення уроків" є невід'ємною частиною постійного вдосконалення системи управління інцидентами. Цей етап передбачає проведення ретельного аналізу після інциденту, щоб проаналізувати ефективність реагування та визначити сфери, які потребують вдосконалення. Висновки, отримані в результаті цих аналізів, ретельно документуються і використовуються для оновлення програм підвищення обізнаності з питань безпеки, забезпечуючи інформування співробітників і зацікавлених сторін про найкращі практики та нові загрози. Обмін інформацією сприяє розвитку спільного підходу до управління інцидентами, що дозволяє поширювати цінні уроки по всій організації. Докази інцидентів збираються та зберігаються для підтримки майбутніх розслідувань та аудитів, забезпечуючи дотримання законодавчих та нормативних вимог. Регулярні аудити та огляди системи управління інцидентами проводяться для оцінки її ефективності та внесення необхідних коректив. Цей ітеративний процес оцінки та вдосконалення гарантує, що система залишається надійною та адаптивною, здатною реагувати на мінливий ландшафт кіберзагроз. Інтегруючи отриманий досвід у постійні тренінги та оновлення процедур, організації можуть побудувати стійку систему безпеки, яка постійно розвивається, щоб відповідати новим викликам [22].

Отже, розробка системи управління інцидентами інформаційної безпеки є життєво важливим процесом для будь-якої організації, яка прагне захистити свої інформаційні активи. Систематично плануючи, виявляючи, оцінюючи, реагуючи та вивчаючи інциденти, організації можуть побудувати стійку та адаптивну систему безпеки. Такий комплексний підхід забезпечує готовність до нових кіберзагроз, сприяє ефективному управлінню інцидентами та постійному

вдосконаленню практик безпеки, що в кінцевому підсумку захищає діяльність організації та її репутацію.

Особливості побудови системи управління вразливостями інформаційної безпеки. Незалежно від того, чи вирішить організація віддати управління вразливостями на аутсорсинг СУВІБ або розробити власну програму, команда менеджменту буде тісно співпрацювати з командою управління оновленнями, щоб допомогти визначити процес застосування виправлень у безпечний спосіб.

Щоб почати будувати ефективну програму, є сім ключових кроків, які слід врахувати при впровадженні системи управління вразливостями, що зображені на рис. 2.5.

Рис. 2.5 Побудова системи управління вразливостями інформаційної безпеки [23]

Першим кроком у розробці надійної системи управління вразливостями є проведення комплексної інвентаризації всіх пристроїв і технологій, які впливають на роботу організації. Важливо створити і підтримувати детальний реєстр всіх активів, включаючи робочі станції, ноутбуки, сервери та інші мережеві пристрої. Цей реєстр повинен містити критично важливу інформацію,

таку як типи використовуваних операційних систем (наприклад, Mac або PC), кількість мобільних пристроїв з доступом до VPN, а також географічне розташування центрів обробки даних організації. Картографування та документування цих активів допомагає виявити потенційні вразливості та створити основу для ефективного управління вразливостями. Розуміння повного ландшафту технологічних активів дозволяє організаціям краще передбачати та зменшувати ризики безпеки, забезпечуючи стійкість та безпеку IT-середовища.

Другий крок у системі управління вразливостями передбачає виявлення та класифікацію вразливостей. Це досягається за допомогою комплексного сканування вразливостей мережі та додатків організації. Ці перевірки проводяться з інтервалами, визначеними потребами організації, які можуть бути щоденними, щотижневими або щомісячними. Результати використовуються для класифікації ризиків на основі активів та рівня серйозності виявлених вразливостей, таких як високий, середній або низький. Подальші заходи з усунення вразливостей визначаються за пріоритетністю відповідно до цих рівнів серйозності. Така систематична категоризація не лише визначає пріоритетність факторів ризику, але й генерує метрики з плином часу, надаючи цінну інформацію про стан безпеки організації та ефективність зусиль з усунення вразливостей. Такий методичний підхід гарантує, що найбільш критичні вразливості будуть оперативно усунені, тим самим посилюючи загальну систему безпеки організації [24].

Третім кроком у створенні системи управління вразливостями є розробка пакетів виправлень, що передбачає складання та аналіз необхідних дій для усунення виявлених вразливостей. Цей процес має вирішальне значення для негайного усунення вразливостей, управління відставанням та передбачення майбутніх ризиків. Ретельне дослідження залежностей виправлень має важливе значення, і всі виправлення повинні бути ретельно перевірені, щоб переконатися, що вони не створюють нових проблем. Потім слід провести аналіз впливу, щоб визначити спосіб дій, який принесе найбільшу користь з

найменшим ризиком для виробництва. Цей аналіз допомагає визначити пріоритетність заходів з усунення недоліків і забезпечити оперативне усунення критичних вразливостей, мінімізуючи при цьому потенційні збої в роботі системи. Такий структурований підхід гарантує, що IT-середовище організації залишається безпечним і стійким до нових загроз.

Четвертий крок у структурі управління вразливостями передбачає тестування пакету заходів з усунення наслідків. Використовуючи результати аналізу впливу та досліджень, процес виправлення слід спочатку застосувати до систем нижчого рівня або невиробничих систем. Цей етап тестування є критично важливим для спостереження та звітування про результати роботи після виправлення, гарантуючи, що впроваджені виправлення не порушують функціональність системи. Після застосування патчів проводиться ретельний аналіз результатів, щоб оцінити ефективність виправлення та виявити будь-які непередбачувані проблеми. Цей крок гарантує, що виправлення є ефективним і безпечним для розгортання у виробничому середовищі, підтримуючи цілісність і продуктивність системи [25].

П'ятий крок у структурі управління вразливостями передбачає створення надійного процесу управління змінами. Після успішного тестування та аналізу дуже важливо проінформувати відповідні команди про вимоги до виправлень. Це включає ретельне документування пов'язаних з цим ризиків та розробку плану резервного копіювання, щоб забезпечити можливість відкотити зміни в разі потреби. Після цього важливо отримати схвалення на запуск у виробництво від ключових зацікавлених сторін. Це гарантує, що всі потенційні впливи будуть враховані, і що перед початком роботи буде досягнутий організаційний консенсус, що забезпечить стабільність і цілісність системи.

