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: “ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ (SIEM) У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ”

на здобуття освітнього ступеня магістра

зі спеціальності 125 Кібербезпека

освітньо-професійної програми Управління інформаційною безпекою

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

_____ Богдан Карачун
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Богдан КАРАЧУН

Керівник:
к.в.н., доц. Юрій ЯКИМЕНКО

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Карачуну Богдану Олександровичу
(*прізвище, ім'я, по батькові здобувача*)

1. Тема кваліфікаційної роботи: " СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ (SIEM) У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА "

керівник кваліфікаційної роботи Юрій ЯКИМЕНКО, к.в.н., доцент
(*ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання*)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *управління інформацією та подіями, інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література*

4. Перелік питань, які потрібно розробити:
   1. Проаналізувати вимоги нормативних документів щодо забезпечення інформаційної безпеки на підприємстві.
   2. Проаналізувати практики використання систем управління інформацією та подіями у забезпеченні інформаційної безпеки підприємства.
   3. Провести дослідження процесів управління інформацією і подіями (SIEM) та розробка рекомендацій щодо інформаційної безпеки підприємства.

5. Перелік ілюстративного матеріалу: презентація

6. Дата видачі завдання "26" вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи
студентом **Карачуном Богданом Олександровичем**
Дата видачі завдання: «26» вересня 2023 р.

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	26.09.2023	Виконано
2.	Збір та аналіз літератури.	3.10.2023	Виконано
3.	Розділ 1. Аналіз вимог нормативних документів щодо забезпечення інформаційної безпеки підприємства	17.10.2023	Виконано
4.	Розділ 2. Аналіз практики використання систем управління інформацією та подіями у забезпеченні інформаційної безпеки підприємства	31.10.2023	Виконано
5.	Розділ 3. Дослідження процесів управління інформацією і подіями (SIEM) та розробка рекомендацій щодо інформаційної безпеки підприємства	14.11.2023	Виконано
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2023	Виконано
7.	Оформлення роботи	8.12.2023р.	Виконано
8.	Оформлення презентації	15.12.2023р.	Виконано
9.	Отримання рецензії на роботу .	23.12.2023	Виконано
10.	Захист в ДЕК	___01.2024 р.	Виконано

Здобувач вищої освіти _____ Богдан КАРАЧУН
(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 магістра

Направляється здобувач Карачун Б.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: “ Системи управління інформацією та подіями (Siem) у забезпеченні інформаційної безпеки підприємства ”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **КАРАЧУН Богдан** у кваліфікаційній роботі дослідив систему управління інформацією та подіями на прикладі підприємства «FinTrust Bank» України; визначив потенційні загрози, інциденти і ризики безпеки та можливості сучасних SIEM у контексті забезпечення інформаційної безпеки; розробив методику використання програми Splunk для проведення дослідження ірекомендації щодо оптимізації управління інформаційною безпекою на підприємстві. **КАРАЧУН Богдан** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **КАРАЧУНА Богдана** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

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

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Карачуна Богдана Олександровича
на тему " СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ (SIEM) У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА "

Актуальність

Інформаційна безпека (ІБ) підприємств в сучасному глобалізованому світі є однією з ключових задач, що вимагає високого рівня уваги і компетентності. За умов постійного зростання кількості та складності кіберзагроз, системи управління інформацією та подіями (SIEM – Security Information and Event Management) стають не просто актуальними, але й невід'ємними елементами для забезпечення інтегрованої захищеності інформаційних активів.

Позитивні сторони

В ході виконання роботи було проведено всебічне дослідження систем управління інформацією та подіями на прикладі підприємства «FinTrust Bank». Робота спрямовувалася на оцінку ефективності системи управління інцидентами інформаційної безпеки, з використанням програми Splunk для збору та аналізу даних. У рамках першого розділу було проведено глибоке дослідження нормативно-правової бази України щодо забезпечення інформаційної безпеки підприємства. У другому розділі було детально розглянуто роль та значення SIEM-систем у сучасних умовах цифрової економіки. Виділено та проаналізовано ключові підсистеми управління інформаційною безпекою, включаючи управління ризиками, інцидентами та забезпечення готовності до безперервної діяльності. У рамках третього розділу, з використанням програми Splunk, було проведено детальний аналіз ефективності SIEM. Отримані дані демонструють значне покращення в таких ключових областях, як час виявлення інцидентів та швидкість реагування, а також зменшення помилкових спрацьовувань.

Недоліки

У роботі також доцільно було б визначити заходи застосування штучного інтелекту при плануванні, але вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Карачун Богдан Олександрович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 97 стор., 31 рис., 9 табл., 63 джерел.

Метою роботи є дослідження процесів управління інформацією і подіями та розробца рекомендацій щодо інформаційної безпеки підприємства.

Об'єктом дослідження є процес управління інформаційною безпекою підприємства через системи управління інформацією та подіями.

Предмет дослідження - комплекс методів, підходів та технологій, що використовуються для підвищення ефективності SIEM-систем в контексті забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення зазначеного завдання в роботі використані методи системного аналізу, теорії ІБ та аналізу даних.

Короткий зміст роботи. В ході виконання роботи було проведено всебічне дослідження систем управління інформацією та подіями на прикладі підприємства «FinTrust Bank». Робота спрямовувалася на оцінку ефективності системи управління інцидентами інформаційної безпеки, з використанням програми Splunk для збору та аналізу даних.

Галузь застосування. Результати цієї роботи можуть бути використані для управління інформаційною безпекою підприємств, що використовують інформаційні технології в своїй діяльності.

Ключові слова: ЗАХИСТ ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТ, КІБЕРБЕЗПЕКА, КІБЕРЗАГРОЗА, МОНІТОРИНГ ІНФОРМАЦІЙНИХ СИСТЕМ, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЄЮ, УПРАВЛІННЯ ПОДІЯМИ, SIEM.

ABSTRACT

The text part of the qualification work for the degree of

Master's degree: 97 pages, 31 figures, 9 tables, 63 sources.

The purpose of the work is to study the processes of information and event management and to develop recommendations for enterprise information security.

Object of research of managing the information security of an enterprise through information and event management systems.

Subject of research is a set of methods, approaches and technologies used to improve the efficiency of SIEM systems in the context of ensuring the information security of the enterprise.

Research methods To solve this problem, the methods of system analysis, IS theory and data analysis are used in the work.

Brief content of research In the course of the work, a comprehensive study of information and event management systems was conducted on the example of FinTrust Bank. The work was aimed at evaluating the effectiveness of the information security incident management system, using the Splunk program for data collection and analysis.

Field of research The results of this work can be used to manage the information security of enterprises that use information technology in their activities.

Keywords: DATA PROTECTION, INFORMATION SECURITY, INCIDENT, CYBERSECURITY, CYBER THREAT, INFORMATION SYSTEMS MONITORING, INFORMATION SECURITY RISKS, INFORMATION MANAGEMENT, EVENT MANAGEMENT, SIEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АІ - Аналіз інциденту

АІБ - Автоматизація інформаційної безпеки

ВІ - Виявлення інциденту

ДССЗЗІ -Державна служба спеціального зв'язку та захисту інформації України

ЗІС - Захист інформаційних систем

ІБ - Інформаційна безпека

ІІ - Інциденти інформаційної безпеки

МН - Моніторинг та нагляд

ПЗ - програмне забезпечення

РІ - Реагування на інцидент

СУІБ - Система управління інформаційною безпекою

ШД - Шифрування даних

SIEM - Система управління інформацією та подіями (Security Information and Event Management)

ВСТУП

Актуальність теми. Інформаційна безпека (ІБ) підприємств в сучасному глобалізованому світі є однією з ключових задач, що вимагає високого рівня уваги і компетентності. За умов постійного зростання кількості та складності кіберзагроз, системи управління інформацією та подіями (SIEM – Security Information and Event Management) стають не просто актуальними, але й невід'ємними елементами для забезпечення інтегрованої захищеності інформаційних активів.

Оскільки кіберзлочинність динамічно розвивається, стаючи все більш організованою і технічно оснащеною – це породжує ряд наукових та практичних проблем: від виявлення і аналізу нових векторів атак до оптимізації процесів реагування на інциденти інформаційної безпеки. Сучасні методики, засновані на машинному навчанні та штучному інтелекті, є перспективними, але не завжди ефективно інтегрованими в корпоративні екосистеми.

Слід зазначити, що в Україні проблема інформаційної безпеки набуває особливої актуальності в контексті війни, економічної нестабільності та політичних ризиків. Відсутність єдиної методології для інтеграції SIEM-систем у національних підприємствах є критичним недоліком, що обмежує можливості для ефективного протидії кіберзагрозам.

З огляду на зазначене, тема кваліфікаційної роботи є актуальною, а використання її результатів буде спрямовано на поглиблене розуміння процесів управління інформацією та подіями в контексті підприємства.

Мета і завдання дослідження. Мета роботи полягає в дослідженні процесів управління інформацією і подіями та розробці рекомендацій щодо інформаційної безпеки підприємства.

Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Аналіз нормативно-правової бази України та міжнародних стандартів, що регулюють питання інформаційної безпеки, з акцентом на роль систем управління інформацією та подіями (SIEM).

2. Дослідження сучасних підходів до управління інцидентами інформаційної безпеки, з особливим акцентом на використання програми Splunk для моніторингу та аналізу інцидентів безпеки.

3. Аналіз процесів управління інцидентами інформаційної безпеки в конкретному підприємстві «FinTrust Bank», використовуючи програму Splunk, та розробка рекомендацій щодо оптимізації управління інформаційною безпекою.

Об'єктом дослідження є процес управління інформаційною безпекою підприємства через системи управління інформацією та подіями.

Предметом дослідження є комплекс методів, підходів та технологій, що використовуються для підвищення ефективності SIEM-систем в контексті забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення зазначеного завдання в роботі використані методи системного аналізу, теорії ІБ та аналізу даних.

Наукова новизна. Розроблені рекомендації можуть бути використані для оптимізації систем управління інформацією та подіями (SIEM) в контексті забезпечення ІБ підприємств, забезпечуючи більш ефективне виявлення та реагування на інформаційні загрози.

Практичне значення одержаних результатів. Розроблені рекомендації допоможуть компаніям краще виявляти та реагувати на інформаційні загрози, оптимізуючи використання SIEM-систем. Це особливо корисно для організацій, які активно використовують інформаційні технології та стикаються із викликами інформаційного протиборства.

Галузь застосування. Результати кваліфікаційної роботи у вигляді тез були опубліковані на міжнародній науково-технічній конференції «Безпека інформаційних технологій: ITSec» а також на «Всеукраїнська конференція» кафедри управління інформаційною та кібернетичною безпекою ДУІКТ.

Розділ 1. АНАЛІЗ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В даному розділі буде проведений аналіз нормативно-правових вимог, що стосуються забезпечення інформаційної безпеки підприємств через використання систем управління інформацією та подіями. Основна мета полягає в детальному розкритті ключових аспектів, пов'язаних із забезпеченням інформаційної безпеки, роллю SIEM-систем в цьому процесі, а також аналізу основних вимог, які встановлені національними та міжнародними стандартами в даній сфері. Зокрема, буде зроблений акцент на вимогах, що висуваються до організаційно-технічного забезпечення інформаційної безпеки, методах оцінки ризиків, а також процедурах моніторингу та реагування на інциденти інформаційної безпеки.

1.1 Нормативно-правова база регулювання заходів забезпечення інформаційної безпеки підприємства

Забезпечення інформаційної безпеки підприємства є одним із пріоритетних напрямків сучасного суспільства, який потребує кваліфікованого підходу та строгого регулювання. В Україні діє ряд законодавчих актів, нормативних документів та методичних рекомендацій, які визначають основні принципи, методики та критерії для забезпечення інформаційної безпеки.

Закон України «Про інформаційну безпеку» [1] є фундаментальним нормативно-правовим актом, що визначає правові, організаційні та технічні аспекти забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах на території України (рис. 1.1).

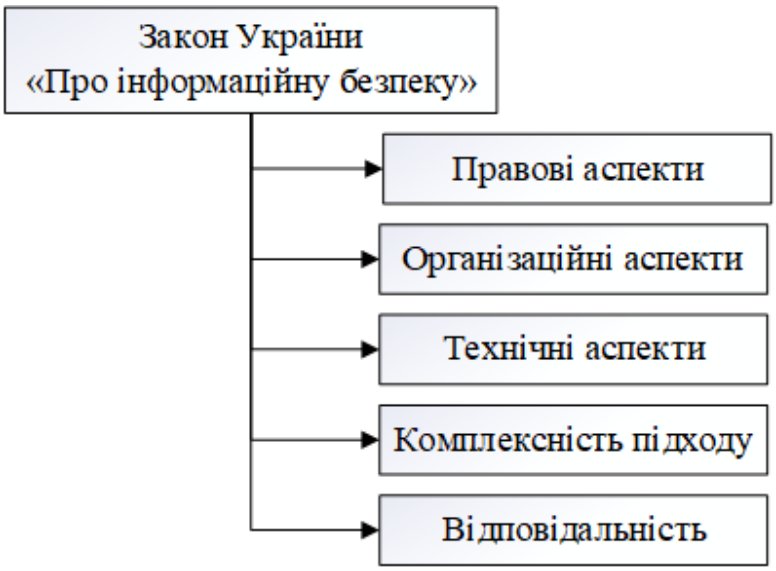

Рис. 1.1. Ключові положення Закону України «Про інформаційну безпеку»

Ключові положення цього закону з позицій їх впливу на системи управління інформацією та подіями:

– правові аспекти. Закон встановлює юридичну раму для діяльності суб'єктів, які займаються забезпеченням інформаційної безпеки. Він визначає права та обов'язки органів державної влади, юридичних та фізичних осіб. Для SIEM-систем це означає, що їх розробка, впровадження та експлуатація повинні бути узгоджені з цими правовими нормами;

– організаційні аспекти. Закон регулює взаємовідносини між різними організаційними структурами – від державних до приватних – в контексті інформаційної безпеки. Для SIEM-систем це важливо з точки зору координації дій з іншими системами і службами безпеки, а також з органами, що забезпечують контроль та нагляд;

– технічні аспекти. Закон визначає технічні критерії та стандарти, яким повинні відповідати системи забезпечення інформаційної безпеки. У контексті SIEM це може включати вимоги до зберігання, обробки та передачі інформації, а також до реагування на інциденти безпеки;

– комплексність підходу. Один із ключових моментів закону – це підкреслення необхідності комплексного підходу до інформаційної безпеки. Системи SIEM є важливою складовою цього комплексного підходу, оскільки

вони дозволяють забезпечити централізований моніторинг, аналіз і реагування на події, що стосуються безпеки інформації;

– відповідальність. Закон також встановлює форми відповідальності за порушення в сфері інформаційної безпеки. Це дуже важливо для SIEM-систем, оскільки вони часто є ключовим елементом в ідентифікації та розслідуванні таких порушень.

Отже, Закон України «Про інформаційну безпеку» створює солідну основу для розробки, впровадження та експлуатації систем управління інформацією та подіями (SIEM) у сфері загальної політики інформаційної безпеки в Україні.

Закон України «Про захист персональних даних» [2] є нормативно-правовим актом, який безпосередньо впливає на питання інформаційної безпеки, включаючи системи управління інформацією та подіями (рис. 1.2).

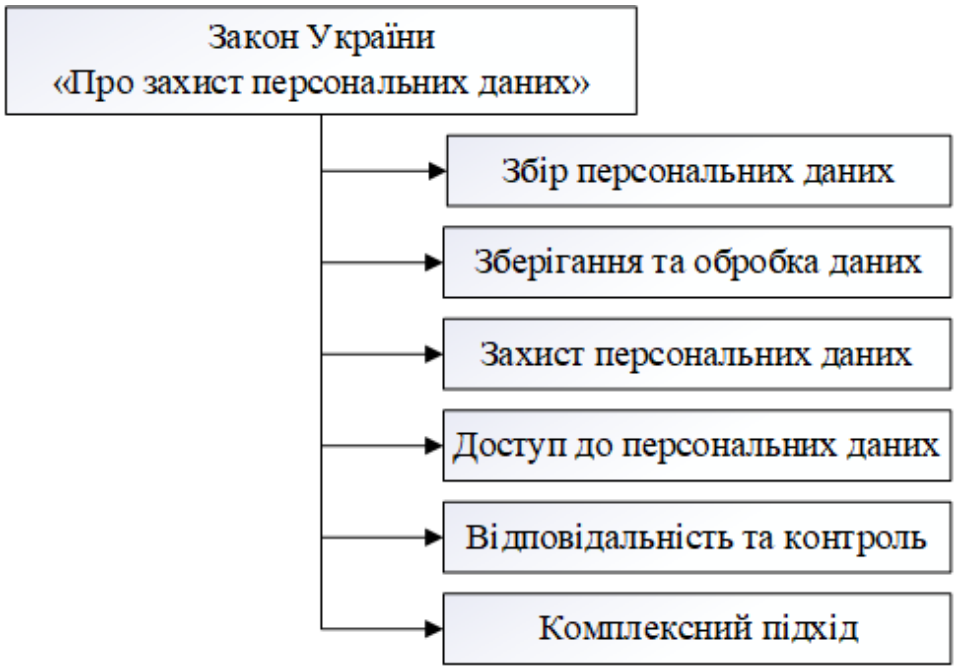

Рис. 1.2. Основні аспекти Закону України «Про захист персональних даних»

Детальний аналіз цього закону з точки зору SIEM-систем включає наступні елементи:

– збір персональних даних. Закон регламентує правила збору персональних даних, включаючи необхідність забезпечення згоди суб'єкта даних. В контексті SIEM, це означає, що всі процеси збору логів і моніторингу,

які можуть містити персональні дані, повинні бути виконані відповідно до цього закону;

– зберігання та обробка даних. Закон встановлює вимоги до зберігання і обробки персональних даних, що є особливо важливим для конфігурації та управління базами даних в SIEM-системах;

– захист персональних даних. Однією з ключових функцій SIEM є забезпечення захисту інформації. Закон вимагає від організацій вживати необхідних заходів для захисту персональних даних, що може включати в себе застосування шифрування, аудиту, моніторингу доступу тощо;

– доступ до персональних даних. Закон контролює, хто може мати доступ до персональних даних і під якими умовами. В контексті SIEM, це може включати в себе налаштування політик доступу та контролю авторизації;

– відповідальність та контроль. Закон встановлює відповідальність за порушення правил зберігання, обробки та захисту персональних даних. SIEM-системи можуть служити інструментом для дотримання цих вимог, а також для документування всіх дій, що відбулися з даними, для подальшого контролю або аудиту;

– комплексний підхід. Враховуючи, що персональні дані часто є цільовими об'єктами для кібератак, комплексний підхід до інформаційної безпеки, який пропонується законом, безпосередньо стосується SIEM-систем.

Таким чином, Закон України «Про захист персональних даних» має низку важливих імплікацій для розробки, впровадження та експлуатації SIEM-систем. Він створює регулятивну раму, яка обов'язкова для дотримання всіма учасниками, що займаються забезпеченням інформаційної безпеки в Україні.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) не лише формує загальнодержавні принципи інформаційної безпеки [3], але і виставляє конкретні технічні та організаційні вимоги до систем управління інформацією та подіями (рис. 1.3). Відповідність цим вимогам не просто є законодавчим обов'язком підприємства, але і ключем до підвищення їх репутації та довіри з боку клієнтів і партнерів. При цьому, розуміння специфіки

цих вимог дозволяє підприємству ефективно адаптувати та конфігурувати свої SIEM-системи для забезпечення найвищого рівня безпеки, що в свою чергу є стратегічним пріоритетом в умовах зростаючих кіберзагроз.

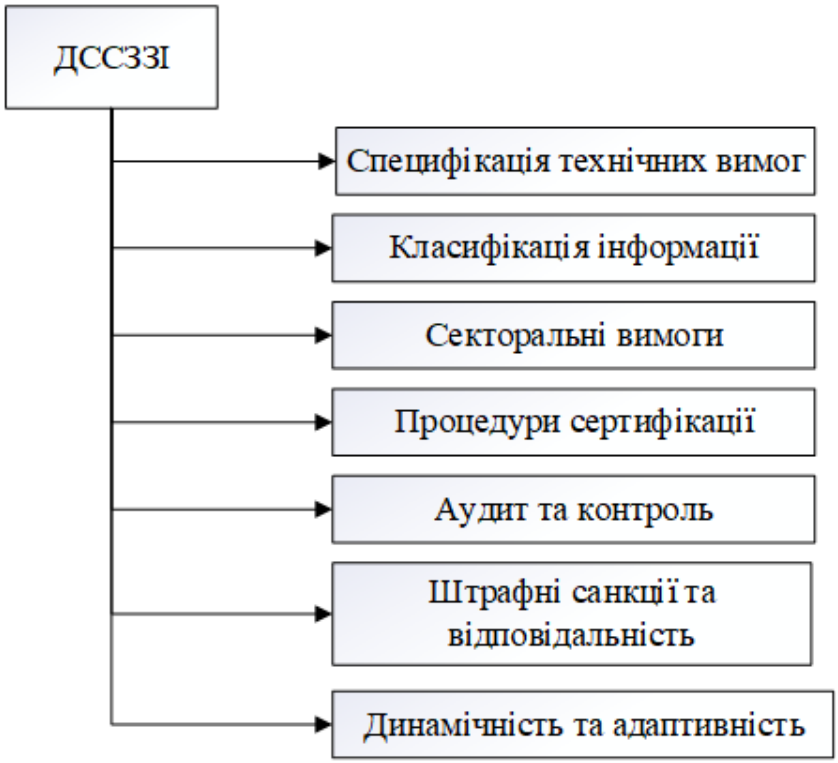

Рис. 1.3. Розповсюдження ДССЗЗІ на різні сектори діяльності

У поданому переліку пунктів розкриваються ключові аспекти нормативно-правового регулювання в сфері інформаційної безпеки, що від ДССЗЗІ розповсюджуються на різні сектори діяльності:

– специфікація технічних вимог. ДССЗЗІ часто випускає технічні документи, які визначають стандарти та вимоги до систем інформаційної безпеки [4]. Це може включати в себе вимоги до збору, обробки та зберігання даних, критерії для шифрування, а також процедури аудиту та моніторингу;

– класифікація інформації. Документи від ДССЗЗІ можуть містити класифікацію інформації та визначати рівні її захисту. Це є особливо важливим для SIEM-систем, які збирають і обробляють різні типи інформації;

– секторальні вимоги. Державна служба часто розробляє спеціалізовані вимоги для різних секторів: державного управління, комерційних структур, науково-дослідних інститутів, освітніх установ. Це дає можливість адаптувати SIEM-рішення під конкретні потреби;

– процедури сертифікації. Документи можуть включати в себе вимоги до сертифікації обладнання та програмного забезпечення, яке використовується в SIEM-системах. Сертифікація забезпечує додатковий рівень довіри до рішень з інформаційної безпеки;

– аудит та контроль. Важливою частиною документів є процедури аудиту та контролю. SIEM-системи можуть бути використані для забезпечення відповідності цим вимогам, зокрема через зберігання логів, аналіз подій та налаштування звітності;

– штрафні санкції та відповідальність. Рішення та накази часто включають штрафні санкції за недотримання вимог. Це акцентує увагу на важливості строгого дотримання положень з інформаційної безпеки;

– динамічність та адаптивність. ДССЗЗІ регулярно оновлює свої рекомендації та вимоги, що вимагає від SIEM-систем спроможності до швидкої адаптації.

Загалом, рішення та накази ДССЗЗІ створюють складний правовий ландшафт, який вимагає від організацій глибокого розуміння та строгого дотримання норм і правил. SIEM-системи, в свою чергу, можуть служити ефективним інструментом для забезпечення цієї відповідності.

Стандарт ISO/IEC 27001:2013 представляє собою міжнародний стандарт, що встановлює вимоги до систем управління інформаційною безпекою. Стандарт видається Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) [5].

Табл. 1.1 відображає основні аспекти кожного нормативного документа та їх відповідність ключовим елементам стандарту ISO/IEC 27001:2013, таким як управління ризиками, політика безпеки, захист інформації та контроль доступу.

Таблиця 1.1

Аналіз основних нормативних документів України по відношенню до стандарту ISO/IEC 27001:2013

Нормативний документ	Опис	Відношення до ISO/IEC 27001:2013

Продовження табл. 1.1

Закон України «Про інформацію» (2657-XII) [6]	Визначає основні принципи зберігання, поширення та захисту інформації.	Цей закон задає загальні рамки для управління інформацією, що відповідає принципам ISO/IEC 27001 щодо захисту інформації та її конфіденційності.
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (80/94-ВР)	Регулює захист інформації в ІТ системах, включаючи її обробку та передачу.	Підкреслює важливість управління ризиками та безпекою систем, що є ключовим елементом ISO/IEC 27001.
Закон України «Про державну таємницю» (3855-XII) [7]	Встановлює принципи класифікації та захисту державної таємниці.	Відповідає вимогам ISO/IEC 27001 щодо розробки та впровадження політики безпеки для конфіденційної інформації.
Закон України «Про захист персональних даних» (2297-VI) [8]	Визначає принципи обробки та захисту персональних даних.	Сприяє реалізації стандарту ISO/IEC 27001 через вимоги до захисту персональних даних та приватності.
Постанова КМУ «Про затвердження Правил забезпечення захисту інформації...» (№373) [9]	Встановлює правила захисту інформації в системах та вимоги до їх безпеки.	Узгоджується з ISO/IEC 27001 у частині розробки та реалізації мір безпеки інформаційних систем.
Постанова КМУ «Про затвердження Типової інструкції...» (№ 736) [10]	Регулює порядок зберігання та обігу службової інформації.	Відповідає вимогам ISO/IEC 27001 щодо управління активами та контролю доступу.

Аналізуючи нормативно-правову базу України щодо інформаційної безпеки, можна побачити, що вона в значній мірі відповідає та доповнює ключові аспекти міжнародного стандарту ISO/IEC 27001:2013. Закони та постанови, які були проаналізовані, встановлюють чіткі рамки для захисту інформації,

персональних даних, а також забезпечення конфіденційності та безпеки інформаційних систем. Ці документи не тільки сприяють впровадженню політик та процедур, передбачених ISO/IEC 27001, але й забезпечують додатковий контекст та напрямки для адаптації цих стандартів до специфіки українського законодавства та вітчизняних умов. Вони формують базу для комплексного підходу до управління інформаційною безпекою на підприємстві, що є важливим для впровадження ефективних систем управління інформаційною безпекою відповідно до міжнародних стандартів.

Розглядаючи нормативно-правову базу України у контексті стандарту ISO/IEC 27002:2013 для забезпечення інформаційної безпеки підприємства, створено табл. 1.2, де розкритий аналіз ключових нормативних документів.

Таблиця 1.2

Аналіз основних нормативних документів України по відношенню до стандарту ISO/IEC 27002:2013

Нормативний документ	Опис	Відношення до ISO/IEC 27002:2013
Закон України «Про інформацію» (2657-XII)	Встановлює основні правила щодо збору, зберігання, та розповсюдження інформації.	Відповідає рекомендаціям ISO/IEC 27002 стосовно керування інформаційними активами та забезпечення їх конфіденційності.
Закон України «Про захист інформації...» (80/94-ВР)	Регулює захист даних в інформаційно-телекомунікаційних системах.	Сприяє запровадженню контролю доступу та захисту інформації, як рекомендовано в ISO/IEC 27002.
Закон України «Про державну таємницю» (3855-XII)	Визначає правила класифікації та захисту державної таємниці.	Відображає принципи ISO/IEC 27002 щодо управління конфіденційністю та інтегритетом інформації.

Продовження табл. 1.2

Нормативний документ	Опис	Відношення до ISO/IEC 27001:2013
Закон України «Про захист персональних даних» (2297-VI)	Встановлює рамки для обробки та захисту персональних даних.	Відповідає рекомендаціям ISO/IEC 27002 щодо захисту персональних даних та приватності.
Постанова КМУ «Про затвердження Правил...» (№373)	Визначає правила захисту інформації в різних системах.	Підтримує рекомендації ISO/IEC 27002 щодо технічних та організаційних заходів безпеки.
Постанова КМУ «Про затвердження Типової інструкції...» (№ 736)	Регламентує обіг службової інформації.	Співвідноситься з принципами ISO/IEC 27002 стосовно контролю доступу та захисту інформації.

Проведений аналіз вказує на те, що ключові закони та постанови уряду України тісно корелюють з рекомендаціями стандарту ISO/IEC 27002:2013. Українське законодавство забезпечує міцну правову основу для впровадження ефективних заходів інформаційної безпеки на підприємстві, відповідаючи міжнародним стандартам. Це включає захист інформаційних активів, управління конфіденційністю та інтегритетом інформації, а також розробку та впровадження політик і процедур інформаційної безпеки. Українські нормативні акти підкреслюють важливість технічного та організаційного захисту інформації, що є ключовими аспектами ISO/IEC 27002:2013, та сприяють створенню безпечного інформаційного середовища на підприємстві.

1.2 Вимоги стандартів щодо впровадження і експлуатації систем управління інформаційною безпекою в Україні

Стандартизація в сфері інформаційної безпеки відіграє вирішальну роль у створенні єдиного та сумісного підходу до захисту інформації на різних рівнях – від державних органів до приватних підприємств. В Україні це досягається

шляхом застосування як національних, так і міжнародних стандартів, що є особливо важливим для бізнесу з метою забезпечення його безперервної готовності до виконання задач та адекватного реагування на інциденти інформаційної безпеки.

Значимість цих стандартів полягає в наданні конкретних вказівок та вимог до впровадження та експлуатації систем управління інформаційною безпекою (ISMS), які дозволяють підприємству ефективно управляти ризиками, пов’язаними з інформаційною безпекою. Це включає в себе ідентифікацію загроз, оцінку вразливостей та впровадження відповідних контрольних заходів для запобігання або мінімізації потенційних інцидентів.

Одним із ключових стандартів у цій області є ISO/IEC 27001:2013, який встановлює вимоги до системи управління інформаційною безпекою та забезпечує рамки для підтримки конфіденційності, цілісності та доступності інформації. Впровадження цього стандарту на підприємстві сприяє створенню суворої структури управління, яка включає в себе політику безпеки, планування, реалізацію, моніторинг, перегляд та покращення безпекових процесів.

Іншим важливим документом є ISO/IEC 27002:2013, який визначає керівні принципи та найкращі практики для впровадження заходів інформаційної безпеки. Цей стандарт допомагає підприємству розробляти та впроваджувати ефективні механізми управління ризиками та безпекою інформації, включаючи процедури реагування на інциденти та відновлення після них.

Перелічені стандарти стають невід'ємною частиною стратегії інформаційної безпеки підприємства, що дозволяє не лише забезпечувати захист інформації та інформаційних активів, а й підтримувати стабільну та безперервну роботу бізнесу в умовах постійно зростаючих кіберзагроз.

ДСТУ ISO/IEC 27001 є українською версією міжнародного стандарту ISO/IEC 27001, який визначає вимоги до системи управління ІБ організацій [56]. Він включає положення про встановлення, впровадження, функціонування, моніторинг, перегляд, підтримку та вдосконалення системи управління ІБ. Стандарт допомагає організаціям захищати конфіденційність, цілісність та

доступність інформації шляхом впровадження адекватних заходів управління ризиками. Він також наголошує на необхідності залучення вищого керівництва та систематичного підходу до управління інформаційною безпекою.

Стандарт ДСТУ ISO/IEC 27001 встановлює вимоги до системи управління ІБ для підприємства будь-якого розміру (рис. 1.4).

Рис. 1.4. Вимоги стандарту ДСТУ ISO/IEC 27001 до системи управління ІБ

Вимоги ДСТУ ISO/IEC 27001 забезпечують комплексний підхід до управління інформаційною безпекою, акцентуючи на важливості систематичного оцінювання та управління ризиками, зокрема:

– оцінка ризиків ІБ. Ідентифікація ризиків для інформаційних активів, оцінка потенційних наслідків, ймовірності їх виникнення та вибір заходів для обробки ризиків;

– заходи управління ризиками. Вибір та застосування контрольних заходів для мінімізації ідентифікованих ризиків;

– політика ІБ. Розробка політики, що відображає наміри та напрямки діяльності організації у сфері ІБ;

– організаційні аспекти ІБ. Визначення ролей, відповідальності та повноважень у сфері ІБ;

– управління активами ІБ. Ідентифікація та класифікація інформаційних активів, розробка процедур обробки;

– фізична та технічна безпека. Захист інформаційних систем, забезпечення безпечного фізичного середовища;

– управління доступом. Контроль доступу до інформації та інформаційних систем;

– управління інцидентами ІБ. Розробка процедур реагування на інциденти ІБ;

– неперервність діяльності. Планування неперервності діяльності та відновлення після інцидентів;

– суміжні аспекти. Забезпечення відповідності законодавчим та контрактним вимогам, підвищення обізнаності та навчання персоналу.

Отже, стандарт ДСТУ ISO/IEC 27001, надає організаціям комплексний підхід до управління ІБ. Він допомагає ідентифікувати, оцінювати та управляти ризиками, пов'язаними з інформаційними активами, забезпечуючи захист конфіденційності, цілісності та доступності інформації. Такий підхід сприяє вдосконаленню ділової репутації та забезпечує відповідність законодавчим та контрактним вимогам у сфері ІБ.

Стандарт ISO/IEC 27002:2013 визначає керівні принципи та найкращі практики для впровадження заходів інформаційної безпеки в рамках систем управління ІБ (рис. 1.5).

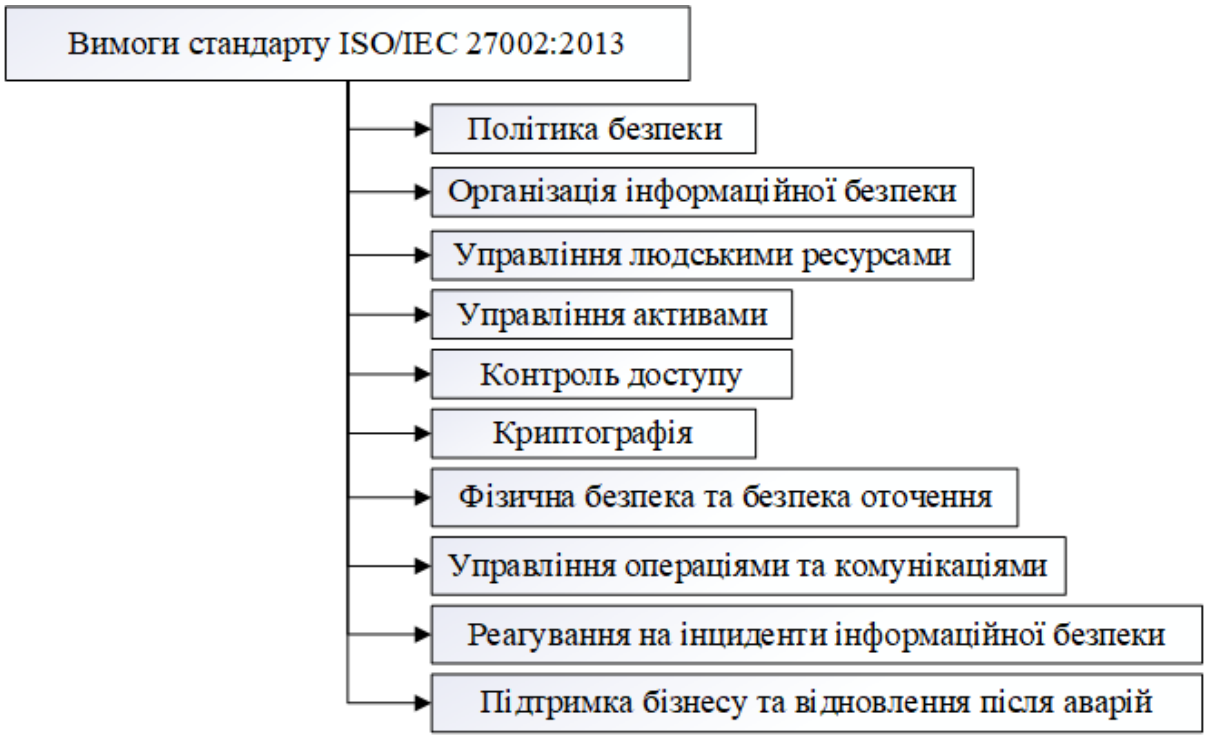

Рис. 1.5. Вимоги стандарту ISO/IEC 27002:2013 до системи управління ІБ

Розглянутий стандарт не встановлює конкретних вимог, але надає рекомендації та рекомендовані процедури, які можуть бути адаптовані під конкретні потреби підприємства. Основні аспекти вимог даного стандарту включають:

– політика безпеки. Розробка та імплементація політики безпеки, яка чітко відображає зобов'язання підприємства до забезпечення інформаційної безпеки;

– організація інформаційної безпеки. Встановлення структури управління для підтримки інформаційної безпеки, включаючи розподіл відповідальності та координацію зусиль між різними підрозділами;

– управління людськими ресурсами. Забезпечення, що всі співробітники, підрядники та треті сторони розуміють свої обов'язки щодо інформаційної безпеки, особливо під час найму, працевлаштування та припинення трудових відносин;

– управління активами. Ідентифікація та класифікація інформаційних активів, включаючи встановлення відповідальності за збереження цих активів;

– контроль доступу. Обмеження доступу до інформації та інформаційних систем лише авторизованим особам згідно з їхніми ролями та потребами;

– криптографія. Використання криптографічних заходів для захисту конфіденційності, автентичності та цілісності інформації;

– фізична безпека та безпека оточення. Захист фізичних приміщень та обладнання від несанкціонованого доступу, збитку та втручання;

– управління операціями та комунікаціями. Забезпечення безпечного управління операціями та процесами комунікації в IT-інфраструктурі;

– реагування на інциденти інформаційної безпеки. Розробка та впровадження планів реагування на інциденти для ефективного відновлення після порушень безпеки;

– підтримка бізнесу та відновлення після аварій. Планування продовження бізнесу та стратегії відновлення для забезпечення безперервності операцій.

У контексті України, впровадження рекомендацій ISO/IEC 27002:2013 також вимагає врахування місцевих законодавчих та нормативних вимог, що регулюють інформаційну безпеку. Це забезпечує, що підходи та процедури, застосовані на підприємстві, відповідають як міжнародним стандартам, так і національним законодавчим вимогам.

ДССЗЗІ відіграє ключову роль у визначенні та регулюванні стандартів інформаційної безпеки на території України. Її вимоги до систем управління ІБ спрямовані на забезпечення адекватного захисту інформаційних активів від різноманітних загроз, що можуть виникнути як ззовні, так і зсередини підприємства. Враховуючи сучасні виклики в сфері кібербезпеки, ДССЗЗІ формулює ряд ключових вимог, які повинні бути враховані при впровадженні та експлуатації ISMS на підприємствах та у державних установах (рис. 1.6).

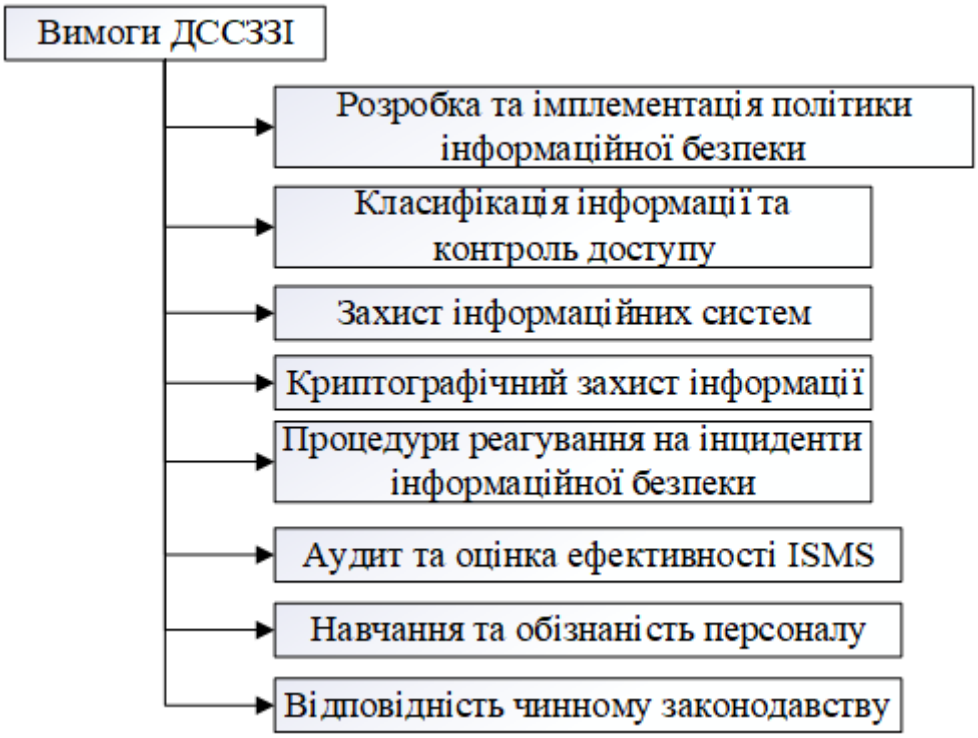

Рис. 1.6. Вимоги ДССЗЗІ до системи управління ІБ

Основні вимоги ДССЗЗІ до системи управління ІБ включають:

– розробку та імплементацію політики інформаційної безпеки. Створення документу, який визначає підходи, цілі та принципи інформаційної безпеки в підприємства;

– класифікацію інформації та контроль доступу. Визначення рівнів конфіденційності інформації та розробка процедур, що обмежують доступ до інформації відповідно до її класифікації;

– захист інформаційних систем. Впровадження заходів технічного та організаційного захисту для запобігання несанкціонованому доступу, зловмисному програмному забезпеченню та іншим загрозам;

– криптографічний захист інформації. Використання криптографічних методів для захисту конфіденційності та цілісності даних під час зберігання та передачі;

– процедури реагування на інциденти інформаційної безпеки. Розробка плану дій для виявлення, аналізу та реагування на інциденти інформаційної безпеки;

– аудит та оцінку ефективності ISMS. Проведення регулярних перевірок та оцінок системи управління інформаційною безпекою для забезпечення її відповідності встановленим вимогам;

– навчання та обізнаність персоналу. Організація тренінгів і семінарів для підвищення обізнаності співробітників з питань інформаційної безпеки та їх ролі в захисті інформаційних активів;

– відповідність чинному законодавству. Забезпечення, що система управління ІБ відповідає національним законодавчим та нормативним вимогам.

Впровадження вимог ДССЗЗІ в системи управління ІБ є критично важливим для забезпечення ефективного захисту інформаційних активів на рівні підприємств та урядових організацій в Україні. Ці вимоги допомагають створити структурований та систематизований підхід до інформаційної безпеки, який включає розробку політики безпеки, класифікацію інформації, захист інформаційних систем, реагування на інциденти, а також навчання та розвиток обізнаності персоналу. Виконання цих стандартів і рекомендацій не лише відповідає національному законодавству та нормативам, але й сприяє підвищенню рівня довіри та безпеки в інформаційному просторі країни, а також підтримує безперервність бізнес-процесів і знижує ризики, пов'язані з інформаційними загрозами.

Закон України № 2163-VIII «Про основні засади кібербезпеки України» встановлює правові та організаційні основи для забезпечення кібербезпеки в країні (рис. 1.7). Він окреслює ролі та обов'язки державних органів і приватних суб'єктів, зокрема об'єктів критичної інфраструктури [11].

Рис. 1.7. Основні положення Закону України № 2163-VIII

Застосування Закону України № 2163-VIII в системах SIEM виділяється у таких аспектах:

– моніторинг та аналіз [12]. SIEM-системи дозволяють виконувати неперервний моніторинг та аналіз безпекових подій, що відповідає вимогам Закону про превентивні заходи проти кіберзагроз;

– звітування про інциденти [13]. Закон вимагає від суб'єктів критичної інфраструктури своєчасне звітування про кіберінциденти, що може бути автоматизовано за допомогою SIEM;

– відповідність та дотримання стандартів [14]. SIEM-системи можуть бути налаштовані так, щоб відповідати стандартам інформаційної безпеки, встановленим законодавством;

– аудит та звітність. Забезпечення можливості аудиту та звітності відповідно до вимог закону, що є важливим для демонстрації відповідності до регулятивних вимог.

Отже, Україна, враховуючи світові тенденції та власний досвід, активно розвиває законодавчу та нормативну базу в сфері інформаційної безпеки. Закони та стратегічні документи встановлюють рамки для ефективного реагування на кіберзагрози, зокрема, для критичної інфраструктури. В цьому контексті SIEM відіграють ключову роль, допомагаючи підприємству дотримуватися вимог і забезпечувати високий рівень захисту.

Табл. 1.3 підсумовує дослідження вимог до впровадження і експлуатації систем управління інформаційною безпекою в Україні.

Таблиця 1.3

Аналіз вимог до впровадження і експлуатації SIEM

	Закон України «Про основні засади кібербезпеки України»	Стратегія кібербезпеки України	Резолюція КМУ щодо кібербезпеки КІ
Дата	05.10.2017	15.03.2016	19.06.2019
Основні положення	Встановлює засади кібербезпеки	Визначає дії для збільшення кібербезпеки	Встановлює вимоги до кібербезпеки
Орган влади	Державна служба спеціального зв'язку та інформаційного захисту України	Кіберполіція	–
Санкції	Кримінальна відповідальність за створення та поширення шкідливого ПЗ, незаконні дії з інформацією	Посилення контролю та запровадження заходів для попередження кіберзлочинності	Розробка механізмів відповідальності за недотримання встановлених норм кібербезпеки
Основні обов'язки	Розробка та впровадження національних стандартів кібербезпеки, координація діяльності у сфері кібербезпеки між різними органами влади, нагляд за дотриманням кібербезпеки в критичній інфраструктурі.	Визначення стратегічних напрямів розвитку кібербезпеки, встановлення пріоритетів для захисту національних інтересів у кіберпросторі, визначення механізмів реагування на кіберзагрози.	Розробка конкретних вимог та рекомендацій для захисту об'єктів критичної інфраструктури, забезпечення впровадження та дотримання цих вимог у відповідних секторах.
Застосування	Компанії критичної інфраструктури	Компанії критичної інфраструктури	Об'єкти критичної інфраструктури

Таблиця вище показує аналіз основних законодавчих актів, що регулюють сферу кібербезпеки в Україні. Через зазначені документи, які визначають обов'язки та відповідальності суб'єктів критичної інфраструктури, можна бачити зростаючу потребу в системах SIEM для моніторингу, аналізу та реагування на інциденти безпеки. Стратегія та законодавчі вимоги вимагають від підприємства впровадження комплексних систем управління безпекою, що робить тему SIEM надзвичайно актуальною для подальших досліджень і розвитку.