Шостий крок у структурі управління вразливостями включає власне процес виправлення виявлених вразливостей. Він починається з планування розгортання виправлень з використанням відповідних інструментів для забезпечення структурованого та організованого підходу. Для мінімізації впливу на бізнес-операції часто рекомендується метод розгортання за

принципом водоспаду, що дозволяє здійснювати систематичне та поетапне розгортання. Дуже важливо заздалегідь повідомляти користувачів про будь-які потенційні перебої в роботі сервісів, щоб управляти очікуваннями і зменшити незручності. Цей етап гарантує, що вразливості будуть усунені швидко та ефективно, тим самим підвищуючи загальний рівень безпеки організації.

Сьомий крок Рамкової програми управління вразливостями зосереджений на звітності після впровадження. Цей критичний етап передбачає оцінку результатів усунення вразливостей, щоб зрозуміти їхню ефективність. Він включає рекомендації щодо компенсації контролів для будь-яких вразливостей, що залишилися, та надання детальних звітів про діяльність зі значущими метриками. Ці звіти повинні не лише давати уявлення про успішність процесу виправлення, але й забезпечувати підзвітність окремих осіб за їхню роль в ініціативі. Цей крок є важливим для отримання уроків з впровадження, покращення майбутніх дій та забезпечення постійного вдосконалення системи безпеки організації [26].

На завершення, розробка комплексної системи управління вразливостями має важливе значення для забезпечення надійної інформаційної безпеки. Це передбачає систематичну інвентаризацію активів, класифікацію вразливостей, створення пакетів виправлень, тестування виправлень, управління змінами, розгортання виправлень і ретельне звітування після впровадження. Кожен крок забезпечує ефективне виявлення, оцінку та усунення вразливостей, а також надає цінну інформацію для постійного вдосконалення. Такий структурований підхід не лише посилює безпеку організації, але й забезпечує стійкість до нових кіберзагроз.

2.2 Сучасні практики проектування і впровадження системи управління інформаційною безпекою в світі і Україні

До сучасних практик проектування і впровадження системи управління інформаційною безпекою в світі і Україні слід розглядати як глобальні практики і практики в Україні [27,28].

Глобальні практики

На міжнародному рівні поширені такі стандарти, як ISO/IEC 27001, що пропонують структуровані методології для управління ризиками інформаційної безпеки за допомогою систематичних політик і процедур. Прийняття цих стандартів зумовлене необхідністю забезпечення комплексних заходів безпеки, які охоплюють оцінку ризиків, постійний моніторинг та управління інцидентами. Ці рамки підкреслюють важливість збереження конфіденційності, цілісності та доступності інформації, а також відповідності регуляторним вимогам і зміцнення корпоративної репутації та продуктивності [27].

Практики в Україні

В Україні на впровадження СУІБ впливають як міжнародні стандарти, так і місцеві регуляторні вимоги. Український уряд запровадив спеціальні керівні принципи та закони для посилення заходів кібербезпеки в різних секторах. Організації в Україні все частіше впроваджують стандарт ISO/IEC 27001, щоб відповідати кращим світовим практикам і водночас вирішувати місцеві проблеми безпеки. Основна увага приділяється створенню стійкої системи безпеки, яка включає в себе комплексну оцінку ризиків, розробку надійних політик безпеки та постійний моніторинг для виявлення та реагування на інциденти безпеки в режимі реального часу. Крім того, програми навчання та підвищення обізнаності співробітників мають вирішальне значення для формування культури безпеки та забезпечення дотримання встановлених протоколів безпеки [28].

Інтеграція технологічних досягнень

Як у світі, так і в Україні, інтеграція передових інструментів моніторингу, таких як системи управління інформацією та подіями безпеки (SIEM) і системи виявлення вторгнень (IDS), має важливе значення для виявлення загроз у режимі реального часу та реагування на інциденти. Ці інструменти забезпечують безперервний моніторинг мережевої активності та поведінки систем, що дозволяє організаціям швидко виявляти та пом'якшувати потенційні загрози. Впровадження таких технологій доповнюється розробкою детальних

планів реагування на інциденти, які регулярно тестуються за допомогою симуляцій для забезпечення їхньої ефективності в управлінні та пом'якшенні наслідків порушень безпеки [29].

Загалом, успішна розробка та впровадження СУІБ вимагає комплексного підходу, який поєднує в собі дотримання міжнародних стандартів, узгодження з місцевими нормативно-правовими актами та інтеграцію передових технологій. Надаючи пріоритет захисту даних і розвиваючи культуру безпеки за допомогою регулярного навчання та інформаційних програм, організації можуть підвищити свою стійкість до нових кіберзагроз і забезпечити цілісність і конфіденційність своїх інформаційних активів.

Висновки до розділу 2

Встановлено, що побудова системи управління інформаційною безпекою вимагає комплексного підходу, що включає методи та засоби для виявлення, оцінки та управління ризиками інформаційної безпеки. Основні методичні підходи, такі як ризик-орієнтований, нормативно-правовий, технічний, організаційний та проактивний, забезпечують ефективність СУІБ шляхом своєчасного реагування на інциденти та мінімізації ризиків.

Дослідження показало, що ефективне управління ризиками є важливою складовою для забезпечення стабільного та безпечного функціонування організації. Процес управління ризиками включає кілька етапів: визначення контексту, ідентифікація, оцінка ризиків, розробка стратегій управління, впровадження заходів та постійний моніторинг. Інтеграція цих етапів дозволяє знижувати невизначеність та забезпечувати стійкість до зовнішніх і внутрішніх загроз.

Аналіз практик проектування і впровадження СУІБ на міжнародному рівні та в Україні показав, що дотримання стандартів, таких як ISO/IEC 27001, є критично важливим. Це дозволяє організаціям забезпечувати конфіденційність, цілісність та доступність інформації, а також відповідати регуляторним

вимогам. Інтеграція передових технологій моніторингу та систем управління інформаційною безпекою, таких як SIEM та IDS, сприяє своєчасному виявленню та реагуванню на інциденти безпеки.

Таким чином, успішна розробка та впровадження СУІБ вимагає комплексного підходу, який поєднує дотримання міжнародних стандартів, узгодження з місцевими нормативно-правовими актами та інтеграцію передових технологій. Надаючи пріоритет захисту даних і розвиваючи культуру безпеки через регулярне навчання, організації можуть підвищити свою стійкість до нових кіберзагроз та забезпечити цілісність і конфіденційність своїх інформаційних активів.

Розділ 3 РЕКОМЕНДАЦІЇ ПО ВДОСКОНАЛЕННЮ ПІДХОДІВ ЩОДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (для обраного прикладу)

3.1 Вибір підходів і практик щодо побудови системи управління інформаційною безпекою

Впровадження ефективної системи управління інформаційною безпекою вимагає прийняття найкращих практик, спрямованих на захист цінних даних та активів. Ці практики (рис. 3.1) допомагають організаціям впроваджувати надійні заходи безпеки та підтримувати проактивний захист від потенційних загроз.