Комплексний підхід до управління ІБ полягає в інтеграції різних компонентів безпеки в єдину, координовану систему. Цей підхід не обмежується лише моніторингом та аналізом через системи SIEM, а включає набір ширших заходів та процесів:

– комплексні системи захисту інформації (КСЗІ). Це включає в себе різні технічні та адміністративні механізми, які забезпечують захист інформації від несанкціонованого доступу, модифікації, розголошення чи знищення. Вони можуть включати захист мереж, шифрування даних, управління доступом, фізичний захист обладнання та приміщень;

– системи управління ризиками. Ці системи забезпечують процес ідентифікації, аналізу та управління ризиками, які можуть вплинути на інформаційні активи. Вони включають оцінку ризиків, розробку планів мінімізації ризиків та регулярне оновлення стратегій управління ризиками;

– системи управління інцидентами. Ці системи охоплюють процедури та інструменти для ефективного реагування на інциденти безпеки, включаючи їх виявлення, документування, розслідування та відновлення після інцидентів. Важливим є також вчасне повідомлення про інциденти та їх управління;

– системи управління безперервністю бізнесу. Ці системи створені для забезпечення продовження роботи критичних бізнес-процесів у випадку аварій чи інших перебоїв. Вони включають планування безперервності бізнесу, розробку стратегій відновлення та регулярні вправи та тести на випадок виникнення кризових ситуацій.

Інтегруючи всі ці компоненти, комплексний підхід до ІБ дозволяє організаціям ефективно захищати свої інформаційні системи та активи, реагувати на загрози та відповідати вимогам законодавства та регулювань. Це забезпечує більш стійку та гнучку захисну структуру, що важливо для підтримки безперервності та ефективності бізнесу.

Висновки до першого розділу. У рамках даного розділу було проведено глибоке дослідження нормативно-правової бази України щодо забезпечення інформаційної безпеки підприємства. Детальний аналіз Закону України «Про інформаційну безпеку» виявив ключові аспекти його впливу на системи управління інформацією та подіями, включаючи правові, організаційні, технічні аспекти, комплексність підходу та відповідальність. Аналіз Закону України «Про захист персональних даних» охопив збір, зберігання, обробку, захист та доступ до персональних даних, а також відповідальність та контроль, що є важливим для розуміння ролі SIEM-систем.

Додатково, роль ДССЗЗІ у встановленні загальнодержавних принципів інформаційної безпеки була проаналізована з точки зору конкретних технічних та організаційних вимог до систем управління інформацією та подіями. Це дало змогу визначити, як законодавство та регуляторні органи формують рамки для впровадження систем управління інформаційною безпекою на підприємстві.

У секції про стандарти були розглянуті вимоги ДСТУ ISO/IEC 27001 та ISO/IEC 27002:2013, що підкреслює їх важливість у встановленні комплексного підходу до управління інформаційною безпекою. Основні аспекти цих стандартів, такі як оцінка ризиків, управління доступом, неперервність діяльності, та підтримка бізнесу, були проаналізовані для забезпечення розуміння їх застосування у контексті українського законодавства.

Ці дослідження є ключовими для розуміння, як впровадження та експлуатація SIEM-систем можуть бути оптимізовані для відповідності законодавчим вимогам та стандартам, що забезпечить ефективне забезпечення інформаційної безпеки на підприємстві. Результати цього розділу становлять

основу для подальшого аналізу практик використання SIEM-систем та розробки конкретних рекомендацій щодо інформаційної безпеки.

Розділ 2. АНАЛІЗ ПРАКТИКИ ВИКОРИСТАННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА ПОДІЯМИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1 Досвід використання систем управління інформацією та подіями (SIEM)

Системи управління інформацією та подіями SIEM представляють собою комплексний інструментарій, що інтегрується з різноманітними джерелами даних з метою агрегації, аналізу та кореляції інформації щодо інформаційної безпеки. Сучасні підприємства використовують SIEM-системи для автоматизованого виявлення загроз, відстеження несанкціонованої діяльності, а також для забезпечення відповідності нормативно-правовим актам.

2.1.1 Аналіз потенційних загроз, інцидентів і ризиків безпеки та векторів атак на інформаційні системи.

Ефективне управління інформаційною безпекою є критично важливим для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів в сучасному цифровому світі. У центрі ефективної системи управління інформаційною безпекою лежать три ключові підсистеми: управління ризиками, управління інцидентами, та забезпечення готовності до безперервної діяльності.

Підсистема управління ризиками зосереджується на ідентифікації, аналізі та вживанні заходів щодо мінімізації потенційних загроз для інформаційних систем. Управління інцидентами включає в себе процеси виявлення, реагування та відновлення після безпекових порушень або інших небезпечних подій. Забезпечення готовності до безперервної діяльності важливе для підтримки неперервності бізнес-операцій, навіть у випадках серйозних порушень або надзвичайних ситуацій[15].

Кожна з цих підсистем відіграє вирішальну роль у створенні багатогранної оборони проти різноманітних загроз, з якими стикаються сучасні підприємства.

Разом вони формують сильну, адаптивну структуру, яка забезпечує не лише захист інформаційних активів, але й підтримує гнучкість та стійкість бізнес-процесів.

Управління ризиками є ключовою складовою ефективної системи ІБ. Ризик у контексті інформаційної безпеки можна визначити як потенційну можливість виникнення шкідливої події, яка може негативно вплинути на інформаційні активи або процеси підприємства. Це може включати в себе втрату даних, несанкціонований доступ, зловмисне програмне забезпечення, а також різні форми кібератак.

Ідентифікація ризиків вимагає систематичного огляду інформаційних систем для виявлення потенційних вразливостей та загроз [16]. Це може бути здійснено через процеси, такі як аудит безпеки, аналіз вразливостей, а також моніторинг загроз зовнішнього середовища. Оцінка ризиків включає аналіз ймовірності виникнення шкідливої події та потенційного рівня її впливу на організацію [17]. Це вимагає врахування різних факторів, таких як поточний рівень безпеки, значення активів, які можуть бути зачеплені, та потенційні наслідки порушення безпеки [18].

Стратегії мінімізації ризиків та відповіді на них можуть включати різні заходи, такі як посилення фізичної та цифрової безпеки, впровадження політик безпеки, регулярне навчання персоналу, розробка та впровадження процедур відновлення після аварій, а також застосування технологій шифрування та інших захисних заходів [19]. Важливою частиною стратегії є також створення плану реагування на інциденти, який визначає конкретні кроки для реагування на безпекові порушення.

У процесі управління ризиками важливо не лише визначити потенційні загрози та вразливості, але й розробити ефективні методи для їх оцінки та мінімізації [20]. Ретельний аналіз та планування є ключовими для створення стійкої стратегії безпеки. Для наочного представлення основних аспектів цього процесу, нижче наведено табл. 2.1, яка детально описує кожен етап управління ризиками, від ідентифікації до відповіді на виявлені ризики.

Таблиця 2.1

Етапи управління ризиками

Етап	Опис	Ключові дії та інструменти
Визначення ризиків	Аналіз потенційних загроз і вразливостей, які можуть негативно вплинути на інформаційні системи	Сканування вразливостей, аналіз загроз, оцінка впливу на бізнес
Ідентифікація ризиків	Систематичний огляд інформаційних систем для виявлення потенційних вразливостей та загроз.	Аудит безпеки, моніторинг мереж, регулярні інспекції безпеки
Оцінка ризиків	Оцінка ймовірності виникнення шкідливої події та потенційного рівня її впливу на організацію.	Квантитативний та кваліативний аналіз, матриця ризиків, оцінка впливу
Стратегії мінімізації ризиків	Розробка та імплементація заходів для мінімізації виявлених ризиків.	Розробка політик безпеки, застосування технологій шифрування, управління доступом
Відповідь на ризики	Розробка та впровадження планів реагування на інциденти та ризики.	Плани реагування на інциденти, навчання персоналу, процедури відновлення після аварій

Ця таблиця підкреслює комплексний підхід до управління ризиками в контексті інформаційної безпеки. Вона демонструє, як систематичний огляд, оцінка та реагування на потенційні ризики можуть допомогти організаціям не лише захистити свої інформаційні активи, але й підтримувати безперервність бізнес-процесів у випадку виникнення непередбачених подій.

Управління інцидентами інформаційної безпеки є важливим елементом загальної стратегії безпеки підприємства. Інциденти інформаційної безпеки можуть включати в себе різноманітні події, такі як несанкціонований доступ до систем, витік даних, зловмисне програмне забезпечення, а також інші порушення безпеки, що можуть мати негативний вплив на інформаційні ресурси та операції підприємства.

Процес управління інцидентами включає в себе кілька ключових етапів: виявлення інцидентів, реагування на них, та відновлення після інцидентів [21]. Виявлення інцидентів здійснюється через моніторинг систем та мереж на наявність ознак порушення безпеки. Реагування на інциденти включає в себе швидке вжиття заходів для локалізації та усунення загрози, а також зменшення впливу інциденту на операції підприємства [22]. Відновлення після інцидентів спрямоване на відновлення нормального функціонування систем та мінімізацію збитків.

Для ефективного управління інцидентами необхідно розробити та імплементувати детальні плани реагування на інциденти, які визначають конкретні процедури та відповідальних осіб для швидкого і ефективного реагування на безпекові порушення.

Управління інцидентами інформаційної безпеки вимагає чіткої структури та визначених процесів для ефективного виявлення, реагування та відновлення після безпекових порушень [23]. Кожен етап у цьому процесі має свої специфічні завдання та виклики, від первинної ідентифікації потенційних інцидентів до розробки та реалізації комплексних планів відновлення. Для кращого візуального представлення та детального опису ключових елементів управління інцидентами, нижче наведено табл. 2.2, яка включає аспекти кожного етапу цього процесу.

Таблиця 2.2

Елементи управління інцидентами

Елемент	Опис	Ключові дії та інструменти	Додаткові деталі
Визначення інцидентів	Ідентифікація подій, що можуть мати негативний вплив на інформаційні ресурси та операції.	Класифікація інцидентів, процедури оцінки подій	Розробка критеріїв для класифікації, тренування персоналу з виявлення ознак порушення

Продовження табл. 2.2

Елемент	Опис	Ключові дії та інструменти	Додаткові деталі
Виявлення інцидентів	Моніторинг систем на наявність ознак порушення безпеки.	Моніторинг мережі, системи виявлення вторгнень, ПЗ безпеки	Налаштування сигналів тривоги, автоматичне блокування підозрілих дій
Реагування на інциденти	Швидке вжиття заходів для локалізації та усунення загрози.	План реагування на інциденти, команда швидкого реагування	Сценарії реагування для різних типів інцидентів, координація з зовнішніми експертами
Відновлення після інцидентів	Відновлення нормального функціонування систем та мінімізація збитків	Процедури відновлення, засоби резервного копіювання та відновлення даних	Розробка планів для різних рівнів відновлення, періодичне тестування та оновлення планів

Табл. 2.2 надає огляд процесу управління інцидентами, відкриваючи глибше розуміння необхідних заходів для ефективного виявлення, реагування та відновлення в контексті ІБ. Вона служить джерелом для планування та підготовки організацій до різних типів інцидентів, забезпечуючи їх готовність ефективно реагувати на потенційні загрози.

Забезпечення готовності до безперервної діяльності є ключовим компонентом комплексного управління інформаційною безпекою. Це включає в себе розробку та підтримку стратегій та планів, що гарантують безперервність бізнес-процесів навіть у випадку серйозних інцидентів або надзвичайних ситуацій [24]. Підтримка безперервності бізнесу забезпечує, що критичні бізнес-функції залишаються оперативними під час та після інцидентів, мінімізуючи збитки та дискомфорт для клієнтів та співробітників.

Розробка стратегій та планів для підтримки безперервної діяльності включає аналіз критичних бізнес-процесів, визначення потенційних ризиків для цих процесів, та розробку процедур для їх відновлення [25]. Це також включає в

себе вибір відповідних технологій та систем, які можуть підтримати неперервність операцій.

Тестування та оновлення планів готовності є важливими для забезпечення їх актуальності та ефективності. Регулярні вправи та симуляції допомагають виявити потенційні проблеми та слабкі місця в планах, а також забезпечують, що персонал добре підготовлений до дій у випадку реальних інцидентів.

У табл. 2.3 представлено детальний огляд ключових елементів забезпечення готовності до безперервної діяльності підприємства.

Таблиця 2.3

Елементи забезпечення готовності до безперервної діяльності

Елемент	Опис	Ключові дії та інструменти	Додаткові деталі
Важливість підтримки безперервності	Забезпечення неперервності критичних бізнес-процесів	Аналіз критичних функцій, визначення пріоритетів відновлення	Оцінка впливу на бізнес, визначення важливості різних операцій
Розробка стратегій та планів	Створення детальних планів для забезпечення безперервності бізнесу	Розробка планів відновлення, вибір відповідних технологій	Врахування різних сценаріїв інцидентів, інтеграція з іншими планами безпеки
Тестування та оновлення планів	Регулярна перевірка та адаптація планів з метою забезпечення їх актуальності та ефективності.	Проведення тренувань та симуляцій, оновлення планів відповідно до змін у середовищі	Залучення всього персоналу, аналіз результатів тренувань

Табл. 2.3 відображає всебічний підхід до підготовки підприємства до можливих непередбачених обставин, гарантуючи, що критичні бізнес-процеси зможуть витримати різноманітні виклики. Вона служить важливим інструментом для планування, тестування та постійного оновлення стратегій безперервної діяльності, допомагаючи підприємству залишатися стійкими та конкурентоспроможними навіть у найскладніших умовах.

В сфері інформаційної безпеки, важливо враховувати різноманітність загроз, що охоплюють як зовнішні, так і внутрішні виклики [26]. Зовнішні загрози, такі як фішинг, віруси, шкідливе ПЗ, та DDoS-атаки, можуть призвести до несанкціонованого доступу, втрати або пошкодження даних та перерв у сервісі. Внутрішні загрози включають навмисне або несвідоме діяння персоналу, яке може загрожувати цілісності та конфіденційності даних.

Інциденти безпеки часто виникають як результат реалізації цих загроз. Наприклад, успішна фішингова атака може призвести до витоку конфіденційної інформації [27]. Важливість зрозуміння взаємозв'язку між ризиками та інцидентами полягає у вмінні антиципувати потенційні порушення та розробляти стратегії для запобігання чи мінімізації їх впливу.

Взаємодія між інцидентами та ризиками впливає на загальну безпеку системи. Наприклад, регулярне виявлення вразливостей та їх своєчасне усунення допомагає знизити ймовірність успішних кібератак [28]. Крім того, ефективне управління ризиками, включаючи навчання персоналу та впровадження сильних політик безпеки, може значно знизити вплив внутрішніх загроз.

У табл. 2.4 нижче представлено всебічний огляд різноманітних типів загроз, інцидентів та ризиків, які можуть впливати на інформаційні системи. Цей огляд допомагає ідентифікувати потенційні виклики та розробити стратегії для їх запобігання та ефективного реагування.

Таблиця 2.4

Огляд типів загроз та інцидентів

Тип загрози/інциденту	Потенційний вплив на систему	Стратегії запобігання та реагування
Віруси та шкідливе ПЗ	Несанкціонований доступ, втрата або пошкодження даних.	Антивірусне програмне забезпечення, регулярні оновлення.
Фішингові атаки	Крадіжка конфіденційної інформації, шахрайство.	Навчання персоналу, застосування фільтрів електронної пошти.

Продовження табл. 2.4

Тип загрози/інциденту	Потенційний вплив на систему	Стратегії запобігання та реагування
DDoS-атаки	Порушення доступності ресурсів, зупинка бізнес-операцій.	Захисні мережеві рішення, плани реагування на інциденти.
Неавторизований доступ	Втрата або пошкодження даних, порушення конфіденційності.	Системи контролю доступу, шифрування даних.
Витоки даних	Втрата конфіденційності, репутаційні збитки, юридичні наслідки.	Захист даних та шифрування, контроль доступу до інформації.
Інсайдерські загрози	Саботаж, крадіжка даних, шпигунство.	Політики безпеки, моніторинг поведінки співробітників.
Фізичні загрози	Пошкодження обладнання, втрата даних.	Фізичні заходи безпеки, плани відновлення після стихійних лих.
Застаріле програмне забезпечення	Вразливості у застарілому ПЗ, легкий доступ для хакерів.	Регулярне оновлення програмного забезпечення, патч-менеджмент.

Ця таблиця є важливим інструментом для керівників інформаційної безпеки, надаючи їм необхідну інформацію для розуміння та відповіді на широкий спектр можливих загроз. Вона сприяє розробці гнучких та ефективних стратегій безпеки, що забезпечують захист цінних інформаційних активів.

2.1.2 Аналіз можливостей сучасних SIEM – систем у контексті забезпечення інформаційної безпеки.

В сучасному світі інформаційних технологій системи управління інформацією та подіями (SIEM) відіграють вирішальну роль у забезпеченні безпеки інформаційних систем. SIEM-системи здатні ефективно збирати, аналізувати та корелювати величезні обсяги даних з різноманітних джерел, включаючи мережеві пристрої, сервери, системи кібербезпеки та інші. Ці системи забезпечують комплексний огляд безпеки, швидко виявляючи

потенційні загрози та реагуючи на інциденти в режимі реального часу. Ключовою перевагою SIEM є можливість інтеграції та аналізу даних з різних джерел для створення більш глибокого розуміння загроз та управління інформаційною безпекою.

Серед найвідоміших SIEM-систем можна виділити такі як Splunk, IBM QRadar, ArcSight та OSSIM. Splunk відомий своєю потужною аналітичною здатністю та гнучкістю у візуалізації даних, що робить його ідеальним для складного аналізу безпекових подій. IBM QRadar вирізняється своїми здібностями до авансованого корелювання подій та швидкої ідентифікації загроз. ArcSight від Micro Focus забезпечує міцну платформу для збору та аналізу логів, сприяючи ефективному управлінню інцидентами. OSSIM, як відкрите програмне забезпечення, надає основні можливості SIEM, включаючи збір та аналіз логів, а також корелювання подій, що є корисним для організацій з обмеженим бюджетом.

Splunk

Splunk є високопродуктивною платформою для пошуку, моніторингу, аналізу та візуалізації машинно-згенерованих даних у реальному часі [29]. Ця система знаходить широке застосування у сфері інформаційної безпеки, де вона допомагає аналізувати логи та інші дані для виявлення потенційних загроз та незаконних дій (рис. 2.1).

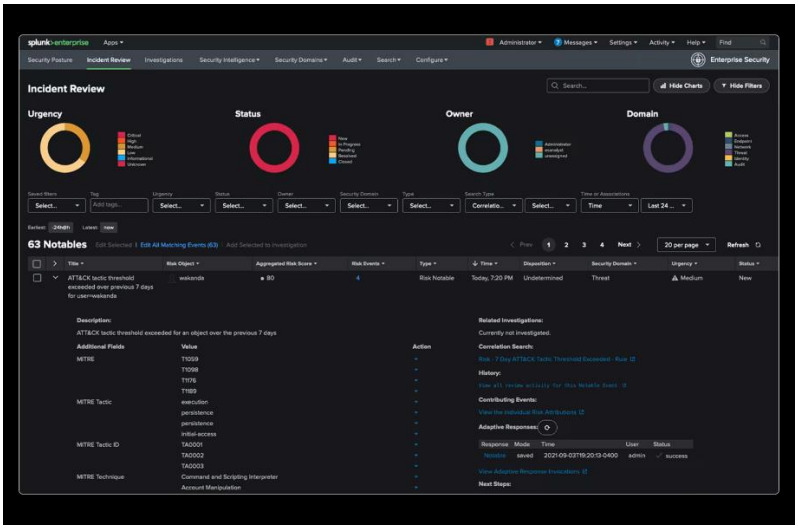

Рис. 2.1. Інтерфейс користувача системи «Splunk»

Архітектура Splunk побудована на модульному принципі та включає такі ключові компоненти:

– проміжні сервери (Forwarders). Збирають дані з різних джерел і пересилають їх на індексатори;

– індексатори (Indexers). Зберігають і індексують отримані дані;

– пошукові голови (Search Heads). Надають інтерфейс для пошуку, аналізу та візуалізації даних.

Основні функції Splunk включають [30]:

– моніторинг в реальному часі. Splunk дозволяє відстежувати системні події нальоту;

– управління логами. Ефективне управління лог-файлами з різних систем та додатків;

– попередження. Автоматична генерація сповіщень при виявленні певних подій або аномалій;

– візуалізація даних. Графічна візуалізація інформації для зручнішого аналізу;

– звітність згідно стандартів. Автоматизована підготовка звітів для дотримання вимог стандартів безпеки.

Splunk відіграє ключову роль в ідентифікації та відстеженні можливих інцидентів безпеки, а також у забезпеченні загальної операційної ефективності. Для всебічного розуміння цієї системи, необхідно розглянути її основні переваги та недоліки (рис. 2.2).