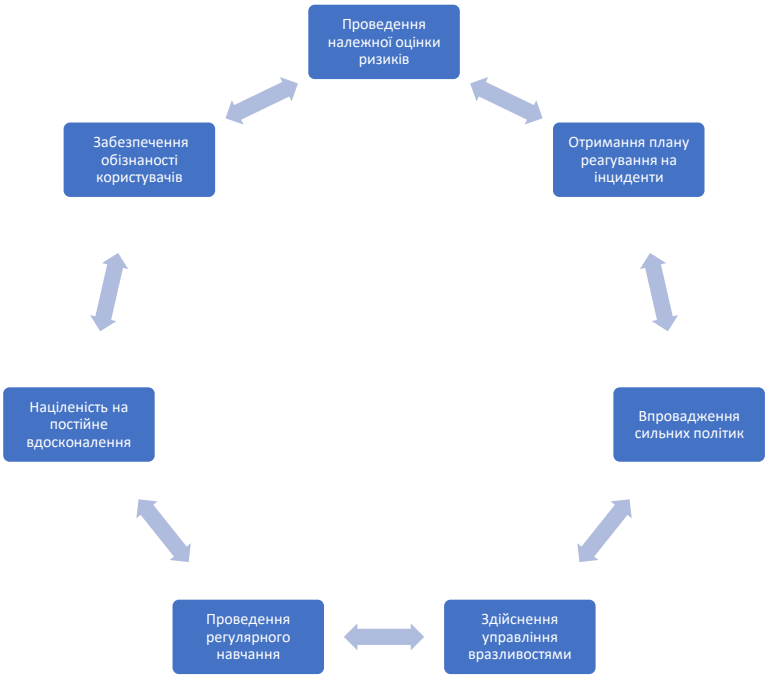

Рис. 3.1. Найкращі практики побудови СУІБ [30]

Критично важливим компонентом є проведення комплексної оцінки ризиків. Це передбачає визначення потенційних ризиків для інформації та систем, враховуючи мотивацію та методи потенційних зловмисників. Розуміючи ці ризики, організації можуть зосередитися на захисті своїх найбільш важливих сфер.

Ще однією ключовою практикою є розробка чітких політик. Чіткі, зрозумілі правила поводження з інформацією створюють основу для безпечних практик в організації. Ці правила мають бути ефективно донесені до всіх членів організації та дотримуватися всіма співробітниками.

Регулярне навчання має важливе значення для того, щоб працівники були здатні розпізнавати загрози безпеці та реагувати на них. Навчальні програми повинні охоплювати такі теми, як виявлення фішингових електронних листів, створення надійних паролів і практика безпечного користування Інтернетом. Добре поінформовані працівники формують першу лінію захисту від кіберзагроз [31].

Управління контролем доступу є життєво важливим для обмеження доступу до конфіденційних даних. Доступ повинен надаватися на основі ролі та обов'язків особи, гарантуючи, що лише уповноважений персонал може отримати доступ до критично важливої інформації.

План реагування на інциденти повинен бути розроблений для підготовки до потенційних інцидентів безпеки. Цей план визначає кроки, які необхідно вжити у випадку порушення, щоб мінімізувати збитки та забезпечити швидке відновлення. Регулярне тестування та оновлення цього плану має вирішальне значення для його ефективності.

Важливим є постійний моніторинг систем на предмет незвичної активності. Використання передових інструментів, які можуть попередити організацію про підозрілу поведінку, допомагає в ранньому виявленні та пом'якшенні загроз. Регулярне управління вразливостями, що передбачає сканування систем на наявність слабких місць і оперативне усунення будь-яких виявлених вразливостей, ще більше зміцнює безпеку [32].

Шифрування є фундаментальною практикою захисту даних. Шифрування даних гарантує, що навіть якщо неавторизовані особи отримають доступ до інформації, вони не зможуть зрозуміти її без правильного ключа розшифрування.

Регулярне резервне копіювання необхідне для захисту від втрати даних. Резервне копіювання даних гарантує, що їх можна буде відновити в разі кібератаки або збою системи, підтримуючи безперервність бізнесу.

Регулярне проведення аудиту безпеки допомагає перевірити ефективність заходів безпеки. Ці аудити схожі на перевірку замків і сигналізації в будинку, гарантуючи, що всі механізми безпеки функціонують за призначенням.

Постійне вдосконалення має бути постійною метою. Вивчення досвіду минулих інцидентів та адаптація заходів безпеки до нових загроз має вирішальне значення для підтримання ефективної СУІБ [33].

Залучення вищого керівництва є життєво важливим для успіху зусиль з безпеки. Вище керівництво повинно підтримувати ініціативи з безпеки та брати на себе зобов'язання щодо їх реалізації, демонструючи, що безпека є пріоритетом для всієї організації.

Забезпечення безпеки постачальників також є важливим, особливо коли сторонні постачальники працюють з даними або системами організації. Організації повинні переконатися, що їхні постачальники дотримуються суворих правил безпеки для захисту спільної інформації.

Не слід забувати про фізичну безпеку. Захист фізичних приміщень, включаючи офіси, сервери та пристрої, від несанкціонованого доступу так само важливий, як і заходи цифрової безпеки.

Підвищення обізнаності користувачів має вирішальне значення. Всі співробітники повинні бути пильними, повідомляти про підозрілі дії та дотримуватися правил безпеки для підтримки безпечного середовища.

Ведення ретельного документування політик, процедур і дій з безпеки допомагає відстежувати прогрес і демонструвати відповідність вимогам. Ця документація слугує фіксацією прихильності організації до безпеки та забезпечує основу для постійного вдосконалення.

Інтегруючи ці кращі практики, організації можуть розробити та впровадити ефективну СУІБ, яка не лише захистить їхні інформаційні активи,

але й покращить загальний стан безпеки, забезпечуючи стійкість до нових кіберзагроз [34].

Розгляемо рішення **компанії The Corporate Information Security Management (ISM)**, які є прикладом найкращих практик створення ефективної системи управління інформаційною безпекою шляхом інтеграції передових технологій і методологій для задоволення складних потреб сучасних організацій у сфері безпеки. Це рішення покликане забезпечити комплексне управління безпекою, використовуючи аналітику даних, автоматизовані процеси та моніторинг у режимі реального часу для забезпечення надійного захисту інформаційних активів. Основні його переваги зображені на рис. 3.2.