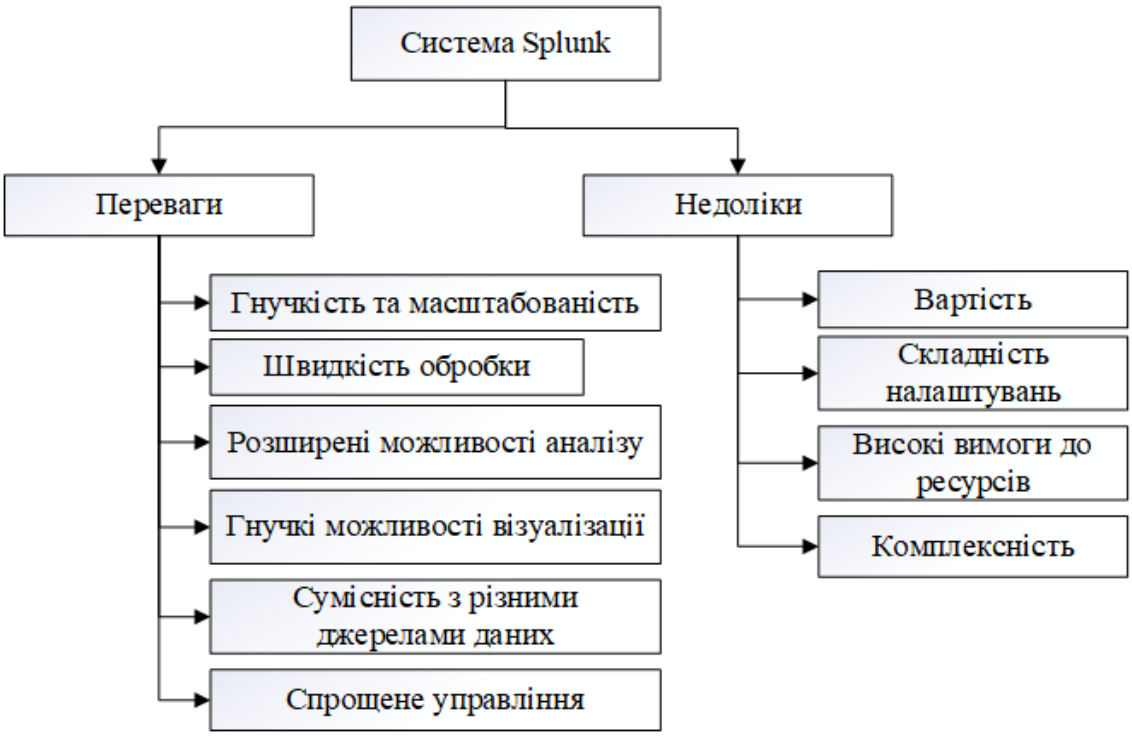

Рис. 2.2. Переваги та недоліки системи «Splunk»

До переваг даної системи відносяться [31]:

– гнучкість та масштабованість. Splunk може легко масштабуватися від невеликих до великих підприємств;

– швидкість обробки. Висока швидкість пошуку та аналізу даних в реальному часі;

– розширені можливості аналізу. Глибокий аналіз даних з можливістю кореляції різних типів інформації;

– гнучкі можливості візуалізації. Множинні опції для налаштування дашбордів та звітів;

– сумісність з різними джерелами даних. Можливість інтеграції з різними системами та платформами;

– спрощене управління. Інтуїтивний користувацький інтерфейс та легкість в управлінні.

Недоліки Splunk [32]:

– вартість. Ліцензійна політика базується на об'ємі оброблюваних даних, що може бути дорогою для невеликих підприємств;

– складність налаштувань. Необхідність глибокого знання для налаштування більш складних функцій;

– високі вимоги до ресурсів. Для ефективної роботи потребує значних обчислювальних ресурсів;

– комплексність. Для використання всіх функціональних можливостей потрібно мати досить великий досвід роботи з системою.

Отже, Splunk є високоефективним рішенням для управління інформацією та подіями в контексті інформаційної безпеки. Ця система відзначається високою гнучкістю, масштабованістю і швидкістю обробки даних. До того ж, вона пропонує розширені можливості для аналітичного моделювання та візуалізації. Однак ефективне використання Splunk потребує відповідного фінансування та технічної експертизи.

IBM QRadar

IBM QRadar є інтегрованою системою управління інформаційною безпекою та подіями, розробленою для ефективного моніторингу, виявлення, дослідження та звітування про загрози безпеки в реальному часі (рис. 2.3). Ця система широко використовується в корпоративних мережах для аналізу подій та даних журналів з різноманітних джерел [33].

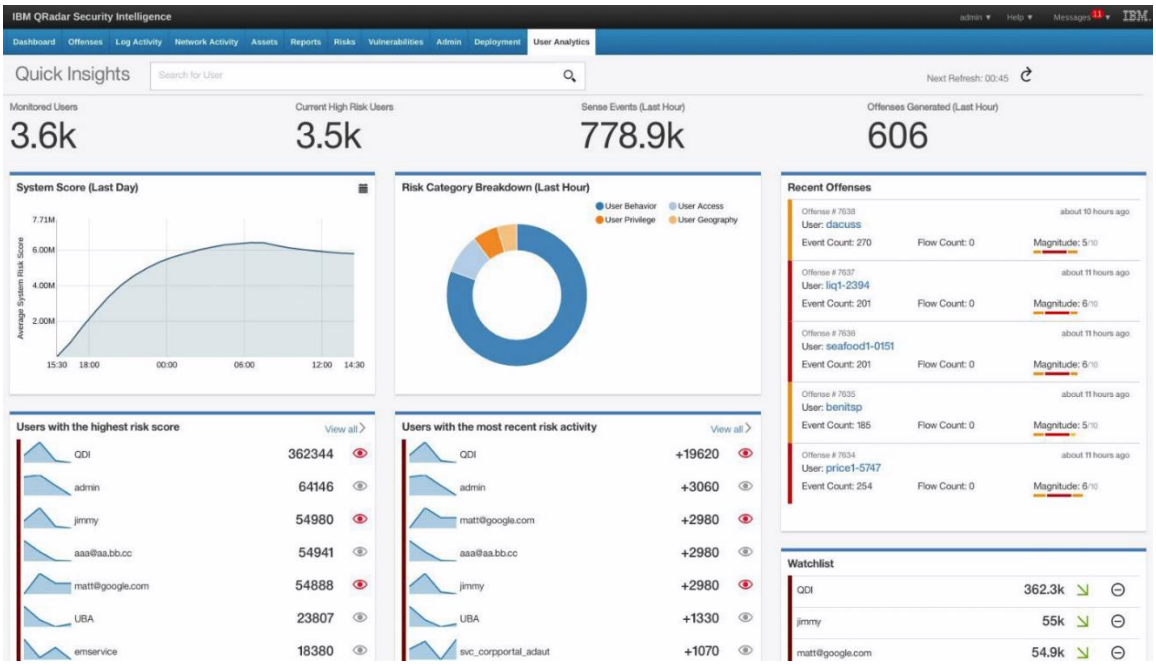

Рис. 2.3. Інтерфейс користувача системи «IBM QRadar»

QRadar використовує розподілену архітектуру, що дозволяє забезпечити масштабованість та гнучкість. Вона складається з кількох компонентів [34]:

– QRadar Event Collector. Збір та агрегація даних;

– QRadar Event Processor. Зберігання, нормалізація та кореляція подій;

– QRadar SIEM Console. Інтерфейс користувача для аналізу даних, створення правил та візуалізація;

– QRadar Flow Processor. Аналіз мережевих потоків;

– QRadar Data Node. Додаткове сховище для даних.

До функціональних можливостостей, що роблять IBM QRadar ефективним інструментом для комплексного управління інформаційною безпекою в корпоративних мережах можна віднести [35]:

– моніторинг в реальному часі. QRadar відстежує події безпеки та мережеві потоки в реальному часі, що дозволяє оперативно реагувати на загрози;

– управління логами. Система забезпечує централізоване зберігання, агрегацію та нормалізацію логів з різних джерел, що спрощує їх аналіз;

– попередження та кореляція подій. QRadar автоматично генерує сповіщення на основі заданих правил та кореляції подій, що дозволяє виявляти складні загрози;

– візуалізація даних. Система пропонує широкий набір дашбордів та графічних інструментів для ефективного аналізу стану безпеки;

– звітність. QRadar може автоматизовано генерувати звіти для відповідності регуляторним стандартам та політикам безпеки, таким як GDPR, PCI DSS, і так далі.

Ця система забезпечує комплексний аналіз мережевих подій та логів з різних джерел, включаючи фізичні, віртуальні та хмарні середовища. Щоб дати повне розуміння потенціалу цього продукту, потрібно розглянути його ключові переваги та недоліки (рис. 2.4).

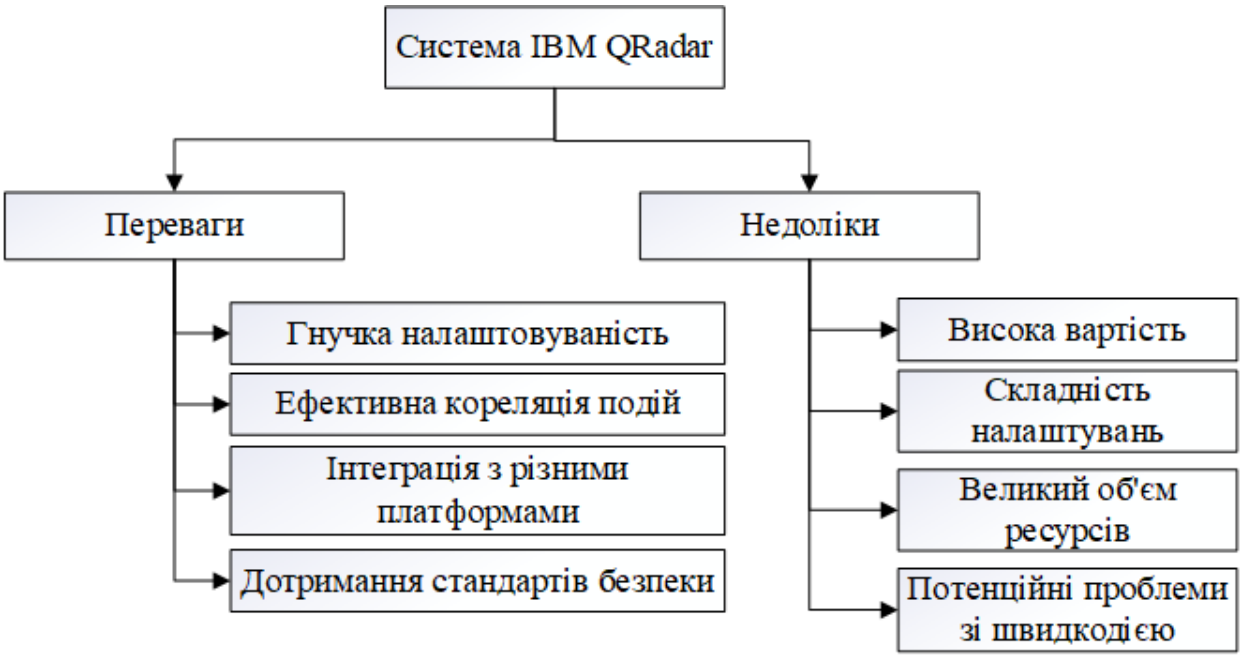

Рис. 2.4. Переваги та недоліки системи «IBM QRadar»

Переваги системи [36]:

– гнучке налаштування. Високий рівень налаштування для конкретних потреб підприємства;

– ефективна кореляція подій. Розширені алгоритми для виявлення складних загроз;

– інтеграція з різними платформами. Широкі можливості інтеграції з іншими системами безпеки;

– дотримання стандартів безпеки. Забезпечує автоматизовану звітність для регуляторних стандартів, таких як GDPR, HIPAA, тощо.

Недоліки [37]:

– висока вартість. Ліцензійні та експлуатаційні витрати можуть бути досить великими, особливо для малих та середніх підприємств;

– складність налаштувань. Для ефективної роботи може знадобитися досвідчений персонал;

– великий об'єм ресурсів. Для повноцінної роботи системи може знадобитися потужне апаратне забезпечення;

– потенційні проблеми зі швидкодією. При обробці великих об'ємів даних може спостерігатися зниження продуктивності.

Отже, IBM QRadar є потужним рішенням для управління інформаційною безпекою та подіями, яке відзначається гнучкістю, ефективною кореляцією подій та широкими можливостями інтеграції. Ця система ідеально підходить для великих підприємств, які прагнуть високого рівня захисту та дотримання регуляторних стандартів. Проте, висока вартість та вимоги до кваліфікованого персоналу та апаратних ресурсів можуть стати обмеженням для малих та середніх підприємств.

ArcSight (Micro Focus)

ArcSight від компанії Micro Focus – це розширене рішення для управління безпекою та подіями в інформаційних системах (рис. 2.5). Система розроблена для збору, аналізу та кореляції логів і подій з різних джерел з метою надання оперативної картини стану безпеки корпоративної мережі [38].

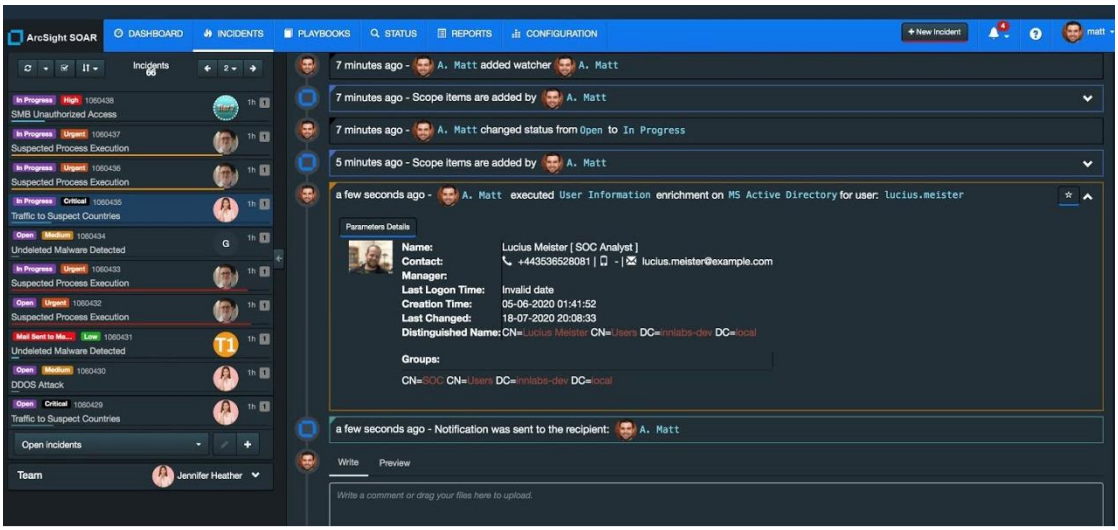

Рис. 2.5. Інтерфейс користувача системи «ArcSight»

Система «ArcSight» працює на основі модульної архітектури, що включає в себе [39]:

– ArcSight Logger. Модуль для збору і зберігання логів;

– ArcSight ESM (Enterprise Security Manager). Центральний компонент для кореляції подій та видачі сповіщень;

– ArcSight Connectors. Модулі для інтеграції з різними джерелами даних;

– ArcSight Investigate. Модуль для проведення розширених розслідувань.

Основні функції даної системи складаються із [40]:

– реальний моніторинг. ArcSight дозволяє відстежувати події в корпоративній мережі в реальному часі;

– управління логами. Збір, архівація та пошук логів з різних систем;

– автоматичні попередження. Генерація сповіщень при виявленні аномалій або підозрілих дій;

– аналіз кореляції. Ідентифікація зв'язків між різними подіями для виявлення комплексних загроз;

– дотримання стандартів безпеки. Підтримка різних регуляторних стандартів через автоматизовану звітність.

ArcSight забезпечує комплексний підхід до управління інформаційною безпекою. Ця система використовується підприємствами різного розміру для моніторингу, аналізу та реагування на інциденти безпеки. Однак, як і будь-яка технологічна платформа, ArcSight має свої переваги та недоліки (рис. 2.6).

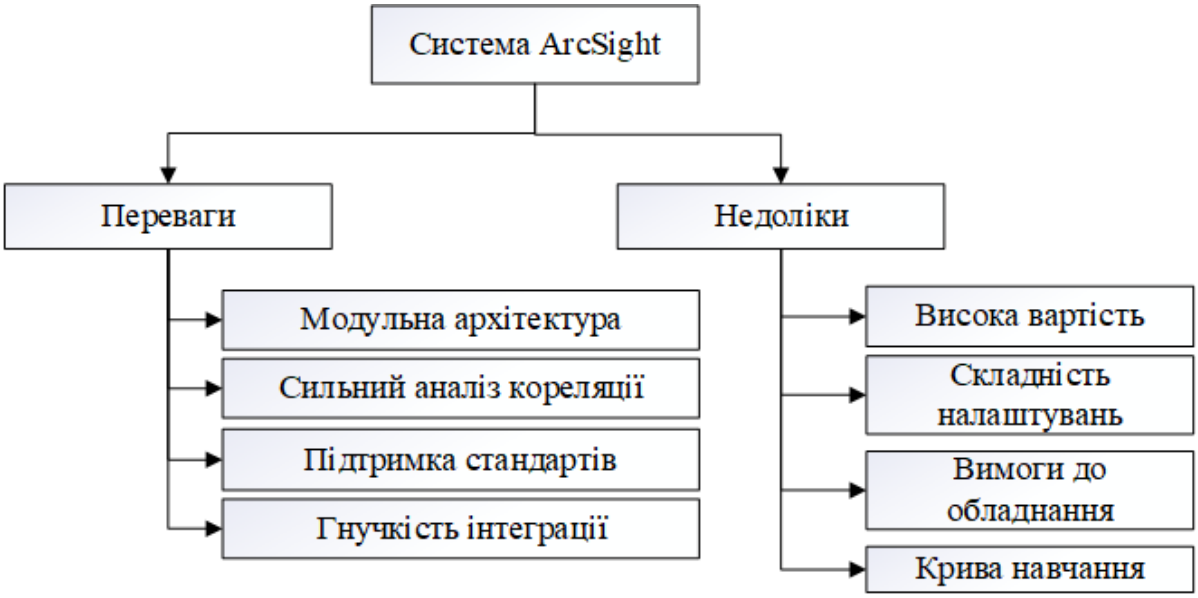

Рис. 2.6. Переваги та недоліки системи «ArcSight»

До основних переваг системи належать [41]:

– модульна архітектура. Легкість внесення змін та масштабування системи;

– сильний аналіз кореляції. Ефективна ідентифікація складних загроз на основі аналізу кореляції;

– підтримка стандартів. Вбудовані можливості для звітності згідно з різними регуляторними стандартами;

– гнучкість інтеграції. Широкі можливості для інтеграції з іншими системами безпеки та джерелами даних.

Недоліки [42]:

– висока вартість. Початкова вартість та вартість власності можуть бути досить великими;

– складність налаштування. Може знадобитися багато часу та ресурсів для правильного налаштування системи;

– вимоги до обладнання. Високі системні вимоги для оптимальної роботи;

– крива навчання. Для ефективної роботи з системою потрібна кваліфікована команда спеціалістів.

Отже, ArcSight від Micro Focus є потужним інструментом для управління інформаційною безпекою, що надає високий рівень контролю та аналітичних можливостей. Його модульна архітектура, розширені функції кореляційного аналізу та гнучкість інтеграції роблять його привабливим вибором для багатьох підприємств. Однак, висока вартість, складність налаштування та вимоги до технічних ресурсів можуть стати перешкодами для малого та середнього бізнесу. Загалом, це є ефективне рішення для великих підприємств з достатніми ресурсами для його імплементації та підтримки.

OSSIM

OSSIM від AlienVault - це інтегроване рішення для управління безпекою та подіями (SIEM) в інформаційних системах (рис. 2.7). Розроблений як відкрите програмне забезпечення, OSSIM забезпечує збір, аналіз та кореляцію логів і подій з різних джерел, дозволяючи користувачам отримувати уявлення про стан безпеки їх мереж.

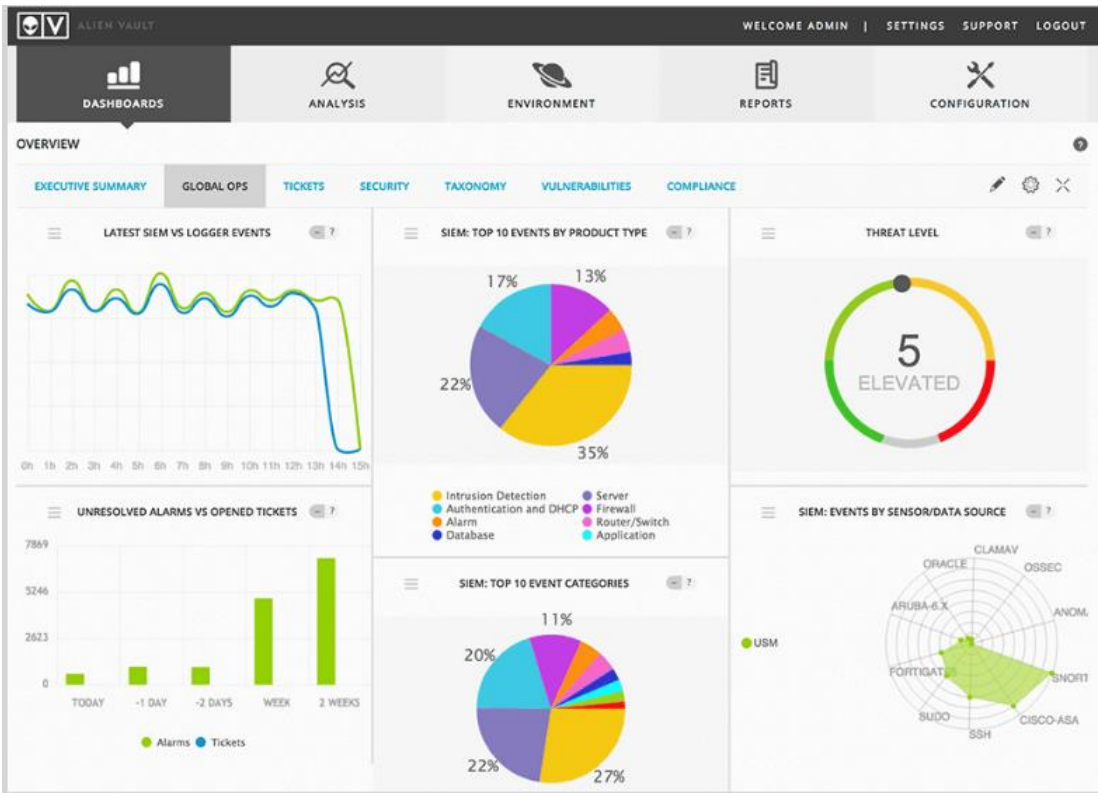

Рис. 2.7. Інтерфейс користувача системи «OSSIM»

Система OSSIM базується на модульній архітектурі, що включає:

– OSSIM Server. Центральний компонент для кореляції подій та видачі сповіщень;

– Sensor. Модулі для збору даних з різних джерел;

– Database. Склад для зберігання та аналізу даних;

– Web Interface. Інтерфейс для візуалізації даних та управління системою.

OSSIM, як відкрите рішення для управління інформаційною безпекою, забезпечує інструменти для моніторингу, аналізу та виявлення загроз в мережі. Його використання підходить для різних організацій, зокрема тих, які шукають економічно ефективні рішення. Однак, як і будь-яка технологічна платформа, OSSIM має свої переваги та недоліки, що важливо врахувати при оцінці його придатності для конкретного бізнесу (рис. 2.8).