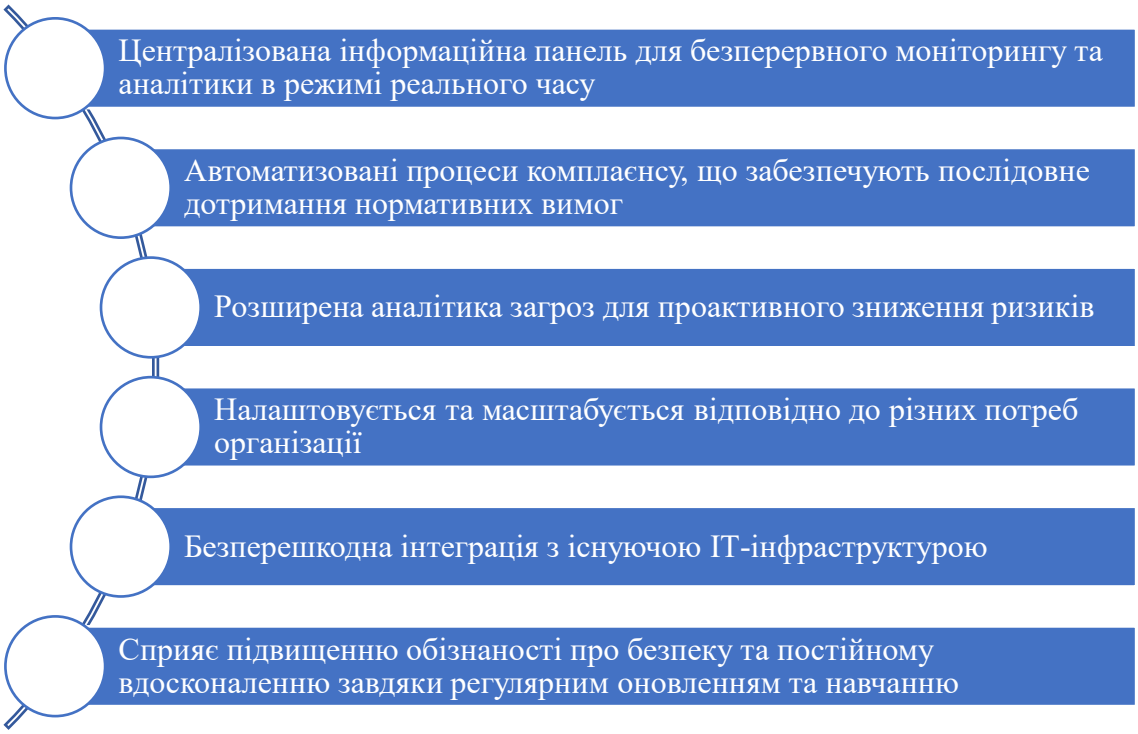

Рис. 3.2. Переваги Corporate ISM

Corporate ISM забезпечує уніфікований підхід до управління інформаційною безпекою, дозволяючи організаціям безперешкодно узгоджувати свої стратегії безпеки з бізнес-цілями. Завдяки централізованій інформаційній панелі вона дозволяє здійснювати безперервний моніторинг показників безпеки та ефективності, забезпечуючи тим самим не лише впровадження, але й суворе дотримання та оцінку практик безпеки. Така

інтеграція покращує видимість ландшафту безпеки, дозволяючи своєчасно виявляти потенційні загрози та реагувати на них [35].

Однією з відмінних рис Corporate ISM є зосередженість на дотриманні нормативних вимог та управлінні ризиками. Рішення допомагає організаціям дотримуватися нормативних вимог і галузевих стандартів, тим самим мінімізуючи юридичні та фінансові ризики, пов'язані з невідповідністю. Воно дозволяє автоматизувати комплаєнс-процеси, зменшуючи навантаження на служби безпеки та забезпечуючи послідовне і точне виконання завдань з комплаєнсу.

Corporate ISM також підкреслює важливість проактивного підходу до забезпечення безпеки. Завдяки розширеним можливостям розвідки загроз, вона надає організаціям практичну інформацію про загрози та вразливості, що з'являються. Такий проактивний підхід дозволяє передбачати і зменшувати ризики до того, як вони матеріалізуються в серйозні інциденти безпеки. Крім того, рішення підтримує комплексне управління інцидентами, сприяючи ефективному реагуванню на інциденти та процесам відновлення.

Ще одним ключовим аспектом Corporate ISM є його адаптивність та масштабованість. Рішення розроблене таким чином, щоб розвиватися разом з організацією, пристосовуючись до зростання та змін у ландшафті безпеки. Воно пропонує настроювані модулі, які можна адаптувати до конкретних потреб різних галузей та організаційних структур, гарантуючи, що система безпеки залишається актуальною та ефективною.

Corporate ISM також легко інтегрується з існуючою IT-інфраструктурою (рис. 3.3), сприяючи інтероперабельності та знижуючи складність впровадження. Така безперешкодна інтеграція гарантує, що організації можуть ефективно використовувати існуючі інвестиції в технології, одночасно підвищуючи загальний рівень безпеки.