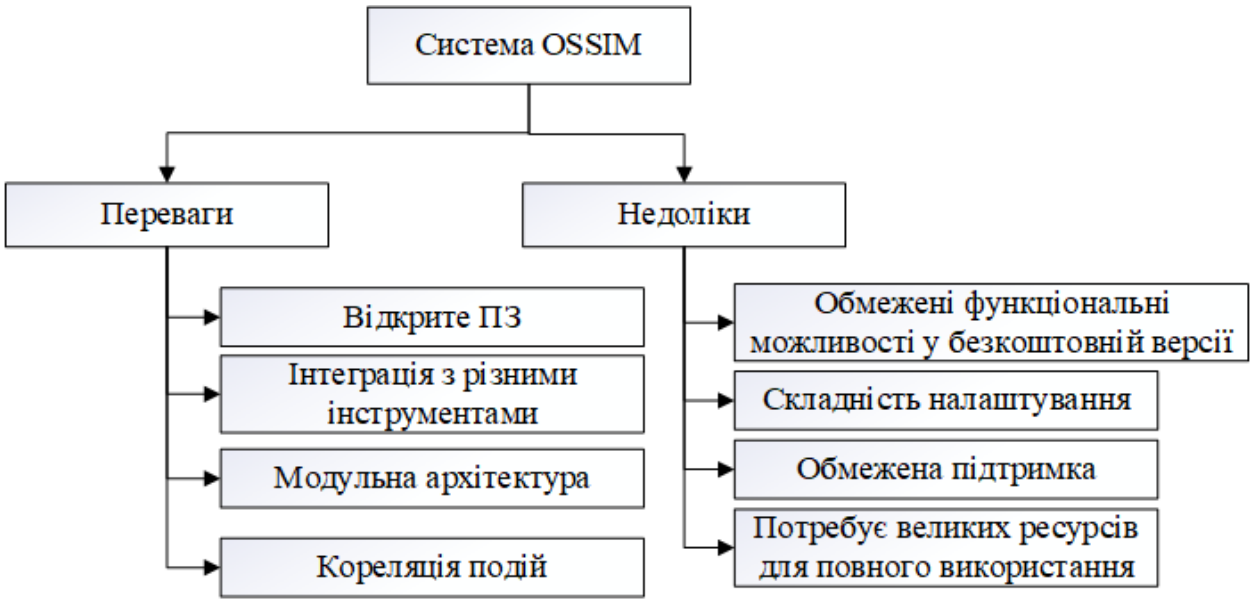

Рис. 2.8. Переваги та недоліки системи «OSSIM»

Переваги OSSIM:

– відкрите ПЗ. Безкоштовне використання та можливість налаштування під конкретні потреби;

– інтеграція з різними інструментами. Підтримка широкого спектру засобів моніторингу та безпеки;

– модульна архітектура. Гнучкість у виборі компонентів для специфічних задач;

– кореляція подій. Ефективне виявлення складних загроз.

Недоліки OSSIM:

– обмежені функціональні можливості у безкоштовній версії. Повний спектр функцій доступний лише у комерційній версії;

– складність налаштування. Вимагає певних знань та навичок для ефективного налаштування;

– обмежена підтримка. Як відкрите програмне забезпечення, має меншу підтримку порівняно з комерційними продуктами;

– потребує великих ресурсів для повного використання. Ефективна робота системи вимагає значних обчислювальних ресурсів.

Отже, OSSIM, як відкрите програмне забезпечення для управління інформаційною безпекою, пропонує безкоштовний, але ефективний

інструментарій для моніторингу та аналізу безпеки мережі. Воно інтегрує різні засоби безпеки в одну систему, забезпечуючи гнучкість та модульність. Однак, його використання може бути ускладненим через складність налаштувань та обмежену підтримку. Це робить OSSIM підходящим для організацій з технічними знаннями та ресурсами для налаштування системи.

2.2 Організація розробки сучасних систем управління інформацією та подіями інформаційної безпеки

В сучасному інформаційному просторі важливість систем управління інформацією та подіями для забезпечення інформаційної безпеки підприємства не може бути переоцінена. Створення ефективної SIEM-системи є високо складним та багатоетапним завданням, яке вимагає вдумливого планування, аналізу і координації зусиль численних зацікавлених сторін. Весь процес, від вибору платформи до впровадження та підтримки, має бути чітко організований. Недооцінка будь-якого з цих етапів може призвести до серйозних ризиків безпеки та додаткових фінансових витрат. Тому важливо зосередитися на кожному аспекті розробки, включаючи архітектуру, функціональність, тестування та супроводження системи.

2.2.1 Аналіз методичних матеріалів щодо розробки ефективної системи управління інформаційною безпекою підприємства.

Система управління інформаційною безпекою (СУІБ) відіграє ключову роль у стратегічному плануванні будь-якої підприємства, оскільки вона повинна бути тісно інтегрованою з основними бізнес-процесами та стратегіями компанії. Її роль полягає у забезпеченні захисту та підтримки тих інформаційних активів, які відіграють вирішальну роль у досягненні бізнес-цілей підприємства [43]. Ефективно впроваджена СУІБ дозволяє підприємства захистити свої критичні інформаційні ресурси, враховуючи їх важливість та вплив на загальну стратегію та успіх компанії. Це гарантує, що інформаційні активи оберігаються відповідно

до їх значущості, що є невід'ємною частиною загальної стратегії інформаційної безпеки та стратегічного планування підприємства.

У рамках ефективної СУІБ критично важливим є чітке визначення та розподіл відповідальностей між усіма учасниками процесу [44]. Це включає встановлення конкретних ролей та обов'язків не лише для керівництва, але й для співробітників, користувачів систем та інших зацікавлених сторін. Такий розподіл відповідальності сприяє підвищенню обізнаності та залученості всіх членів підприємства у процес захисту інформаційних активів. Важливо, щоб кожен розумів свою роль у системі безпеки та був відповідальним за дотримання встановлених правил та процедур. Це допомагає створити організаційну культуру, в якій безпека інформації є загальною відповідальністю, а не лише обов'язком окремо визначених відділів чи осіб.

Забезпечення послідовності та ефективності в СУІБ вимагає використання стандартизованих процесів управління. Важливим аспектом тут є прийняття та застосування міжнародних стандартів, таких як ISO/IEC 27001 [45]. Ці стандарти надають організаціям уніфіковані керівництва та найкращі практики для розробки, імплементації, управління та постійного вдосконалення їхніх систем інформаційної безпеки. Вони включають у себе чіткі вказівки щодо таких аспектів, як оцінка ризиків, управління інцидентами, контроль доступу та інші ключові елементи. Застосування таких стандартів дозволяє забезпечити, що управління інформаційною безпекою у компанії відповідає високим міжнародним вимогам, а також сприяє уніфікації та координації зусиль зі зміцнення безпеки на всіх рівнях підприємства. Це, у свою чергу, веде до зменшення відхилень та помилок у процесах управління безпекою, підвищуючи загальну надійність та ефективність системи.

Інтегруючи СУІБ зі стратегічним плануванням, розподілом відповідальності, та стандартизацією процесів, підприємства можуть забезпечити, що їх система не тільки ефективно захищає інформаційні активи, але й сприяє досягненню загальних бізнес-цілей та корпоративних місій [46]. Ця

комплексна підготовка створює надійну основу для безпечного інформаційного середовища, готового адаптуватися до змінних умов та викликів.

Для забезпечення ефективності та послідовності в роботі СУІБ важливо використовувати стандартизовані процеси. Це означає, що управління ІБ повинно базуватися на загальноприйнятих принципах і методологіях, які визначені у відповідних міжнародних стандартах, таких як ISO/IEC 27001. Ці стандарти надають детальні вказівки щодо того, як створювати, імплементувати, управляти та постійно вдосконалювати систему управління ІБ. Вони включають у себе найкращі практики, що дозволяють уніфікувати підходи до ІБ, забезпечуючи їхню послідовність і надійність. Стандартизація в цій області грає ключову роль у мінімізації відхилень та помилок у процесах управління безпекою, забезпечуючи високий рівень захисту інформаційних активів підприємства.

Реалізація СУІБ є важливим кроком для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів підприємства. Цей процес включає інтеграцію різних етапів, починаючи від стратегічного планування і закінчуючи оперативним виконанням, щоб створити комплексну та ефективну систему [47]. Візуалізація цих етапів на рис. 2.9 може допомогти зрозуміти їх послідовність і взаємозв'язок, сприяючи кращому розумінню та впровадженню СУІБ.

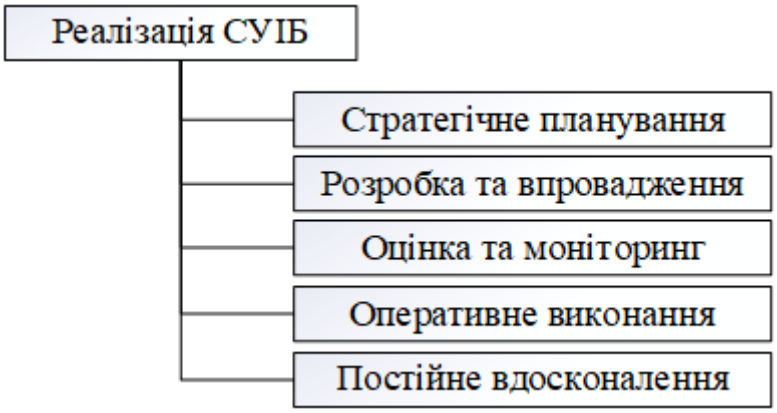

Рис. 2.9. Етапи реалізації СУІБ

Реалізація СУІБ складається із таких етапів:

– стратегічне планування. На цьому етапі встановлюються основні цілі інформаційної безпеки, аналізуються ризики та розробляються стратегії їх мінімізації. Важливо визначити ключові активи та вразливості підприємства;

– розробка та впровадження. Після стратегічного планування необхідно розробити конкретні механізми та процедури управління безпекою. Це включає створення політик безпеки, впровадження технічних засобів захисту та організацію навчання персоналу;

– оцінка та моніторинг. На цьому етапі проводиться оцінка впроваджених заходів безпеки, щоб переконатися у їх ефективності. Регулярний моніторинг та аудит допомагають виявляти нові загрози та вразливості;

– оперативне виконання. Цей етап зосереджений на щоденному застосуванні політик і процедур безпеки. Важливо забезпечити, щоб всі співробітники дотримувалися встановлених правил і стандартів;

– постійне вдосконалення. Останній етап передбачає аналіз результатів та внесення необхідних змін для підвищення ефективності СУІБ. Це включає оновлення політик, покращення процесів та впровадження нових технологій.

Перелічені етапи утворюють циклічний процес, який дозволяє постійно адаптуватися до нових викликів у сфері ІБ, забезпечуючи надійний захист підприємства [48]. У цьому контексті, модель ІБ (рис 2.10) відіграє ключову роль, інтегруючи та систематизуючи різні аспекти захисту інформації.

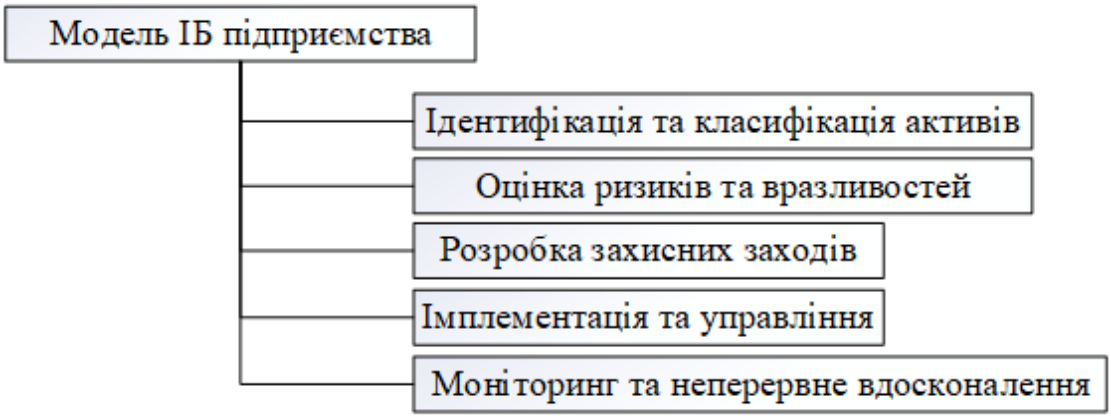

Рис. 2.10. Модель ІБ підприємства

Основними елементами моделі ІБ підприємства є:

– ідентифікація та класифікація активів. Перший крок полягає у визначенні та класифікації інформаційних активів, які потребують захисту. Це включає в себе дані, апаратне та програмне забезпечення, мережеву інфраструктуру та інші важливі ресурси. Класифікація допомагає визначити рівень важливості та чутливості кожного активу;

– оцінка ризиків та вразливостей. Модель передбачає аналіз потенційних ризиків та вразливостей, з якими можуть зіткнутися інформаційні активи. Це включає в себе оцінку ймовірності та потенційного впливу різних загроз, від кібератак до внутрішніх помилок;

– розробка захисних заходів. На основі оцінки ризиків, розробляються захисні заходи для кожного класу активів. Це може включати технічні рішення (як-от шифрування, брандмауери, антивірусне програмне забезпечення), організаційні політики (наприклад, політики доступу, процедури управління інцидентами) та фізичні заходи безпеки;

– імплементація та управління. Впровадження захисних заходів вимагає ефективного управління та координації. Це включає належне адміністрування систем безпеки, регулярне оновлення ПЗ та навчання персоналу;

– моніторинг та неперервне вдосконалення. Важливим аспектом моделі є постійний моніторинг ефективності захисних заходів та регулярне оновлення стратегії безпеки. Це забезпечує, що система безпеки залишається актуальною та ефективною у відповіді на нові виклики та загрози.

За допомогою цієї моделі підприємства можуть створити стратифікований та багаторівневий підхід до інформаційної безпеки, що забезпечує захист на різних рівнях та адаптується до змін у зовнішньому та внутрішньому середовищі.

Ефективна СУІБ є важливим інструментом для захисту інформаційних активів підприємства від різноманітних загроз. Вона забезпечує не лише технічний захист, але й включає організаційні та управлінські аспекти, спрямовані на зниження ризиків та підвищення рівня безпеки [47]. Ефективна

СУІБ вимагає постійного моніторингу, аналізу загроз та гнучкого реагування на змінювані умови.

На рис. 2.11 зображено ключові етапи створення та впровадження СУІБ. Ці етапи включають аналіз потреб, розробку політики безпеки, планування заходів, імплементацію та навчання, моніторинг та оцінку, а також відгуки та вдосконалення. Кожен етап є невід'ємною частиною загальної стратегії безпеки, спрямованої на всебічний захист інформаційних ресурсів підприємства, підкреслюючи комплексний підхід до управління інформаційною безпекою.

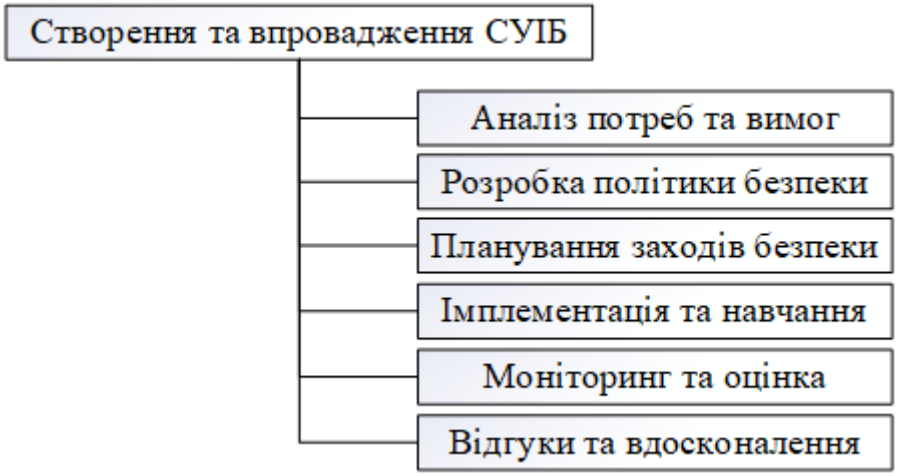

Рис. 2.11. Етапи створення та впровадження СУІБ

Створення та впровадження СУІБ складається із таких етапів:

– аналіз потреб та вимог. Перший крок полягає в оцінці поточного стану інформаційної безпеки та ідентифікації вимог. Це включає аналіз вразливостей, загроз, правових та нормативних вимог, а також бізнес-потреб підприємства;

– розробка політики безпеки. На основі зібраної інформації розробляється політика безпеки, яка визначає загальні принципи, цілі та відповідальності у сфері інформаційної безпеки;

– планування заходів безпеки. Розробка конкретних заходів та контролів для захисту інформаційних активів. Це може включати технічні рішення (шифрування, брандмауери), організаційні заходи (політики доступу, процедури відповіді на інциденти) та фізичні заходи безпеки;

– імплементація та навчання. Впровадження запланованих заходів безпеки, включаючи встановлення та налаштування технічних засобів, реалізацію організаційних процесів та навчання персоналу;

– моніторинг та оцінка. Постійний моніторинг і оцінка ефективності заходів безпеки. Це включає регулярне тестування систем безпеки, аудити та аналіз інцидентів;

– відгуки та вдосконалення. Збір відгуків та аналіз інцидентів для виявлення можливостей для вдосконалення. На цьому етапі також проводиться оновлення політик та процедур у відповідь на нові загрози та виклики.

Кожен з цих етапів є важливим для забезпечення комплексної та ефективної СУІБ, яка може адаптуватися до змінних умов та забезпечити надійний захист від різноманітних інформаційних загроз.

У рамках СУІБ, впровадження механізму управління доступом відіграє критично важливу роль у забезпеченні контролю над доступом до інформаційних ресурсів підприємства. Цей механізм фокусується на забезпеченні того, щоб доступ до інформації отримували виключно уповноважені користувачі, що важливо для запобігання несанкціонованому або неправомірному доступу до цінних і чутливих даних.

Важливим аспектом управління доступом є методологія розмежування доступу, яка базується на принципах найменшого привілею та потреби у знанні [48]. Цей підхід передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їх робочих завдань, тим самим мінімізуючи потенційні ризики. Також важливим є впровадження диференційованих рівнів доступу, що відповідають ролі та обов'язкам кожного співробітника в підприємства. Наприклад, вище керівництво може мати доступ до більш широкого спектру інформації, ніж звичайні працівники.

Окрім того, для ефективного управління доступом важливо розробити чіткі політики і процедури, які регулюють процеси надання, перегляду та відкликання прав доступу [51]. Це допомагає створити прозору та контрольовану

систему управління доступом, що є невід'ємною частиною комплексної стратегії інформаційної безпеки в підприємства.

Впровадження технологій для управління доступом є фундаментальною частиною СУІБ, спрямованої на мінімізацію ризиків, пов'язаних з несанкціонованим доступом. Ці технології включають в себе системи ідентифікації та аутентифікації, які можуть використовувати різноманітні методи, від традиційних паролів до біометричних даних, смарт-карт або спеціальних токенів [52]. Ці системи гарантують, що доступ до інформації та ресурсів отримують лише уповноважені користувачі.

Системи управління доступом ефективно контролюють та відстежують, хто, коли та як використовує ресурси та додатки організації. Це допомагає виявляти нестандартну поведінку та потенційні загрози. Також існують системи для керування цифровими ідентифікаторами, які дозволяють централізовано управляти ідентифікаторами користувачів і їхніми правами доступу. Це сприяє більшій ефективності та прозорості в управлінні доступом.

Ще одним важливим компонентом є шифрування даних, яке захищає конфіденційність та цілісність інформації під час її передачі та зберігання.

Загалом, ефективне впровадження цих технологій у СУІБ дозволяє значно знизити ризики, пов'язані з несанкціонованим доступом, та підвищити рівень безпеки інформаційних систем підприємства.

Розробка ефективної стратегії управління ІБ вимагає глибокого розуміння та аналізу функціональних процесів в організації, визначення порогів ризику та інтеграції цих елементів у загальну стратегію СУІБ.

Глибокий аналіз функціональних процесів передбачає оцінку всіх аспектів роботи організації, які впливають на ІБ. Це включає в себе аналіз поточних систем управління даними, комунікаційних каналів, операційних процесів та робочих потоків. Основна мета полягає у виявленні потенційних вразливостей та загроз, які можуть вплинути на безпеку інформації.

Визначення порогу ризику є критично важливим для розробки стратегії. Це включає в себе оцінку рівня ризику, яке підприємство готове прийняти, та

визначення критеріїв, за якими ризики будуть класифікуватися як прийнятні або неприйнятні. Встановлення чітких порогів допомагає приймати обґрунтовані рішення щодо заходів безпеки та розподілу ресурсів.

Інтеграція цих елементів у загальну стратегію СУІБ полягає в узгодженні ідентифікованих ризиків та процесів з загальними цілями та стратегіями організації у сфері ІБ. Це включає розробку комплексних планів захисту, процедур реагування на інциденти, політик доступу та контролю, а також стратегій забезпечення неперервності бізнесу та відновлення після порушень. Ефективна стратегія управління ІБ повинна бути гнучкою та адаптивною, здатною відповідати на швидкі зміни в технологіях, загрозах та бізнес-умовах. Це вимагає постійного моніторингу, оцінки та вдосконалення процесів управління безпекою, а також залучення та підвищення обізнаності всіх співробітників організації.

2.2.2. Оцінка ефективності процесів розробки та впровадження системи управління інформацією та подіями інформаційної безпеки.

Процеси розробки та впровадження СУІБ охоплюють комплексну діяльність, починаючи з аналізу потреб та визначення вимог, проектування архітектури системи, до її розробки, тестування та зрештою впровадження у робоче середовище. На рис. 2.12 показано процеси розробки та впровадження СУІБ, що дозволяє краще зрозуміти їх послідовність.

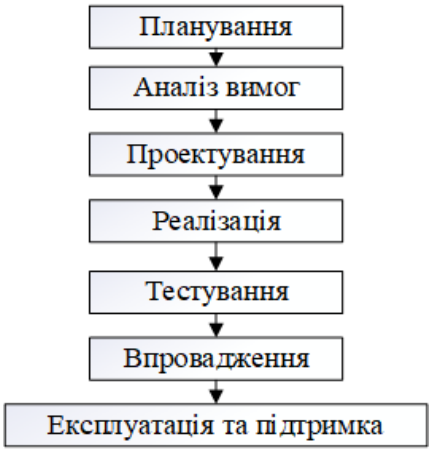

Рис. 2.12. Процеси розробки та впровадження СУІБ

Процеси, які включають в себе створення та впровадження СУІБ, можна розглянути як послідовність дій та діяльності, які ведуть до розробки та запуску системи:

– планування. Визначення мети, обсягу проекту, функціональних та технічних вимог, а також ресурсного планування;

– аналіз вимог. Збір та аналіз вимог користувачів і зацікавлених сторін, документування вимог у специфікаціях;

– проектування. Створення архітектури системи та розробка користувацького інтерфейсу;

– реалізація (Розробка). Кодування компонентів системи та їх інтеграція в єдину систему;

– тестування. Перевірка виконання вимог системи, виявлення та усунення помилок;

– впровадження. Розгортання системи в експлуатацію, виконання перехідних заходів;

– експлуатація та підтримка. Підтримка та обслуговування системи, моніторинг та управління змінами.

Ці процеси разом формують повний цикл створення та впровадження СУІБ, кожен з яких має свої унікальні завдання та вимоги.

Головна мета впровадження СУІБ полягає у створенні оптимальних умов в організації для безперервного моніторингу та удосконалення процесів інформаційної безпеки та пов'язаних з ними процедур [53]. Це включає постійне виявлення і усунення слабких місць, поліпшення внутрішніх процедур та систем, з метою створення ефективнішої та безпечнішої робочої середовища. Одним із способів оцінювання ефективності цих поліпшень є аналіз кількості невідповідностей, які виявляються під час різних форм контролю, включаючи внутрішні аудити та аналіз ефективності процесів. Такий підхід допомагає не лише виявляти слабкі місця, але й систематично працювати над їх усуненням, тим самим постійно підвищуючи рівень інформаційної безпеки в організації.