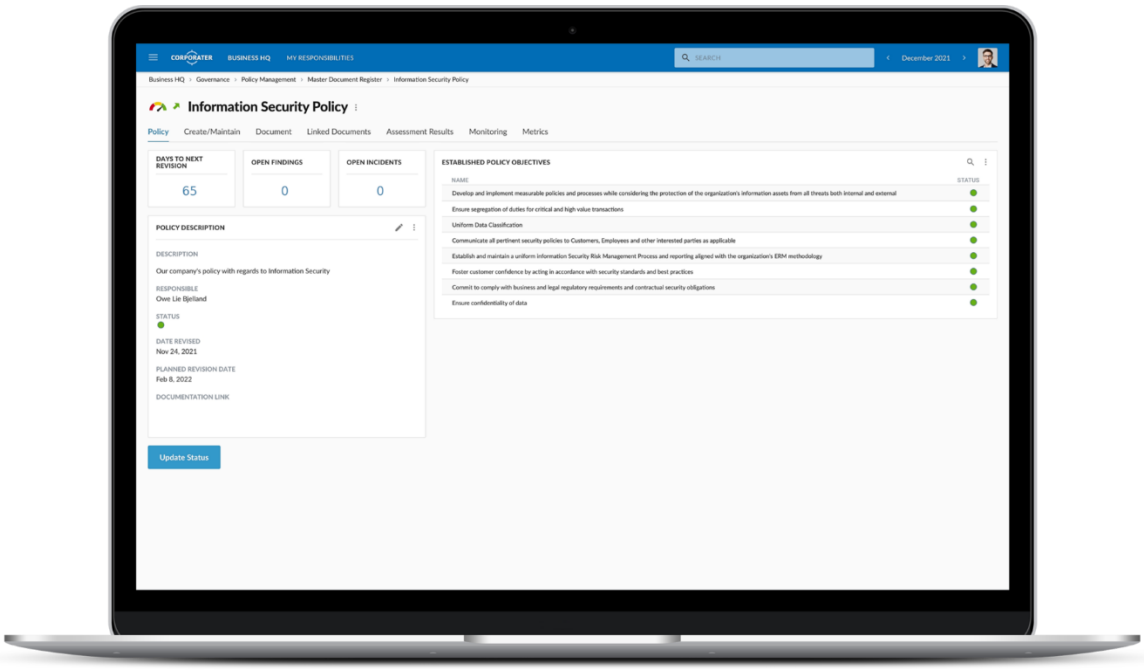

Рис. 3.3. Інтерфейс Corporate ISM

Рішення також сприяє підвищенню рівня обізнаності про безпеку та постійному вдосконаленню. Надаючи регулярні оновлення та навчальні матеріали, воно гарантує, що співробітники залишаються в курсі останніх практик безпеки та загроз. Такий акцент на освіті та обізнаності сприяє формуванню культури безпеки, що має важливе значення для підтримання надійного середовища безпеки.

Таким чином, рішення Corporate ISM являє собою комплексний і передовий підхід до побудови ефективної системи управління інформаційною безпекою. Інтегруючи моніторинг у режимі реального часу, автоматизацію дотримання нормативних вимог, проактивну розвідку загроз та адаптивність, воно вирішує багатогранні проблеми інформаційної безпеки в сучасному цифровому ландшафті.

3.2 Рекомендації щодо впровадження системи управління інформаційною безпекою

Впровадження системи управління інформаційною безпекою, узгодженої з бізнес-цілями організації, вимагає комплексного та структурованого підходу.

Першим кроком є забезпечення прихильності з боку вищого керівництва, підкреслюючи критичну роль інформаційної безпеки в досягненні бізнес-цілей. Це передбачає виділення необхідних ресурсів і формування культури обізнаності про безпеку в організації [36].

Далі необхідно створити структуру управління, яка визначатиме ролі, обов'язки та підпорядкованість у сфері інформаційної безпеки. Це може включати призначення керівника служби інформаційної безпеки (CISO) або створення керівного комітету з інформаційної безпеки для нагляду за впровадженням СУІБ.

Визначення сфери застосування та меж СУІБ має важливе значення. Це передбачає визначення інформаційних активів, процесів і систем, які потребують захисту, з урахуванням бізнес-цілей і пріоритетів організації. Розробка політики інформаційної безпеки, яка окреслює підхід організації до інформаційної безпеки, має вирішальне значення. Ця політика високого рівня має бути затверджена вищим керівництвом і доведена до відома всіх співробітників, щоб забезпечити її розуміння і дотримання.

Необхідно впровадити програму моніторингу та вимірювання для визначення ключових показників ефективності (KPI), які вимірюють ефективність СУІБ та її відповідність бізнес-цілям. Регулярне звітування про ці показники вищому керівництву та відповідним зацікавленим сторонам забезпечує постійний нагляд та підзвітність [37].

Ще одним важливим кроком є розробка методології оцінки ризиків, яка відповідає апетиту організації до ризику та її бізнес-цілям. Проведення оцінки ризиків для виявлення, аналізу та оцінки потенційних ризиків для інформаційних активів є життєво важливим. На основі цих оцінок слід розробити план управління ризиками, вибравши відповідні заходи для їх зниження, такі як політики, процедури і технічні засоби контролю.

Реалізація плану управління ризиками передбачає розгортання обраних заходів і забезпечення навчання працівників відповідним процедурам і

політикам. Слід визначити чіткі ролі та обов'язки щодо інформаційної безпеки та узгодити їх зі структурою організації та бізнес-цілями [38].

Програми навчання та підвищення обізнаності персоналу, адаптовані до бізнес-цілей організації, мають важливе значення для забезпечення розуміння працівниками своєї ролі в захисті інформаційних активів. Для реагування на інциденти безпеки слід запровадити процес управління інцидентами, надаючи пріоритет захисту бізнес-цілей.

Періодичні внутрішні аудити та управлінські огляди необхідні для оцінки продуктивності та ефективності СУІБ, зосереджуючись на її здатності підтримувати бізнес-цілі. Виявлення можливостей для вдосконалення та впровадження коригувальних дій гарантує, що СУІБ розвивається відповідно до мінливих потреб [39].

Постійне вдосконалення СУІБ досягається шляхом постійного моніторингу та аналізу, забезпечення відповідності бізнес-цілям організації та адаптації до змін у ландшафті загроз та бізнес-середовищі.

Нарешті, організації можуть вирішити пройти сертифікацію СУІБ в акредитованому органі сертифікації, наприклад, ISO/IEC 27001, щоб забезпечити зовнішнє підтвердження своєї прихильності до інформаційної безпеки [40].

Платформа ISMS.online є найкращою практикою для впровадження системи управління інформаційною безпекою, надаючи інтегроване, зручне для користувача рішення, яке спрощує складнощі, пов'язані з досягненням і підтримкою відповідності стандартам, таким як ISO/IEC 27001. Ця платформа пропонує комплексний набір інструментів, призначених для оптимізації всього життєвого циклу СУІБ, від початкового планування та оцінки ризиків до постійного моніторингу та вдосконалення. Автоматизуючи багато аспектів управління СУІБ, ISMS.online зменшує адміністративне навантаження на команди безпеки, дозволяючи їм більше зосередитися на стратегічній діяльності [41].

Однією з ключових переваг ISMS.online є її акцент на простоті використання та доступності. Платформа розроблена з інтуїтивно зрозумілим інтерфейсом, який полегшує навігацію та використання навіть для користувачів з обмеженими технічними знаннями. Така доступність гарантує, що організації можуть впроваджувати та управляти своїми СУІБ без необхідності проходження тривалого навчання або спеціальних знань, що сприяє більш широкому впровадженню та залученню в організації.

Платформа також інтегрує надійні функції співпраці, що дозволяє різним командам в організації безперешкодно працювати разом над ініціативами у сфері безпеки. Такий спільний підхід гарантує, що всі зацікавлені сторони залучені до процесу впровадження СУІБ, сприяючи формуванню всеосяжної та інклюзивної культури безпеки. Можливість призначати завдання, відстежувати прогрес і управляти документацією в рамках єдиної платформи підвищує ефективність і забезпечує підзвітність. Основні переваги рішення зображені на рис. 3.4.