Після оцінки та поліпшення процесів ОІБ у рамках СУІБ, наступним кроком є перехід до використання метрик, які служать як ключовий інструмент для оцінювання ефективності цих процесів, як у якісному, так і в кількісному аспектах. Метрики допомагають вимірювати успішність процесів, зокрема через аналіз продуктивності, відповідності стандартам, ефективності реакції на інциденти та інші критичні параметри. Важливо не лише обрати відповідні метрики, але й правильно їх застосувати для визначених процесів.

Технічні метрики

Технічні метрики є неабияк важливими для глибокого аналізу ефективності SIEM на підприємстві. Вони відображають реальну здатність системи відповідати на виклики інформаційної безпеки, починаючи від швидкості виявлення інцидентів до забезпечення цілісності даних. Технічні метрики часто є прямими індикаторами ефективності та надійності системи. На рис. 2.13 представлено найбільш важливі технічні метрики, що дозволяють оцінити ефективність використання SIEM на підприємстві.

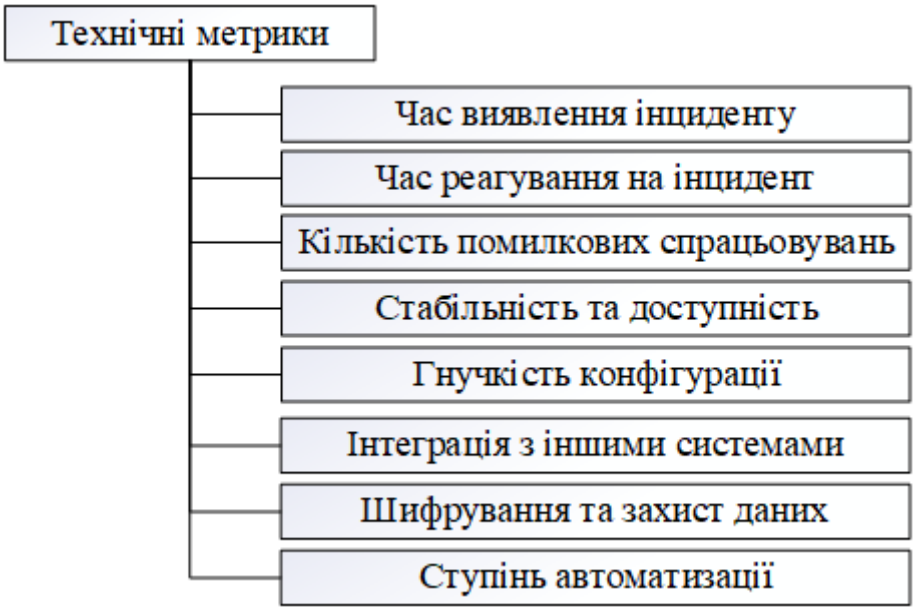

Рис. 2.13. Технічні метрики оцінки ефективності SIEM

До основних технічних метрик оцінки ефективності SIEM належать [54]:

– час виявлення інциденту. Ця метрика вимірює, наскільки швидко система може виявити потенційний інцидент безпеки;

– час реагування на інцидент. Здатність системи швидко реагувати на виявлені інциденти та нейтралізувати їх;

– кількість помилкових спрацьовувань. Важливо знати, наскільки часто система дає помилкові або хибні сповіщення, які можуть спотворювати аналіз безпеки;

– стабільність та доступність. Оцінка того, наскільки стабільно та безперебійно функціонує система;

– гнучкість конфігурації. Можливість легко адаптувати систему до змінних умов та вимог безпеки;

– інтеграція з іншими системами. Здатність системи ефективно інтегруватися з іншими застосунками і системами на підприємстві;

– шифрування та захист даних. Наскільки ефективно система може шифрувати чутливу інформацію та захищати її від несанкціонованого доступу;

– ступінь автоматизації. Здатність системи автоматизувати рутинні процеси, зменшуючи тим самим людський фактор та можливість помилок.

Детальна оцінка технічних метрик дозволяє підприємству не лише оцінити поточний стан системи управління інформацією та подіями, але і прогнозувати її подальшу ефективність. Ці метрики служать ключовими показниками для прийняття управлінських рішень, планування бюджетів та розробки стратегій по підвищенню рівня інформаційної безпеки. Завдяки цьому підприємство може активно адаптуватися до змінюваних умов та викликів, пов'язаних з інформаційною безпекою, та таким чином забезпечувати стабільну та безпечну діяльність.

Організаційні метрики

Організаційні метрики для оцінки ефективності системи управління інформацією та подіями допомагають розуміти, як система взаємодіє з різними відділами підприємства, та її вплив на загальну ефективність діяльності. Організаційні метрики відіграють ключову роль у визначенні ROI (Повернення на інвестиції) та TCO (Загальні витрати на власність) системи [55]. На рис. 2.14 представлено основні аспекти організаційних метрик для оцінки SIEM.

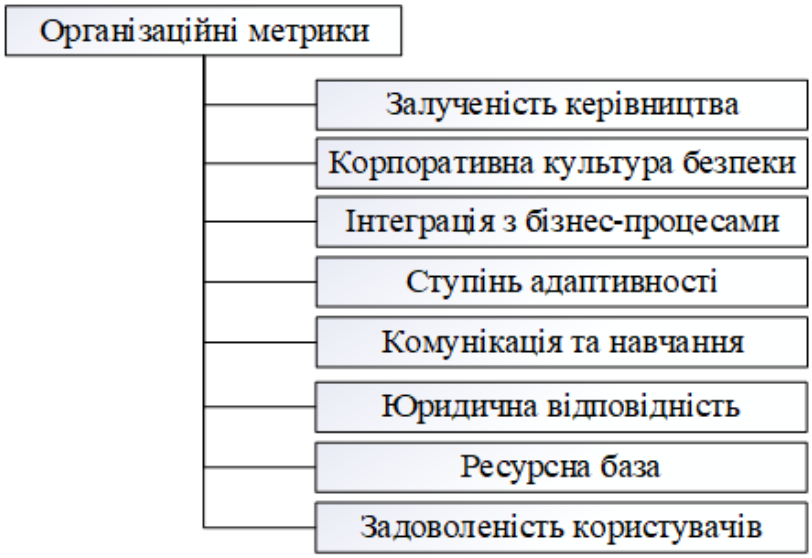

Рис. 2.14. Організаційні метрики оцінки ефективності SIEM

До основних організаційних метрик оцінки ефективності SIEM належать:

– залученість керівництва. Оцінка рівня участі та підтримки з боку верхнього менеджменту в процесі розробки та впровадження системи;

– корпоративна культура безпеки. Рівень освіченості та залученості співробітників у питаннях інформаційної безпеки;

– інтеграція з бізнес-процесами. Міра, в якій система SIEM інтегрована в ключові бізнес-процеси підприємства;

– ступінь адаптивності. Здатність підприємства адаптувати систему до змінних умов та вимог;

– комунікація та навчання. Ефективність комунікації між різними відділами та рівень навчання персоналу для роботи з системою;

– юридична відповідність. Оцінка того, наскільки система відповідає законодавчим та регулятивним вимогам;

– ресурсна база. Наявність необхідних ресурсів (людських, фінансових, технічних) для ефективного функціонування системи;

– задоволеність користувачів. Оцінка того, наскільки користувачі системи задоволені її функціональністю, зручністю та ефективністю.

Організаційні метрики допомагають визначити, які аспекти системи потребують уваги, а також служать важливим індикатором для оцінки ефективності, задоволеності користувачів та відповідності юридичним вимогам.

Для наочності та кращого розуміння впливу цих метрик на різні аспекти системи SIEM, створено табл. 2.5, яка демонструє ці взаємозв'язки.

Таблиця 2.5

Вплив метрик на системи SIEM

Організаційні метрики	Вплив на ефективність системи SIEM	Задоволеність користувачів	Відповідність регулятивним вимогам	Вплив на інші ключові параметри
Залученість керівництва	Високий	Покращує	Підвищує	Підвищує гнучкість
Корпоративна культура безпеки	Середній	Покращує	Покращує	Зміцнює довіру
Інтеграція з бізнес-процесами	Високий	Нейтрально	Забезпечує	Оптимізує процеси
Ступінь адаптивності	Суттєвий	Підвищує	Покращує	Забезпечує гнучкість
Комунікація та навчання	Важливий	Покращує	Важлива	Покращує розуміння
Юридична відповідність	Критичний	Підвищує	Критична	Забезпечує юридичну впевненість
Ресурсна база	Важливий	Нейтрально	Важлива	Забезпечує необхідні ресурси
Задоволеність користувачів	Середній	Критично важлива	Покращує	Покращує загальне сприйняття

Проведення детальної оцінки організаційних метрик є важливою складовою загального процесу оцінки ефективності системи SIEM. Це не тільки дозволяє керівництву підприємства зрозуміти реальну вартість та вплив системи на організацію, але й служить базою для прийняття обґрунтованих управлінських рішень. Організаційні метрики також можуть служити відправним пунктом для подальших удосконалень та оптимізації, враховуючи динамічну природу інформаційної безпеки та бізнес-вимог.

Висновки до другого розділу.У даному розділі було детально розглянуто роль та значення SIEM-систем у сучасних умовах цифрової економіки. Виділено та проаналізовано ключові підсистеми управління інформаційною безпекою, включаючи управління ризиками, інцидентами та забезпечення готовності до безперервної діяльності. Значна увага приділяється процесам ідентифікації, аналізу, оцінки та реагування на різноманітні інформаційні ризики та загрози.

Особливо важливою є частина, присвячена аналізу можливостей сучасних SIEM-систем, зокрема Splunk, IBM QRadar, ArcSight та OSSIM. Для кожної з цих систем надається детальний опис їхніх функціональних можливостей, переваг та обмежень. Таким чином, розділ надає всебічний огляд сучасних підходів та рішень у сфері інформаційної безпеки, особливо в контексті впровадження та використання SIEM-систем.

Окремо виділена частина присвячена організації розробки сучасних систем управління інформацією та подіями інформаційної безпеки, в якій акцентується увага на необхідності інтеграції таких систем із загальною стратегією підприємства, врахування міжнародних стандартів та постійної адаптації до змін умов та загроз.

Отже, розділ детально висвітлює ключові аспекти та методології SIEM-систем, які можуть бути застосовані для аналізу та вдосконалення інформаційної безпеки на прикладі конкретного підприємства. Результати цього розділу надають інструменти та підходи для ефективного управління інформацією та подіями, які можуть бути інтегровані у стратегію інформаційної безпеки, допомагаючи у розробці відповідних рекомендацій.

Розділ 3. ДОСЛІДЖЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ІНФОРМАЦІЄЮ І ПОДІЯМИ (SIEM) ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У цьому розділі досліджується застосування систем управління інформацією та подіями (SIEM) з особливим фокусом на програму Splunk для аналізу процесів у "FinTrust Bank". Мета полягає у виявленні найбільш ефективних стратегій підвищення інформаційної безпеки підприємства. Розділ включає аналітичний огляд існуючих підходів у цій сфері та розробку конкретних рекомендацій, заснованих на отриманих даних. Ці рекомендації спрямовані на досягнення загальної мети роботи - забезпечення надійного захисту інформаційних ресурсів у фінансовому секторі.

3.1 Використання програми Splunk для проведення дослідження

Для проведення дослідження взято підприємство «FinTrust Bank» з урахуванням реалістичних аспектів, які характерні для цієї галузі. «FinTrust Bank» - це великий комерційний банк, який має філії в понад 50 містах, що свідчить про його значний вплив і присутність у фінансовому секторі. Основні послуги, які надає банк, включають проведення різноманітних фінансових транзакцій, кредитування, надання інвестиційних послуг, а також інтернет-банкінг, що відповідає сучасним вимогам цифрової ери. Клієнтська база банку дуже різноманітна, вона включає як індивідуальних споживачів, так і корпоративні облікові записи, що свідчить про широкий спектр банківських продуктів та послуг.

Вибір «FinTrust Bank» для дослідження в контексті систем управління інформацією та подіями є особливо важливим з кількох причин. По-перше, великий розмір банку та його широка географічна присутність означають, що він обробляє величезний обсяг даних, що робить його ідеальним для аналізу великих даних та оцінки ефективності системи SIEM. По-друге, різноманіття послуг, які

надає банк, та його клієнтська база вимагають високого рівня безпеки та конфіденційності, забезпечуючи комплексний підхід до оцінки та вдосконалення механізмів захисту інформації. Крім того, оскільки фінансовий сектор часто стає мішенню для кіберзлочинців, дослідження ефективності SIEM у такому великому та важливому банку дозволить не тільки оцінити поточний стан безпеки, але й виявити потенційні напрямки для покращення.

«FinTrust Bank», як великий гравець у фінансовому секторі, зіштовхується з низкою унікальних викликів та специфічних вимог, що випливають із його діяльності (рис. 3.1).

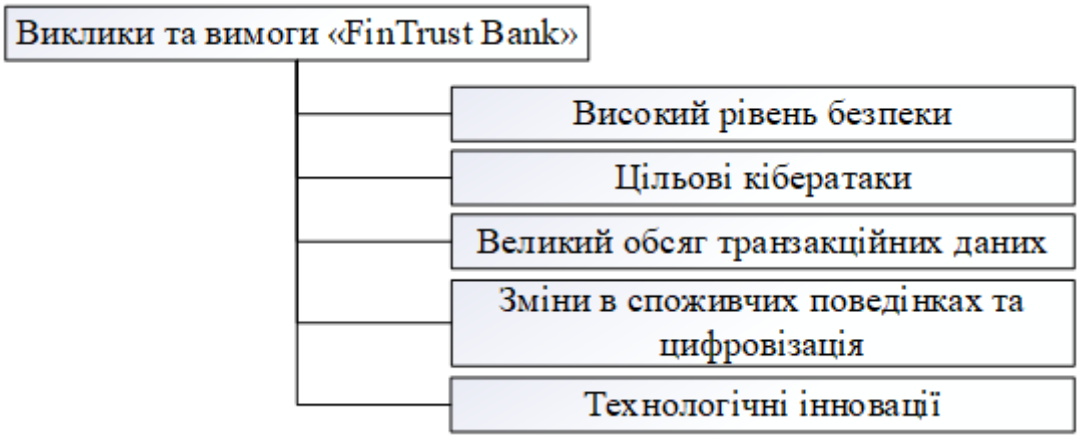

Рис. 3.1. Основні виклики та вимоги «FinTrust Bank»

До основних викликів та вимог підприємства «FinTrust Bank» відносяться:

– високий рівень безпеки. Будучи фінансовою установою, «FinTrust Bank» підпорядковується строгим нормативним вимогам щодо безпеки даних та приватності. Ці вимоги включають в себе дотримання законодавства, такого як GDPR в Європі та інших аналогічних законів у різних країнах. Банк зобов'язаний забезпечувати захист особистих даних клієнтів, фінансових записів та інших конфіденційних інформацій. Для цього необхідно впроваджувати комплексні системи шифрування, двофакторну автентифікацію та інші механізми безпеки. Важливим аспектом також є регулярний моніторинг та оновлення систем безпеки, адже технології та методи кіберзлочинців постійно еволюціонують;

– цільові кібератаки. Банківський сектор часто стає ціллю для кіберзлочинців, оскільки контролює значні фінансові активи та обробляє чутливі дані. Кібератаки можуть включати фішинг, встановлення шкідливого

програмного забезпечення, DDoS-атаки, проникнення в мережу банку та навіть складні APT (Advanced Persistent Threats) кампанії. «FinTrust Bank» повинен мати високоефективну систему виявлення та реагування на інциденти, щоб швидко ідентифікувати та нейтралізувати потенційні загрози. Важливо також проводити регулярні тренінги для співробітників щодо кібербезпеки, адже людський фактор часто є слабкою ланкою в системі безпеки;

– великий обсяг транзакційних даних. «FinTrust Bank» щодня обробляє мільйони транзакцій, що вимагає від банку мати потужну та ефективну систему для моніторингу та аналізу цих даних. Це не тільки включає в себе відстеження звичайних фінансових операцій, але й виявлення шахрайських дій, таких як несанкціоновані транзакції або незвичайні патерни поведінки, які можуть вказувати на спроби шахрайства чи відмивання грошей. Система управління інформацією та подіями, така як Splunk, може забезпечити ефективний збір, аналіз та візуалізацію цих даних, допомагаючи виявляти та відповідати на аномалії в реальному часі;

– зміни в споживчих поведінках та цифровізація .Фінансовий сектор, і зокрема «FinTrust Bank», переживає період значних змін у споживчих поведінках, особливо з розвитком цифрових технологій. Це включає збільшення використання онлайн-банкінгу та мобільних додатків, що ставлять перед банком нові виклики забезпечення безпеки цифрових каналів комунікації. Також це означає необхідність адаптації до змінних вимог клієнтів та надання високоякісних, інтуїтивно зрозумілих цифрових послуг;

– технологічні інновації. Технологічний прогрес, включаючи розвиток штучного інтелекту, блокчейну та машинного навчання, створює нові можливості для фінансового сектору, але одночасно приносить нові виклики. «FinTrust Bank» повинен бути на передньому краї інновацій, інтегруючи ці технології для покращення ефективності, безпеки та якості обслуговування клієнтів. Однак це також вимагає значних інвестицій у вдосконалення IT-інфраструктури та навчання персоналу.

Перелічені виклики та вимоги визначають комплексний підхід, якого вимагає робота в сучасному фінансовому секторі, і підкреслюють значення впровадження ефективної системи SIEM для забезпечення безпеки, відповідності нормативним вимогам, та інноваційного розвитку. «FinTrust Bank», стикаючись із цими викликами, показує не тільки потребу в постійному вдосконаленні систем безпеки, але й у гнучкому підході до впровадження новітніх технологій.

Завдяки цим аспектам, використання системи SIEM у «FinTrust Bank» дозволить не тільки підвищити загальний рівень безпеки, але й оптимізувати процеси моніторингу та аналізу великих обсягів даних, що є критично важливим для ефективного управління ризиками в сучасному фінансовому світі.

«FinTrust Bank», опинившись у вирі сучасних викликів фінансового сектору, визнає важливість впровадження комплексної системи управління інформацією та подіями для забезпечення вищого рівня безпеки та ефективності своїх операцій (рис. 3.2).

Рис. 3.2. Основні потреби використання SIEM для «FinTrust Bank»

Система SIEM дозволить підприємству не тільки виявляти та реагувати на зовнішні загрози, а й забезпечувати комплексний захист від внутрішніх ризиків, зокрема:

– підвищення внутрішньої безпеки. Надійне виявлення та реагування на внутрішні ризики, включаючи помилки співробітників чи випадки внутрішнього шахрайства;

– комплексний погляд на інфраструктуру безпеки. Інтеграція даних з різних систем безпеки для повного огляду стану безпеки організації;

– запобігання витоку даних. Ефективний захист від несанкціонованого доступу та передачі конфіденційної інформації;

– автоматизація відповіді на інциденти. Швидке та автоматизоване реагування на інциденти для мінімізації ризиків;

– аналіз поведінки користувачів. Виявлення аномальної поведінки, яка може вказувати на потенційні внутрішні загрози;

– забезпечення неперервності бізнесу. Мінімізація впливу інцидентів на бізнес-процеси банку;

– розширення звітності. Покращення процесів документування та звітності для відповідності нормативним вимогам та проведення аудитів.

Таким чином, система SIEM стає не просто інструментом безпеки для «FinTrust Bank», а стратегічним активом, що забезпечує комплексний підхід до управління ризиками та оптимізації бізнес-процесів.

Перед встановленням Splunk, спеціалісти «FinTrust Bank» забезпечують наявність відповідної серверної інфраструктури. Для цього було обрано потужні сервери та мережеве обладнання, які відповідають вимогам обробки великих обсягів даних. Після цього було встановлено відповідні мережеві налаштування, щоб забезпечити безпечне та ефективне з'єднання з джерелами даних.

Після цього спеціаліст із команди ІТ створивши профіль на офіційному веб-сайті завантажив необхідне програмне забезпечення Splunk Enterprise. Це забезпечує, що отримується найновіша та найбезпечніша версія програми. Під час завантаження, обрано версію, яка найкраще відповідає операційній системі серверів банку Windows 10. Також на сайті є інструкція для встановлення дистрибутиву на операційну систему.

Після завантаження, наступним кроком є інсталяція програми на сервер. Цей процес розпочинається з запуску інсталяційного файлу, що запускає майстер установки. Слідуючи інструкціям на екрані налаштовуються важливі параметри, такі як директорії для зберігання даних, налаштування мережі та конфігурації

безпеки. Під час установки, спеціаліст вказує певні налаштування для інтеграції з існуючою інфраструктурою банку, зокрема, підключення до баз даних, інтеграція з іншими системами моніторингу та безпеки, тощо.

Після завершення установки програму можна відкрити у браузері та увійти в свій профіль, який був зареєстрований на офіційному сайті програми (рис. 3.3).

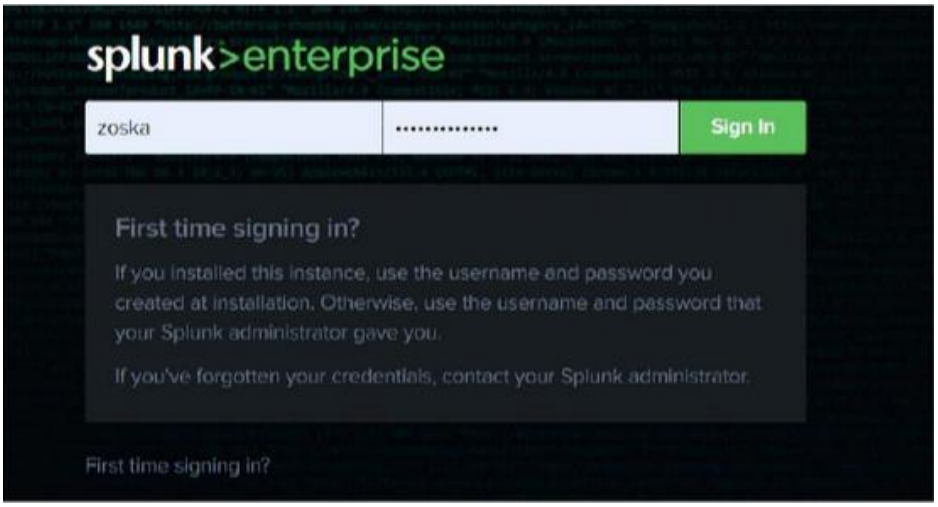

Рис. 3.3. Вхід в програму «Splunk»

Після введення облікових даних відкривається інтерфейс Splunk, який представлено на рис 3.4.

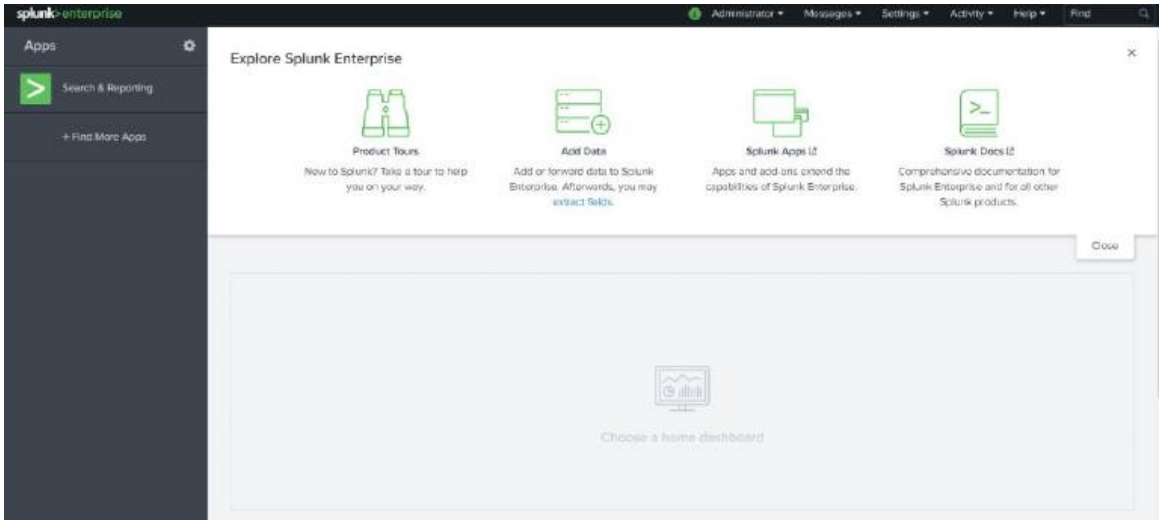

Рис. 3.4. Інтерфейс користувача програми «Splunk»

Після цього спеціаліст провів процес налаштування Splunk для збору та аналізу важливих метрик ефективності SIEM на підприємстві:

– час виявлення інциденту. Спеціаліст налаштував Splunk для автоматичного збору логів з різних систем, таких як файрволи, IDS/IPS, та

сервери. Ці логи включають часові мітки та деталі подій. Використовуючи функції пошуку та кореляції Splunk, визначаються моделі поведінки, які вказують на безпекові інциденти. Час між першим виявленням події та її класифікацією як інциденту фіксується для вимірювання;

– час реагування на інцидент. Встановлена інтеграції Splunk з системою управління інцидентами (ServiceNow). Коли інцидент виявляється, він автоматично реєструється в системі управління інцидентами. Налаштування дашборду для відстеження часу, що пройшов від реєстрації інциденту до його закриття;

– стабільність та доступність. Налаштування Splunk для моніторингу роботи інфраструктури та сервісів через метрики продуктивності та доступності. Налаштування тривог для сповіщення про збої або падіння продуктивності систем;

– гнучкість конфігурації. Створення гнучких дашбордів, які будуть адаптовані під різні аналітичні потреби. Використання можливостей Splunk для налаштування скриптів та автоматизованих завдань, щоб відповідати змінним вимогам підприємства;

– інтеграція з іншими системами. Налаштування Splunk для збору даних з інших систем безпеки, таких як антивіруси, системи керування ідентифікацією. Використання API Splunk для обміну даними з цими системами, забезпечує централізований аналіз;

– шифрування та захист даних. Налаштування Splunk для використання шифрування під час передачі та зберігання даних. Політика безпеки Splunk гарантує захист чутливої інформації та дотримання нормативних вимог;

– ступінь автоматизації. Налаштування автоматизації рутинних завдань в Splunk, таких як звітування, аналіз інцидентів та відповіді на тривоги. Використання можливостей Splunk для створення автоматизованих сценаріїв реагування на типові інциденти.

Проведені налаштування дозволяють спеціалістам «FinTrust Bank» ефективно використовувати Splunk для оцінки ефективності їх SIEM системи, забезпечуючи глибокий аналіз безпеки.

Після 4-ох тижнів роботи програми Splunk було сформовано таблицю метрик ефективності SIEM. Для цього спеціаліст з ІБ підприємства виконав наступні дії:

– налаштування збору даних. Спеціаліст налаштував Splunk для збору логів з мережевих пристроїв, серверів безпеки, і систем управління інцидентами. Це включало налаштування індексації, щоб забезпечити збір комплексної інформації про всі події безпеки;

– створення SPL запитів. Для кожної метрики ефективності SIEM спеціаліст створив специфічні SPL запити. Наприклад, для визначення «Часу виявлення інциденту» він використовував часові мітки з логів для розрахунку середнього часу від реєстрації до виявлення інциденту;

– аналіз часу реагування на інциденти. Спеціаліст аналізував логи систем управління інцидентами в Splunk для визначення швидкості реагування команди безпеки на інциденти;

– моніторинг стабільності та доступності. Використання дашбордів у Splunk для моніторингу часу простою та продуктивності систем, що допомагало оцінити надійність SIEM-системи;

– оцінка гнучкості конфігурації. Збір даних про кількість змін у налаштуваннях системи, які виконувалися без перерв у роботі, для визначення гнучкості системи;

– аналіз інтеграції з іншими системами. Використання даних з логів Splunk для визначення кількості систем, успішно інтегрованих з SIEM;

– перевірка шифрування та захисту даних. Аналіз звітів Splunk на предмет виявлення спроб витоку даних або порушень безпеки, щоб оцінити рівень шифрування та захисту даних;

– оцінка ступеня автоматизації. Аналізування, яка частина процесів моніторингу та реагування на інциденти була автоматизована в Splunk.

Після виконання цих кроків, спеціаліст скомпілював зібрані дані і використав функції експорту Splunk для перенесення цієї інформації у формат, придатний для табличного відображення. Використовуючи ці дані, він сформував табл. 3.1, яка відображає метрики ефективності SIEM за визначені періоди, надаючи команді безпеки чітке уявлення про ефективність їх системи.

Таблиця 3.1

Статистика ефективності SIEM

Метрика	Опис	Тиждень			
		1	2	3	4
Час виявлення інциденту	Середній час між виникненням інциденту та його виявленням	2 год	1.5 год	1.8 год	1.2 год
Час реагування на інцидент	Середній час між виявленням інциденту та реагуванням на нього	30 хв	25 хв	35 хв	20 хв
Кількість помилкових спрацьовувань	Кількість інцидентів, які були класифіковані як помилкові	10	7	5	3
Стабільність системи	Процент часу, коли система була доступна і функціональна	99.9%	99.7%	99.8%	99.95%
Гнучкість конфігурації	Кількість змін у конфігурації системи без перерв у роботі	3	2	4	1
Інтеграція з іншими системами	Кількість зовнішніх систем, інтегрованих з SIEM	5	5	6	6
Шифрування та захист даних	Кількість інцидентів витоку даних	0	1	0	0
Ступінь автоматизації	Відсоток процесів, що автоматизовано	70%	72%	75%	77%

Аналізуючи метрики ефективності SIEM системи FinTrust Bank, зібрані за допомогою Splunk, можна зробити наступні висновки:

– час виявлення інциденту показав суттєве поліпшення протягом аналізованого періоду. Спочатку система витрачала в середньому 2 години на

виявлення інциденту, але до кінця місяця цей час зменшився до 1.2 години. Таке зниження часу може бути результатом ефективнішого використання інструментів Splunk для аналізу та ідентифікації потенційних загроз, а також наслідком удосконалення правил та алгоритмів виявлення. Це свідчить про зростаючу здатність системи швидко реагувати на потенційні загрози безпеці.

– час реагування на інцидент також покращився, хоча і не так стабільно. Спочатку команда безпеки в середньому витрачала 30 хвилин на реагування на інцидент, але з часом цей показник знизився до 20 хвилин. Третій тиждень вирізнявся збільшенням часу реагування, що могло бути викликано особливо складними інцидентами або зовнішніми факторами. Загалом, поліпшення свідчить про зростання ефективності та швидкості роботи команди безпеки;

– зниження кількості помилкових спрацьовувань з 10 до 3 вказує на значне покращення точності системи виявлення інцидентів. Спочатку висока кількість помилкових спрацьовувань могла створювати додаткове навантаження на команду безпеки, але з часом система стала більш точною в розрізненні реальних загроз від нешкідливих подій. Це може бути результатом налаштування фільтрів та удосконалення алгоритмів виявлення в Splunk;

– висока стабільність системи протягом усього місяця з процентом доступності від 99.7% до 99.95% вказує на надійність SIEM системи. Значення понад 99% свідчать про те, що система була постійно доступною та функціональною, забезпечуючи неперервний моніторинг та захист. Незначне коливання доступності може бути пов'язане з рутинними процедурами обслуговування або оновленнями системи;

– час виявлення інциденту показав суттєве поліпшення протягом аналізованого періоду. Спочатку система витрачала в середньому 2 години на виявлення інциденту, але до кінця місяця цей час зменшився до 1.2 години. Таке зниження часу може бути результатом ефективнішого використання інструментів Splunk для аналізу та ідентифікації потенційних загроз, а також

наслідком удосконалення правил та алгоритмів виявлення. Це свідчить про зростаючу здатність системи швидко реагувати на потенційні загрози безпеці;

– час реагування на інцидент також покращився, хоча і не так стабільно. Спочатку команда безпеки в середньому витрачала 30 хвилин на реагування на інцидент, але з часом цей показник знизився до 20 хвилин. Третій тиждень вирізнявся збільшенням часу реагування, що могло бути викликано особливо складними інцидентами або зовнішніми факторами. Загалом, поліпшення свідчить про зростання ефективності та швидкості роботи команди безпеки;

– зниження кількості помилкових спрацьовувань з 10 до 3 вказує на значне покращення точності системи виявлення інцидентів. Спочатку висока кількість помилкових спрацьовувань могла створювати додаткове навантаження на команду безпеки, але з часом система стала більш точною в розрізненні реальних загроз від нешкідливих подій. Це може бути результатом налаштування фільтрів та удосконалення алгоритмів виявлення в Splunk;

– висока стабільність системи протягом усього місяця з процентом доступності від 99.7% до 99.95% вказує на надійність SIEM системи. Значення понад 99% свідчать про те, що система була постійно доступною та функціональною, забезпечуючи неперервний моніторинг та захист. Незначне коливання доступності може бути пов'язане з рутинними процедурами обслуговування або оновленнями системи.

Загалом, зібрані дані свідчать про поступове покращення ефективності SIEM системи в «FinTrust Bank». Покращення в таких ключових областях, як час виявлення інцидентів, швидкість реагування та зниження помилкових спрацьовувань, вказує на зростання ефективності системи управління інформацією та подіями.

3.2 Рекомендації щодо оптимізації управління інформаційною безпекою на підприємстві

Проведений аналіз оцінки поточного стану системи управління ІБ на підприємстві «FinTrust Bank» допоміг визначити, які аспекти SIEM працюють ефективно та в яких областях є потреба у вдосконаленні. На основі цього аналізу, команда визначила декілька областей, де система SIEM працює особливо ефективно та деякі аспекти, що потребують покращення. Зокрема, було ідентифіковано, що час реагування на інциденти, хоча і покращився, все ще має потенціал для скорочення. Також була виявлена потреба у збільшенні гнучкості та масштабованості системи, щоб краще адаптуватися до змінюваних вимог та інтегруватися з іншими системами.

Така оцінка поточного стану SIEM надає цінну інформацію для розробки цілеспрямованих стратегій та рекомендацій щодо подальшої оптимізації управління ІБ підприємства. Вона допомагає виявити ключові сильні сторони системи, а також визначити пріоритетні напрямки для вдосконалення. Для підвищення ефективності управління ІБ на підприємстві «FinTrust Bank», основним пріоритетом має стати розробка рекомендацій щодо оптимізації управління інформаційною безпекою на підприємстві.

Підвищення внутрішньої безпеки

Для підвищення внутрішньої безпеки на підприємстві, важливо визначити цілеспрямовані заходи, які дозволять зміцнити захист внутрішніх мереж та даних. Ключовим є впровадження комплексного підходу, який охоплює різні аспекти безпеки, від ідентифікації користувачів до моніторингу мережевої активності. Ефективне управління ІБ має базуватися на сучасних технологіях та методиках, зокрема, на застосуванні сильного шифрування, регулярному оновленні систем, а також на активному навчанні та підвищенні обізнаності персоналу (рис. 3.5). Це створить надійний бар'єр проти потенційних загроз і в значній мірі зменшить ризики, пов'язані з витоком даних та кібератаками.

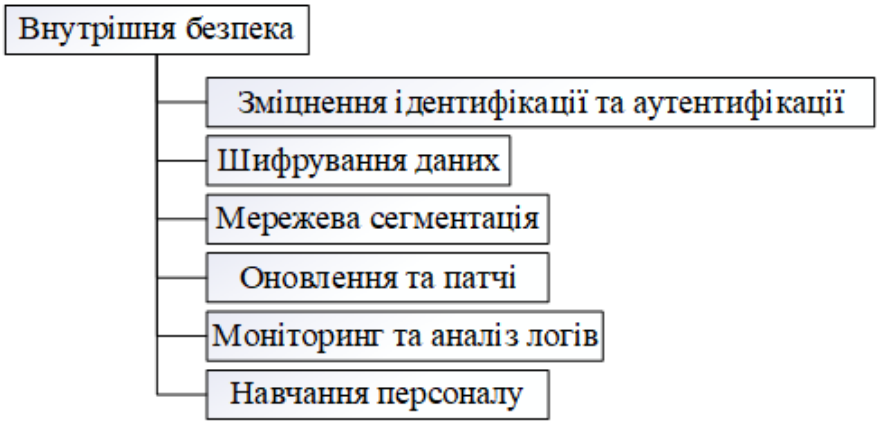

Рис. 3.5. Рекомендації для підвищення внутрішньої безпеки

Рекомендації щодо підвищення внутрішньої безпеки включають:

– зміцнення ідентифікації та аутентифікації. Впровадження багаторівневої аутентифікації, включаючи двофакторну аутентифікацію для всіх користувачів;

– шифрування даних. Застосування сильного шифрування для захисту конфіденційності даних під час передачі та зберігання;

– мережева сегментація. Розділення мереж на сегменти для обмеження доступу та зменшення ризиків поширення загроз;

– оновлення та патчі. Регулярне оновлення всього програмного забезпечення та систем для виправлення вразливостей;

– моніторинг та аналіз логів. Використання систем моніторингу для виявлення нестандартної поведінки або атак;

– навчання персоналу. Проведення тренінгів з підвищення обізнаності персоналу щодо кіберзагроз та безпечних практик.

Отже, для підвищення внутрішньої безпеки підприємства, необхідно зосередитися на зміцненні ідентифікації та аутентифікації користувачів, шифруванні даних, мережевій сегментації, регулярних оновленнях систем, моніторингу та аналізі логів, а також на навчанні персоналу. Ці заходи забезпечать комплексний підхід до захисту внутрішніх мереж і даних, знизять ризики витоку інформації та підвищать загальний рівень безпеки підприємства.

Комплексний погляд на інфраструктуру безпеки

У визначенні комплексного погляду на інфраструктуру безпеки в «FinTrust Bank», ключовим є усвідомлення того, що інформаційна безпека включає багато різноманітних компонентів, які повинні працювати гармонійно, щоб забезпечити ефективний захист. Це вимагає інтеграції та взаємодії між різними системами безпеки, що дозволяє більш точно виявляти та реагувати на загрози. Такий підхід включає: інтеграцію систем виявлення та попередження вторгнень, що забезпечить більш глибокий огляд мережевої активності; уніфікацію контролю доступу, яка допоможе управляти користувацькими правами та доступом до ресурсів; поєднання заходів кібербезпеки з фізичною безпекою, що розширює спектр захисту; та використання розширеного аналітичного ПЗ для аналізу даних безпеки, що дозволить виявляти складні загрози. Все це спрямовано на створення всебічної системи безпеки, здатної адекватно реагувати на зростаючі виклики в сфері інформаційної безпеки.

Запобігання витоку даних

Запобігання витоку даних у «FinTrust Bank» повинні включати заходи для покращення моніторингу даних, впровадження політик DLP, застосування шифрування даних, обмеження доступу до конфіденційної інформації, проведення регулярних аудитів та оцінок вразливостей, а також навчання персоналу щодо питань безпеки (рис. 3.6). Ці рекомендації допоможуть забезпечити комплексний захист від потенційних загроз та зменшити ризики, пов'язані з витоком даних.

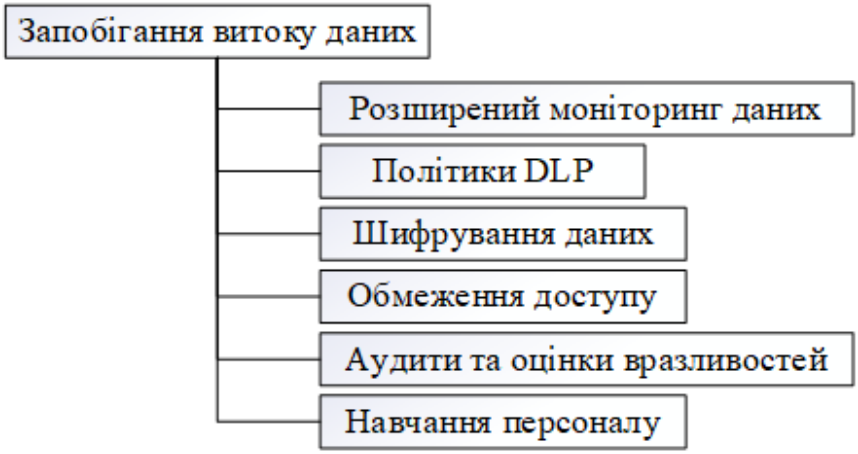

Рис. 3.6. Рекомендації для запобігання витоку даних

На створення ефективної системи захисту інформації та мінімізацію ризиків витоку даних необхідно використовувати наступні методи:

– розширений моніторинг даних. Використання систем для детального відстеження руху даних, щоб виявляти нестандартну активність або потенційні витоки;

– політики DLP (Data Loss Prevention). Встановлення спеціалізованих політик, щоб захистити дані від несанкціонованого використання чи передачі;

– шифрування даних. Використання ефективних методів шифрування для забезпечення конфіденційності даних;

– обмеження доступу. Створення ефективних механізмів контролю доступу для захисту важливих даних;

– аудити та оцінки вразливостей. Проведення перевірок для виявлення та виправлення вразливостей в системах безпеки;

– навчання персоналу. Організація тренінгів з ціллю підвищення обізнаності співробітників щодо ризиків безпеки та захисту даних.

Запропоновані методи є фундаментальними для «FinTrust Bank» у прагненні запобігти витоку даних. Вони сприятимуть створенню міцної системи захисту інформації, забезпечуючи цілісність та конфіденційність корпоративних даних, а також зменшуючи ризик несанкціонованого доступу та інших загроз безпеці інформації.

Автоматизація відповіді на інциденти

Автоматизація відповіді на інциденти в сфері кібербезпеки – це процес, за допомогою якого системи безпеки автоматично виявляють, аналізують та реагують на безпекові порушення або загрози. Цей підхід дозволяє знизити час між виявленням інциденту та його вирішенням, підвищуючи ефективність реагування на загрози та забезпечуючи більш швидке усунення наслідків потенційних атак. Така автоматизація повинна включати в себе розробку системи автоматичного виявлення інцидентів, створення правил та сценаріїв реагування для зменшення людського фактору, інтеграцію з іншими системами безпеки для швидкого обміну інформацією, автоматизацію збору та аналізу

даних, а також регулярне оновлення процесів реагування для відповідності сучасним загрозам (рис. 3.7).

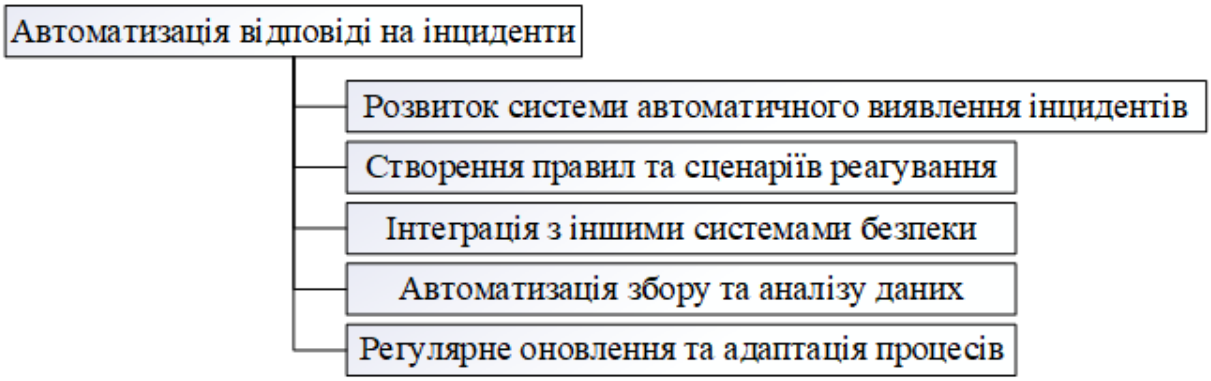

Рис. 3.7. Рекомендації для автоматизації відповіді на інциденти

Для автоматизації відповіді на інциденти в «FinTrust Bank», рекомендується впровадити такі підходи:

– розвиток системи автоматичного виявлення інцидентів. Використання передових технологій для негайного виявлення безпекових порушень;

– створення правил та сценаріїв реагування. Розробка чітких інструкцій для автоматичного реагування на загрози, що мінімізує людський фактор;

– інтеграція з іншими системами безпеки. Забезпечення взаємодії між різними системами безпеки для забезпечення швидкого обміну інформацією;

– автоматизація збору та аналізу даних. Використання інструментів для автоматичного збору даних про інциденти та їх аналізу;

– регулярне оновлення та адаптація процесів. Підтримка актуальності процесів автоматичного реагування для відповідності сучасним викликам безпеки.

Ці кроки дозволять «FinTrust Bank» значно підвищити швидкість та ефективність реагування на інциденти, що є ключовим для забезпечення високого рівня безпеки даних та систем.

Аналіз поведінки користувачів

Аналіз поведінки користувачів — це процес моніторингу та оцінки дій користувачів у мережі або системі з метою виявлення потенційно підозрілої або аномальної активності. Цей аналіз допомагає ідентифікувати незвичну поведінку, яка може вказувати на внутрішні або зовнішні загрози безпеці, такі як витоки даних, шахрайство або кібератаки.

Для поліпшення аналізу поведінки користувачів у «FinTrust Bank», насамперед потрібно зосередитись на впровадженні систем, які дозволяють виявляти аномальну поведінку. Це включає використання спеціалізованих аналітичних інструментів, розробку чітких політик моніторингу, інтеграцію цих систем з іншими інструментами безпеки, а також регулярне оновлення алгоритмів і програмного забезпечення (рис. 3.8). Ці кроки сприятимуть ефективному виявленню та реагуванню на потенційні внутрішні та зовнішні загрози.