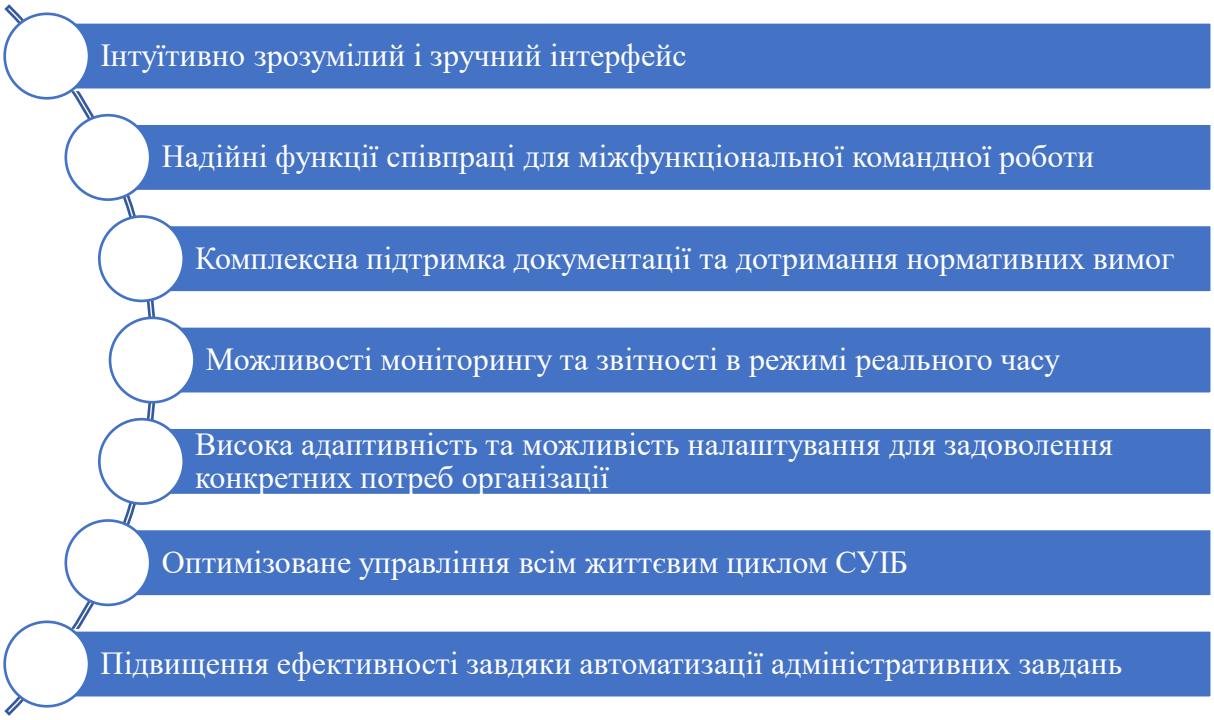

Рис. 3.4. Переваги ISMS.online

ISMS.online також надає широку підтримку в управлінні документацією та дотриманням нормативних вимог. Платформа включає шаблони і керівництва, які відповідають кращим практикам і міжнародним стандартам, що спрощує процес розробки і ведення необхідної документації для забезпечення відповідності вимогам СУІБ. Ця функція особливо корисна для організацій, які прагнуть пройти сертифікацію за такими стандартами, як ISO/IEC 27001, оскільки вона гарантує, що всі вимоги до документації будуть виконані ефективно і результативно.

Крім того, платформа підтримує моніторинг і звітність в режимі реального часу, надаючи організаціям актуальну інформацію про стан їхньої безпеки. Здатність генерувати комплексні звіти за запитом дозволяє організаціям демонструвати відповідність вимогам аудиторам і зацікавленим сторонам, посилюючи їхню прихильність до інформаційної безпеки. Така видимість ефективності системи безпеки в режимі реального часу також дозволяє організаціям виявляти і вирішувати проблеми на випередження, підвищуючи їх загальну стійкість до загроз.

ISMS.online легко адаптується, що дозволяє організаціям налаштовувати платформу відповідно до своїх конкретних потреб і вимог. Ця гнучкість гарантує, що платформа може підтримувати широкий спектр галузей і розмірів організацій, від малого бізнесу до великих підприємств. Надаючи масштабоване рішення, ISMS.online гарантує, що організації можуть рости і розвивати свої СУІБ відповідно до своїх мінливих потреб у сфері безпеки.

Таким чином, ISMS.online є прикладом найкращих практик впровадження системи управління інформаційною безпекою, пропонуючи комплексну, зручну та адаптивну платформу. Зосередженість на автоматизації, співпраці та підтримці дотримання нормативних вимог робить її безцінним інструментом для організацій, які прагнуть посилити свою інформаційну безпеку та досягти відповідності нормативним вимогам.

Висновки до розділу 3

Розглянуто рішення компанії The Corporate Information Security Management (ISM), як приклад найкращої практики створення ефективної системи управління інформаційною безпекою шляхом інтеграції передових технологій і методологій для задоволення складних потреб сучасних організацій у сфері безпеки.

Проаналізовані рекомендації щодо вдосконалення підходів до побудови системи управління інформаційною безпекою. Визначено, що впровадження ефективної СУІБ вимагає прийняття найкращих практик, таких як проведення комплексної оцінки ризиків, розробка чітких політик, регулярне навчання персоналу, управління контролем доступу, розробка плану реагування на інциденти, постійний моніторинг систем, шифрування даних та регулярне резервне копіювання.

Показано, що успішна СУІБ повинна бути узгоджена з бізнес-цілями організації та включати підтримку з боку вищого керівництва, створення структури управління, визначення сфери застосування, розробку політик, впровадження програм моніторингу та оцінки ефективності, а також регулярні аудити та вдосконалення.

Підтверджена важливість дотримання вимог міжнародних стандартів - таких як ISO/IEC 27001 і практик впровадження СУІБ у світі та в Україні, в тому числі - інтеграції передових технологій моніторингу, які забезпечують своєчасне виявлення інцидентів безпеки та реагування на них, що є критично важливим для захисту інформаційних активів організацій.

Таким чином, успішне впровадження та вдосконалення СУІБ потребує комплексного підходу, який поєднує прийняття найкращих практик, дотримання стандартів, інтеграцію технологій та постійне їх вдосконалення. Це забезпечує організаціям можливість ефективно протидіяти кіберзагрозам та підтримувати безпеку своїх інформаційних активів у динамічному цифровому середовищі.