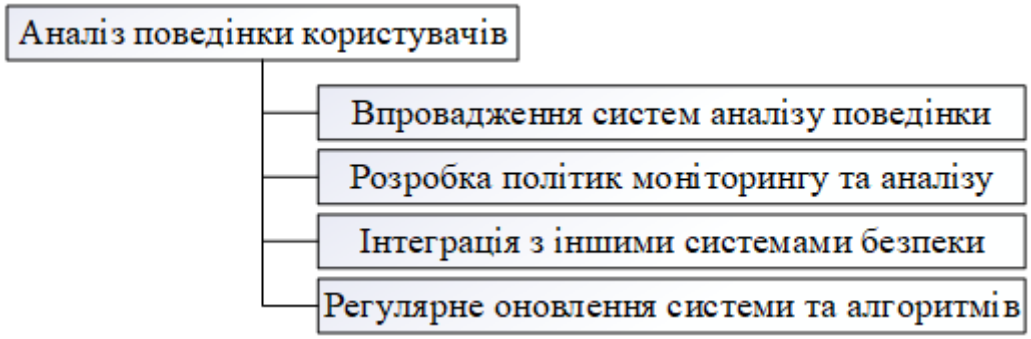

Рис. 3.8. Рекомендації для аналізу поведінки користувачів

Для ефективного аналізу поведінки користувачів в «FinTrust Bank», рекомендується впровадити наступні заходи:

– впровадження систем аналізу поведінки (User Behavior Analytics, UBA). Ці системи дозволять відстежувати та аналізувати активність користувачів, виявляючи аномалії, які можуть вказувати на внутрішні загрози або зовнішні атаки;

– розробка політик моніторингу та аналізу. Встановлення чітких правил щодо моніторингу дій користувачів, забезпечуючи, що це відбувається в рамках правових та етичних норм;

– інтеграція з іншими системами безпеки. Інтеграція UBA-систем з іншими інструментами безпеки для комплексного огляду інформаційної системи та її вразливостей;

– регулярне оновлення системи та алгоритмів. Необхідність постійного оновлення систем і алгоритмів для адаптації до нових типів загроз та змін у поведінці користувачів.

Ці рекомендації сприятимуть виявленню та нейтралізації загроз, пов'язаних з аномальною поведінкою користувачів, забезпечуючи вищий рівень безпеки в банку.

Забезпечення неперервності бізнесу

Для забезпечення неперервності бізнесу в «FinTrust Bank», особливо важливо розробити комплексний підхід, який охоплює кілька ключових елементів. Це включає розробку та впровадження детального плану неперервності бізнесу, встановлення надійних систем резервного копіювання та відновлення даних, регулярне тестування та оновлення цих планів, а також створення системи раннього попередження для виявлення та реагування на загрози (рис. 3.9). Кожен з цих кроків спрямований на мінімізацію можливих перебоїв у роботі банку у випадку надзвичайних ситуацій.

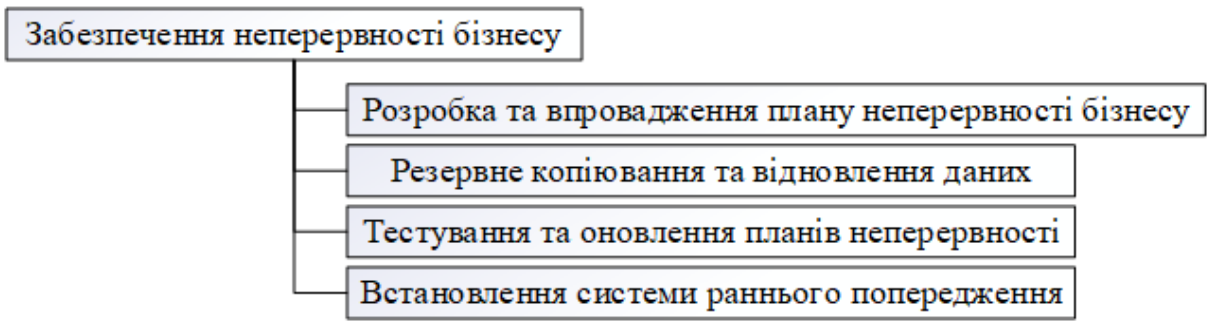

Рис. 3.9. Рекомендації для забезпечення неперервності бізнесу

Для забезпечення неперервності бізнесу в «FinTrust Bank», особливо у випадках інцидентів безпеки, рекомендується впровадити такі кроки:

– розробка та впровадження плану неперервності бізнесу (Business Continuity Plan, BCP). Створення документу, що описує процедури та дії для підтримки критичних бізнес-функцій в умовах різних кризових сценаріїв;

– резервне копіювання та відновлення даних. Встановлення систем регулярного резервного копіювання важливих даних та розробка ефективних механізмів для їх відновлення;

– тестування та оновлення планів неперервності. Проведення регулярних тестів планів неперервності бізнесу для забезпечення їх актуальності та ефективності;

– встановлення системи раннього попередження. Розробка механізмів для раннього виявлення потенційних загроз та своєчасного реагування на них.

Ці заходи допоможуть мінімізувати перебої в роботі «FinTrust Bank» при інцидентах безпеки, забезпечуючи стабільність та ефективність банківської діяльності.

Розширення звітності

Для ефективного розширення звітності в «FinTrust Bank», важливо врахувати кілька ключових аспектів (рис. 3.10). Перш за все, слід вдосконалити інструменти документування для забезпечення точності та ефективності збору даних. Стандартизація процесів звітності допоможе поліпшити якість та зрозумілість звітів. Інтеграція з регулятивними базами даних та регулярне навчання персоналу щодо важливості точного документування забезпечать відповідність всіх процедур нормативним вимогам.

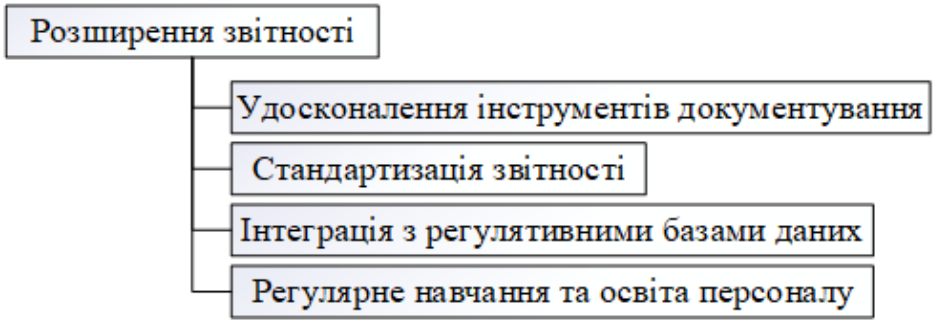

Рис. 3.10. Рекомендації для забезпечення розширення звітності

Для поліпшення процедур документування та звітності в «FinTrust Bank», з метою відповідності регулятивним вимогам, рекомендуються такі кроки:

– удосконалення інструментів документування. Впровадження автоматизованих систем для ефективного збору та обробки даних;

– стандартизація звітності. Розробка єдиних шаблонів і стандартів для звітності, що полегшує процес аналізу та перевірки;

– інтеграція з регулятивними базами даних. Забезпечення постійного оновлення інформації у відповідності до змін у законодавстві та регулятивних вимогах;

– регулярне навчання та освіта персоналу. Проведення тренінгів для співробітників щодо важливості точності та своєчасності документації та звітності.

Ці заходи допоможуть «FinTrust Bank» не тільки підвищити якість та точність звітності, але й гарантувати відповідність діяльності банку регулятивним нормам і стандартам.

Всі ці заходи допоможуть підприємству скоротити час реагування на інциденти та забезпечити більш координоване та ефективне управління загрозами, підвищуючи загальний рівень захисту інформаційних активів банку.

Висновки до третього розділу. У рамках даного розділу, з використанням програми Splunk, було проведено детальний аналіз ефективності SIEM системи в «FinTrust Bank». Отримані дані демонструють значне покращення в таких ключових областях, як час виявлення інцидентів та швидкість реагування, а також зменшення помилкових спрацьовувань. Ці результати вказують на ефективність використання Splunk у забезпеченні глибокого аналізу безпеки та впливають на розробку рекомендацій щодо оптимізації управління інформаційною безпекою, включаючи підвищення внутрішньої безпеки, комплексний погляд на інфраструктуру безпеки, запобігання витоку даних, автоматизацію відповіді на інциденти, аналіз поведінки користувачів, забезпечення неперервності бізнесу та розширення звітності.

ВИСНОВКИ

В ході виконання роботи було проведено всебічне дослідження систем управління інформацією та подіями на прикладі підприємства «FinTrust Bank». Робота спрямовувалася на оцінку ефективності системи управління інцидентами інформаційної безпеки, з використанням програми Splunk для збору та аналізу даних.

Перший розділ був присвячений аналізу нормативно-правової бази України та міжнародних стандартів, що регулюють питання інформаційної безпеки, з акцентом на роль систем управління інформацією та подіями (SIEM). Аналіз включав детальний огляд ключових законів, стандартів та методологій, які формують основу для впровадження та ефективного використання SIEM-систем на підприємствах. Основною метою цього розділу було виявити вимоги до організаційно-технічного забезпечення інформаційної безпеки, методи оцінки ризиків, а також процедури моніторингу та реагування на інциденти інформаційної безпеки. В цьому контексті були розглянуті такі ключові документи, як Закон України «Про інформаційну безпеку», який встановлює правові, організаційні та технічні аспекти забезпечення інформаційної безпеки, а також міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27002, які визначають вимоги до систем управління інформаційною безпекою та найкращі практики для їх впровадження.

Важливим аспектом аналізу було розуміння взаємозв'язку між національним законодавством та міжнародними стандартами. Це дозволило виявити способи, якими українські закони та регуляції співвідносяться та доповнюють міжнародні стандарти, створюючи комплексну основу для забезпечення інформаційної безпеки на підприємствах. Такий підхід сприяє адаптації міжнародних норм до українського контексту та забезпечує ефективне впровадження систем SIEM, відповідно до вимог як місцевого, так і міжнародного законодавства.

У другому розділі було зосереджено увагу на аналізі сучасних підходів до управління інцидентами інформаційної безпеки, з особливим акцентом на використання програми Splunk. Розгляд цього питання включав детальне дослідження різних аспектів і функціональності Splunk як інструмента для моніторингу та аналізу інцидентів безпеки.

Основна увага в розділі була приділена аналізу ключових технічних метрик ефективності систем управління інформацією та подіями, застосовуючи Splunk. Було вивчено ряд важливих параметрів, таких як час виявлення та реагування на інциденти, кількість помилкових спрацьовувань та інші важливі характеристики, які впливають на загальну ефективність SIEM-систем. Цей аналіз допоміг визначити, як Splunk може бути використаний для покращення реагування на інциденти та для підвищення загальної ефективності системи безпеки.

Дослідження включало також оцінку можливостей Splunk для конкретних випадків використання, зокрема, як цей інструмент може допомогти в ідентифікації та аналізі безпекових інцидентів у реальному часі. Було проаналізовано, як специфічні функції Splunk, такі як збір даних, індексація, пошук та візуалізація, можуть використовуватися для виявлення складних загроз та швидкого реагування на них.

Третій розділ був присвячений аналізу процесів управління інцидентами інформаційної безпеки в «FinTrust Bank» за допомогою програми Splunk. Було виявлено значне покращення часу виявлення та реагування на інциденти, а також зменшення кількості хибних спрацьовувань, що підкреслює ефективність використання SIEM систем. Стабільність цієї системи забезпечує надійний моніторинг та захист даних банку. Також було розроблено рекомендації щодо оптимізації управління ІБ, зокрема, підвищення внутрішньої безпеки, комплексний підхід до інфраструктури безпеки, ефективні методи запобігання витоку даних, автоматизацію процесів відповіді на інциденти, детальний аналіз поведінки користувачів, забезпечення безперебійності діяльності банку та розширення звітності. Враховуючи ці аспекти, можна висунути додаткові

пропозиції щодо підвищення ефективності системи управління інцидентами. Наприклад, рекомендується інтеграція різноманітних систем безпеки для створення єдиної, багаторівневої захисної структури. Це також включає в себе розробку спеціалізованих алгоритмів для виявлення незвичайних поведінкових патернів та потенційних загроз, використання новітніх технологій машинного навчання для підвищення точності виявлення інцидентів. Важливо також зосередитись на поліпшенні процедур швидкого реагування, що включає розробку чітких протоколів для різних типів інцидентів, забезпечення адекватної підготовки персоналу, проведення регулярних тренувань і симуляцій для вдосконалення навичок управління інцидентами. Це дозволить не тільки швидко реагувати на виклики, але й прогнозувати потенційні загрози, ефективно запобігаючи їм.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про засади інформаційної безпеки України». URL: https://ips.ligazakon.net/document/JG3TH00A (дата звернення: 23.10.2023).

2. Закон України «Про захист персональних даних» «. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 23.10.2023).

3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» «. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 23.10.2023).

4. Звіт про базове відстеження результативності наказу Адміністрації Держспецзв'язку від 27.10.2020». URL: https://cip.gov.ua/ua/news/zvit-pro-bazove-vidstezhennya-rezultativnosti-nakazu-administraciyi-derzhspeczv-yazku-vid-27-10-2020-687-pro-zatverdzhennya-pereliku-standartiv-ta-tekhnichnikh-specifikacii-dozvolenikh-dlya-realizaciyi-v-zasobakh-kriptografichnogo-zakhistu-informaciyi (дата звернення: 23.10.2023).

5. ISO/IEC 27001:2013 СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ». URL: https://www.ineon.com.ua/poslugi/iso-iec-270012013-sistemi-upravlinnya-informaczijnoyu-bezpekoyu/ (дата звернення: 23.10.2023).

6. Закон № 2657-XII «Про інформацію» «. URL: https://zakononline.com.ua/documents/show/151399___591468 (дата звернення: 23.10.2023).

7. Закон України Про державну таємницю». URL: https://kodeksy.com.ua/pro_derzhavnu_tayemnitsyu.htm (дата звернення: 23.10.2023).

8. Закон України « Про захист персональних даних» «. URL: http://vinfpo.org.ua/index.php?option=com_k2&view=item&id=62:закон-україни-про-захист-персональних-даних&Itemid=14 (дата звернення: 23.10.2023).

9. ПОСТАНОВА від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та

інформаційно-телекомунікаційних системах». URL: https://www.kmu.gov.ua/npas/32791685 (дата звернення: 23.10.2023).

10. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію». URL: https://www.qdpro.com.ua/document/61789 (дата звернення: 23.10.2023).

11. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. – Одеса : ОДУВС, 2018. – 156 с.

12. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків. 2018. 289 с.

13. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації. Дис. … докт. юрид. наук. Харків. 2020. 472 с.

14. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТАН. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/41-1.pdf (дата звернення: 23.10.2023).

15. Управління інцидентами інформаційної безпеки за допомогою SIEM. URL: http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf.

16. SIEM, як один із аспектів забезпечення безперервності бізнесу. URL: https://duikt.edu.ua/uploads/p_2626_12162422.pdf?file=p_2626_12162422.pdf.

17. Глобалізація і сучасний міжнародний процес (2009). За заг ред. Б. Гуменюка, С. Шергіна. К.: Університет “Україна”, С. 42–45.

18. Основні принципи оцінки ризиків. URL: https://qftp.org/wp-content/archive/ukr/1-18-u%20osnovni%20pryncypy%20ocinky%20ryzykiv.pdf (дата звернення: 23.10.2023).

19. Security Information and Event Management (SIEM) . URL: https://www.mdpi.com/1424-8220/21/14/4759 (дата звернення: 23.10.2023).

20. КЕРІВНИЦТВО МАМС №1018 З УПРАВЛІННЯ РИЗИКАМИ. URL: https://hydro.gov.ua/dl/iala/ua/03_1018_MAMS_vol_1.pdf (дата звернення: 23.10.2023).

21. Digital Forensics and Incident Response. URL: https://books.google.com.ua/books?hl=uk&lr=&id=4eZDDwAAQBAJ&oi=fnd&pg=PP1&dq=The+incident+management+process+includes+several+key+steps:+incident+detection,+incident+response,+and+incident+recovery&ots=aPzjrIsqDR&sig=K1KzUNSTFefytq6xL7y6srtPITc&redir_esc=y#v=onepage&q&f=false (дата звернення: 23.10.2023).

22. Янг С., Ярош Л. «Системи управління інцидентами: Практичний підхід». Дніпро: Баланс Бізнес Букс, 2018. - 240 с.

23. Шнайдер Ф. «Інформаційна безпека: Принципи та практика». Львів: Літопис, 2020. - 348 с.

24. Ландау С. «Охорона приватності та безпека в цифрову епоху». Одеса. URL: Астропринт, 2019. - 278 с.

25. A Practical Guide to Assessing Operational Risks. URL: https://hsseworld.com/wp-content/uploads/2021/02/Risk-Assessment-A-Practical-Guide-to-Assessing-Operational-Risks.pdf (дата звернення: 23.10.2023).

26. What Is Information Security (InfoSec)? URL: https://www.hackerone.com/knowledge-center/principles-threats-and-solutions (дата звернення: 23.10.2023).

27. Khoroshko, V. O., Khokhlachova, Yu. Ye. (2016). Information war. Mass media as an instrument of information influence on society. Part 1. Ukrainian Scientific Journal of Information Security, 22(3) . URL: https://doi.org/10.18372/2225-5036.22.11104 (дата звернення: 23.10.2023).

28. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. – К. : НІСД, 2019. – 224 с.

29. Splunk Enterprise Ratings Overview. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendor/splunk/product/splunk-enterprise (дата звернення: 23.10.2023).

30. Defining and measuring the maintainability of Splunk apps. URL: https://theses.liacs.nl/pdf/2020-2021-BrochardMarlo.pdf (дата звернення: 23.10.2023).

31. Splunk Ratings Overview. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendor/splunk (дата звернення: 23.10.2023).

32. Splunk Enterprise Security. URL: https://www.softwarereviews.com/products/splunk-enterprise-security (дата звернення: 23.10.2023).

33. IBM Security QRadar Reviews. URL: https://www.peerspot.com/products/ibm-security-qradar-reviews (дата звернення: 23.10.2023).

34. IBM Qradar architecture. URL: https://www.linkedin.com/pulse/ibm-qradar-architecture-rakesh-patra-3e0xc?trk=public_post_main-feed-card_feed-article-content (дата звернення: 23.10.2023).

35. IBM Security QRadar SIEM. URL: https://www.ibm.com/products/qradar-siem (дата звернення: 23.10.2023).

36. What is QRadar & Its Architecture. URL: https://www.siemxpert.com/blog/what-is-qradar-its-architecture/.

37. IBM QRadar SIEM Deployment (C1000-140) Practice Tests. URL: https://www.udemy.com/course/qradar-certifications-c1000-139140-and-interview-qa/?utm_source=adwords&utm_medium=udemyads&utm_campaign=DSA_Catchall_la.EN_cc.ROW&utm_content=deal4584&utm_term=_._ag_88010211481_._ad_535397282064_._kw__._de_c_._dm__._pl__._ti_dsa-582086350031_._li_1030310_._pd__._&matchtype=&gad_source=1&gclid=CjwKCAiA04arBhAkEiwAuNOsIj3hfr2v-zJ0KfAEoFNZeyr6jBbLeJb14Plftcml2ujOZhKvj6u0vhoCC_UQAvD_BwE (дата звернення: 23.10.2023).

38. ArcSight Enterprise Security Manager (ESM) Reviews. URL: https://www.peerspot.com/products/arcsight-enterprise-security-manager-esm-reviews (дата звернення: 23.10.2023).

39. Global Information Assurance Certification Paper. URL: https://www.giac.org/paper/gcia/1251/distilling-data-sim-strategy-analysis-events-arcsight-esm/102891 (дата звернення: 23.10.2023).

40. ArcSight ESM. URL: https://www.predictiveanalyticstoday.com/arcsight-esm/ (дата звернення: 23.10.2023).

41. ArcSight Reviews. URL: https://www.capterra.com/p/275325/ArcSight/reviews/ (дата звернення: 23.10.2023).

42. Enterprise Security Manager (ESM) . URL: https://www.microfocus.com/marketplace/cybersecurity/content/enterprise-security-manager-esm (дата звернення: 23.10.2023).

43. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ В УПРАВЛІННІ . URL: https://kneu.edu.ua/userfiles/Faculty_of_Information_Systems_and_Technology/kaf%20ise/tezi/17-5315_1_ZbD196rnik_tez_kafedra_D086SE.pdf (дата звернення: 23.10.2023).

44. Гріффітс Дж., Пірс П. «Керівництво з управління ризиками інформаційної безпеки». Львів: Бак, 2018. - 320 с.

45. ISO/IEC 27001:2022. Система управління інформаційною безпекою. URL: https://oleg-dubetcky.medium.com/iso-iec-27001-2022-система-управління-інформаційною-безпекою-db24615a276d (дата звернення: 23.10.2023).

46. Клементс П. «Управління інформаційною безпекою: Підхід на основі ризиків». Одеса: Астропринт, 2017. - 256 с.

47. A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. URL: https://www.researchgate.net/profile/Alix-E-Rojas/publication/362062660_A_Model_of_an_Information_Security_Management_ISOIEC_27001_Standard/links/62d485bcd351bd24f51fa7c5/A-Model-of-an-Information-Security-Management-System-Based-on-NTC-ISO-IEC-27001-Standard.pdf (дата звернення: 23.10.2023).

48. Aligning Enterprise Systems Capabilities with Business Strategy. URL: https://www.sciencedirect.com/science/article/pii/S1877050918317332 (дата звернення: 23.10.2023).

49. Олівер Р. «Управління інформаційною безпекою в організаціях». Дніпро: АртЕк, 2018. - 290 с.

50. Специфіка застосування форм та методів державного управління в сфері інформаційної безпеки: http://mego.info/матеріал/34-специфіка-застосування-форм-та-методів-державного-управління-в-сфері-інформаційної-безпе (дата звернення: 23.10.2023).

51. The Top 5 User Access Review Best Practices. URL: https://www.zluri.com/blog/user-access-review-best-practices/ (дата звернення: 23.10.2023).

52. Secure User Authentication Methods – 2FA, Biometric, and Passwordless Login Explained. URL: https://www.freecodecamp.org/news/user-authentication-methods-explained/ (дата звернення: 23.10.2023).

53. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.

54. What is a SIEM? A Complete Guide. URL: https://securityscorecard.com/blog/what-is-a-siem/#:~:text=After%20correlating%20data%2C%20the%20SIEM,better%20the%20threat%20detection%20is (дата звернення: 23.10.2023).

55. A systematic review of scales for measuring information security culture. URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2019-0140/full/html (дата звернення: 23.10.2023).

56. Якименко Ю.М., Легомінова С.В., Щавінський Ю.В., Рабчун Д.І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навчальний посібник. Київ: Державний університет телекомунікацій, 2023. 241с.

57. Управління інформаційною безпекою: конспект лекцій URL: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С.

О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с. URL: https://ela.kpi.ua/bitstream/123456789/43377/1/Konspekt-Lektsii_UIB.docx (дата звернення: 23.12.2023).

58. ДСТУ ISO/IEC 27001:2015 - (ISO/IEC 27001:2013; Cor 1:2014, IDT) Методи захисту системи управління інформаційною безпекою. Вимоги. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення: 23.12.2023).

59. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911 (дата звернення: 23.12.2023).

60. ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912 (дата звернення: 23.12.2023).

61. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80309 (дата звернення: 23.12.2023).

62. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80310 (дата звернення: 23.12.2023).

63. ДСТУ ISO/IEC 27031:2015 (ISO/IEC 27031:2011, IDT) Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. URL:

https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=81330 (дата звернення: 23.12.2023).