ВИСНОВКИ

В роботі проаналізовано особливості управління інформаційною безпекою підприємства, досліджено основні характеристики практик побудови системи управління інформаційною безпекою; визначено інструменти та методи впровадження системи управління інформаційною безпекою, розроблено практичні рекомендації.

Процес управління інформаційною безпекою є багатоетапним і включає визначення контексту, ідентифікацію та оцінку ризиків, розробку стратегій управління, впровадження заходів та постійний моніторинг.

Розглянуті методичні підходи щодо особливостей побудови окремих і важливих систем управління інформаційною безпекою, які входять в загальну СУІБ: системи управління ризиками, системи управління інцидентами і системи управління вразливостями інформаційної безпеки.

На прикладі рішень для задоволення складних сучасних потреб у сфері безпеки розглянута компанія The Corporate Information Security Management (ISM), яка є однією із найкращих практик створення ефективної СУІБ шляхом інтеграції передових технологій і методологій.

Розроблені рекомендації по вдосконаленню підходів щодо побудови системи управління інформаційною безпекою дозволило визначити, що впровадження ефективної СУІБ вимагає прийняття найкращих практик, таких як проведення комплексної оцінки ризиків, розробка чітких політик, регулярне навчання персоналу, управління контролем доступу, розробка плану реагування на інциденти, постійний моніторинг систем, шифрування даних та регулярне резервне копіювання.

Впровадження ефективної системи управління інформаційною безпекою є критично важливим для забезпечення стабільного та безпечного функціонування організацій. Для ефективного управління інформаційною безпекою необхідно використовувати широкий спектр методів та моделей, що дозволяють організаціям систематично і комплексно захищати свої

інформаційні активи. Серед них аналіз ризиків, впровадження заходів захисту, контроль та моніторинг, а також професійне навчання і підвищення практичної обізнаності працівників при виконанні своїх службових обов’язків.

Загалом, успішне впровадження найкращих практик у побудови та вдосконаленні СУІБ потребує комплексного підходу, який поєднує дотримання міжнародних стандартів і інтеграцію передових технологій. Це забезпечує організаціям можливість ефективно протидіяти кіберзагрозам та підтримувати безпеку своїх інформаційних активів у динамічному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ALEXANDRU A.-C. Information Security Aspects of Business Continuity Management. *International Journal of Information Security and Cybercrime*. 2016. Vol. 5, no. 2. P. 17–24. URL: https://doi.org/10.19107/ijisc.2016.02.02

2. Kukharska N., Polotai O. Information security aspects of business continuity management. *Collection "Information technology and security"*. 2019. Vol. 7, no. 2. P. 126–136. URL: https://doi.org/10.20535/2411-1031.2019.7.2.190555

3. Skrynnyk O. Some Aspects of Information Security in Digital Organizational Management System. *Marketing and Management of Innovations*. 2020. No. 4. P. 279–289. URL: https://doi.org/10.21272/mmi.2020.4-23

4. Panchenko V. State and enterprise information security management: legal and organizational aspects. *Aktual'ni problemi pravoznavstva*. 2020. Vol. 1, no. 1. P. 103–109. URL: https://doi.org/10.35774/app2020.01.103

5. Information Security Management / J. Martins et al. *International Journal of Cyber Warfare and Terrorism*. 2013. Vol. 3, no. 3. P. 32–48. URL: https://doi.org/10.4018/ijcwt.2013070103

6. Kuka E., Bahiti R. Information Security Management: Password Security Issues. *Academic Journal of Interdisciplinary Studies*. 2018. Vol. 7, no. 2. P. 43–47. URL: https://doi.org/10.2478/ajis-2018-0045

7. von Solms R. Information security management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*. 1998. Vol. 6, no. 5. P. 221–223. URL: https://doi.org/10.1108/eum0000000004542

8. Šalgovičová J., Prajová V. Information Security Management (ISM). *Research Papers Faculty of Materials Science and Technology Slovak University of Technology*. 2012. Vol. 20, Special-Number. P. 114–119. URL: https://doi.org/10.2478/v10186-012-0019-0

9. Miloslavskaya N., Tolstaya S. Information Security Management Maturity Models. *Procedia Computer Science*. 2022. Vol. 213. P. 49–57.

URL: https://doi.org/10.1016/j.procs.2022.11.037

10. Somepalli S. H., Tangella S. K. R., Yalamanchili S. Information Security Management. *HOLISTICA – Journal of Business and Public Administration*. 2020. Vol. 11, no. 2. P. 1–16. URL: https://doi.org/10.2478/hjbpa-2020-0015

11. Guarro S. B. Risk analysis and risk management models for information systems security applications. *Reliability Engineering & System Safety*. 1989. Vol. 25, no. 2. P. 109–130. URL: https://doi.org/10.1016/0951-8320(89)90027-6

12. Humphreys E. Information security management system standards. *Datenschutz und Datensicherheit - DuD*. 2011. Vol. 35, no. 1. P. 7–11. URL: https://doi.org/10.1007/s11623-011-0004-3

13. Dykyi O., Fliunt M. Information security standards: a comparative research. *Law and public administration*. 2019. Vol. 2, no. 1. P. 88–95. URL: https://doi.org/10.32840/pdu.2-1.14

14. Alghananeem K. M., Altaee M. A., Jida B. K. The Impact of the Goals of Information Security Standards to Ensure Information Security. *Journal of Management Research*. 2014. Vol. 6, no. 2. P. 74. URL: https://doi.org/10.5296/jmr.v6i2.5024

15. Bensoussan A., Mookerjee V., Yue W. T. Managing Information System Security Under Continuous and Abrupt Deterioration. *Production and Operations Management*. 2020. Vol. 29, no. 8. P. 1894–1917. URL: https://doi.org/10.1111/poms.13198

16. Ozhiganova M., Kalita A., Tishchenko Y. Building Adaptive Information Security Systems. *NBI Technologies*. 2020. No. 4. P. 12–21. URL: https://doi.org/10.15688/nbit.jvolsu.2019.4.2

17. Chowdhury S. R. Managing Information Technology (IT) Security and Risk. *The Management Accountant Journal*. 2021. Vol. 56, no. 9. P. 48. URL: https://doi.org/10.33516/maj.v56i9.48-51p

18. Davis A. Managing third parties – an information security perspective. *Network Security*. 2010. Vol. 2010, no. 5. P. 13–15. URL: https://doi.org/10.1016/s1353-4858(10)70057-x

19. Tóth T., Sebestyén Z. Integrated Risk Management Process for Building Projects. *Procedia Engineering*. 2014. Vol. 85. P. 510–519. URL: https://doi.org/10.1016/j.proeng.2014.10.578

20. Enhancement of a Company-Wide Information Security Management System Through Incident Learning / H. Horikawa et al. *SN Computer Science*. 2023. Vol. 4, no. 3. URL: https://doi.org/10.1007/s42979-023-01691-7

21. Palvia P. Security Risk Management: Building and Information Security Risk. *Journal of Information Privacy and Security*. 2011. Vol. 7, no. 4. P. 72–73. URL: https://doi.org/10.1080/15536548.2011.10855925

22. Soldatov E. Y., Selifanov V. V., Kuvshiov M. A. Development of the information security incident control system. *Digital technology security*. 2023. No. 3. P. 54–66. URL: https://doi.org/10.17212/2782-2230-2023-3-54-66

23. Mitropoulos S., Patsos D., Douligeris C. Incident response requirements for distributed security information management systems. *Information Management & Computer Security*. 2007. Vol. 15, no. 3. P. 226–240. URL: https://doi.org/10.1108/09685220710759568

24. Farn K.-J., Lin S.-K., Fung A. R.-W. A study on information security management system evaluation–assets, threat and vulnerability. *Computer Standards & Interfaces*. 2004. Vol. 26, no. 6. P. 501–513. URL: https://doi.org/10.1016/j.csi.2004.03.012

25. Al-Dhahri S., Al-Sarti M., Abdul A. Information Security Management System. *International Journal of Computer Applications*. 2017. Vol. 158, no. 7. P. 29–33. URL: https://doi.org/10.5120/ijca2017912851

26. Singh A. N., Gupta M. P. Information Security Management Practices: Case Studies from India. *Global Business Review*. 2017. Vol. 20, no. 1. P. 253–271. URL: https://doi.org/10.1177/0972150917721836

27. Rawat S. Study on Management System for Information Security. *Journal of Optical Communication Electronics*. 2022. Vol. 8, no. 2. P. 26–30. URL: https://doi.org/10.46610/jooce.2022.v08i02.005

28. Li Y., Yi X. J., Geng Y. D. Social-Security-System-Based Two-Way

Referral Management Information System. *Applied Mechanics and Materials*. 2011. Vol. 121-126. P. 2248–2252. URL: https://doi.org/10.4028/www.scientific.net/amm.121-126.2248

29. A.A A. Information Security Management System: Emerging Issues and Prospect. *IOSR Journal of Computer Engineering*. 2013. Vol. 12, no. 3. P. 96–102. URL: https://doi.org/10.9790/0661-12396102

30. Li H., Yang X., Feng S. Design and Implementation of International Civil Aviation Security Information Database Management System. *IOP Conference Series: Earth and Environmental Science*. 2019. Vol. 252. P. 052101. URL: https://doi.org/10.1088/1755-1315/252/5/052101

31. Xu Z., Qu H. P. Design and Implementation of Testing and Management System on Special Information Security Products. *Applied Mechanics and Materials*. 2013. Vol. 302. P. 711–716. URL: https://doi.org/10.4028/www.scientific.net/amm.302.711

32. Design and Implementation of Computer Information Security Management System in Colleges and Universities. *International Journal of New Developments in Education*. 2023. Vol. 5, no. 21. URL: https://doi.org/10.25236/ijnde.2023.052116

33. Cao W. L. The Design of Social Security Information Management System. *Applied Mechanics and Materials*. 2013. Vol. 347-350. P. 2734–2738. URL: https://doi.org/10.4028/www.scientific.net/amm.347-350.2734

34. Zhiyong Shan, Vinod Namboodiri. Design and Implementation of A Network Security Management System. *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*. 2020. Vol. 20. P. 95–108. URL: https://doi.org/10.24297/ijct.v20i.8841

35. Information Security Management Software. *Corporater*. URL: https://corporater.com/solution/information-security-management/

36. Ezingeard J.-N., Bowen-Schrire M. Triggers of Change in Information Security Management Practices. *Journal of General Management*. 2007. Vol. 32, no. 4. P. 53–72. URL: https://doi.org/10.1177/030630700703200404

37. Michael K. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. *Computers & Security*. 2012. Vol. 31, no. 2. P. 249–250. URL: https://doi.org/10.1016/j.cose.2011.12.011

38. Anton N., Nedelcu A. Security risk analysis and management. *MATEC Web of Conferences*. 2018. Vol. 178. P. 08015. URL: https://doi.org/10.1051/matecconf/201817808015

39. Cao X. L. Research on Method of Information System Information Security Risk Management. *Advanced Materials Research*. 2014. Vol. 926-930. P. 4105–4109. URL: https://doi.org/10.4028/www.scientific.net/amr.926-930.4105

40. Dreyfuss M., Giat Y. A Risk Management Model for an Academic Institution's Information System. *Information Resources Management Journal*. 2018. Vol. 31, no. 1. P. 83–96. URL: https://doi.org/10.4018/irmj.2018010104

41. Information Security Management System SaaS For ISO 27001. *Isms.online*. URL: https://www.isms.online/information-security-management-system-isms/

42. Information Security and Risk Management for Banking System / D. K. Subrahmanyam et al. *International Journal of Computer Trends and Technology*. 2014. Vol. 10, no. 3. P. 171–176. URL: https://doi.org/10.14445/22312803/ijctt-v10p129

43. Pałęga M., Knapiński M., Kulma W. Risk management in the information security system in the enterprise. *Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa*. 2014. Vol. 2. P. 223–238. URL: https://doi.org/10.16926/tiib.2014.02.19

44. Information Security Risk Assessment / I. Kuzminykh et al. *Encyclopedia*. 2021. Vol. 1, no. 3. P. 602–617. URL: https://doi.org/10.3390/encyclopedia1030050

45. Revenkov P., Krupenko D. Mobile banking: Information Security Risk Assessment. *Voprosy kiberbezopasnosti*. 2019. No. 2(30). P. 21–28. URL: https://doi.org/10.21681/2311-3456-2019-2-21-28

46. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного *ISO/IEC 27001:2013*. Information Technology. Security Techniques. Information Security Management Systems. Requirements).

47. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://www.dut.edu.ua/uploads/l_2230_88161692.pdf.

48. Шевчук І. В. Побудова системи управління інформаційною безпекою на підприємстві: матеріали Всеукр. наук.-практ. конф. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу . Київ : ДУІКТ, 28 лютого 2024. С.91-94 . URL: https://duikt.edu.ua/uploads/p_2661_62255520.pdf