МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ”

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

_____ Юлія МАРТИНОВА

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: Здобувачка вищої освіти гр. УБДМ 61 Юлія МАРТИНОВА

Керівник: к.в.н., доцент Юрій ЯКИМЕНКО

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_____ Світлана ЛЕГОМІНОВА

“____”_____2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Мартиновій Юлії Віталіївні

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Дослідження сучасних методів управління подіями інформаційної безпеки на підприємстві”

керівник кваліфікаційної роботи Юрій ЯКИМЕНКО, к.т.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: *інформаційна безпека підприємства, методи та засоби управління подіями інформаційної безпеки.*

4. Перелік питань, які потрібно розробити:
   1. Розглянути традиційні методи і новітні технологічні рішення управління подіями на підприємстві.
   2. Проаналізувати застосування сучасних методів управління подіями в інформаційній безпеці на підприємстві.
   3. Провести дослідження і сформулювати рекомендації щодо вдосконалення системи управління подіями на підприємстві.
   4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2023	виконано
2.	Збір та аналіз літератури.	03.10.2023	виконано
3.	Огляд сучасних методів управління подіями в інформаційній безпеці на підприємстві	17.10.2023	виконано
4.	Аналіз застосування сучасних методів управління подіями в інформаційній безпеці на підприємстві	31.10.2023	виконано
5.	Дослідження щодо вдосконалення систем управління подіями на підприємстві	14.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	01.12.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	_.01.2024	виконано

Здобувачка вищої освіти _____ Юлія МАРТИНОВА_

(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 здобувачка Мартинова Ю.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Дослідження сучасних методів управління подіями інформаційної безпеки на підприємстві"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка **МАРТИНОВА Юлія** у кваліфікаційній роботі дослідила сучасний стан управління подіями інформаційною безпекою в Україні, визначила основні проблеми та розробила пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності управління подіями інформаційної безпеки організацій (підприємств). **МАРТИНОВА Юлія** показала розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довела уміння самостійного застосування методів наукового дослідження, проявила себе як організована, відповідальна виконавиця. Результати дослідження апробовані на трьох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачці **МАРТИНОВІЙ Юлії** на оцінку "відмінно" та присвоїти їй 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

Кваліфікаційна робота розглянута. Здобувачка **МАРТИНОВА Ю.В.** допускається до захисту даної роботи в Державній екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Мартинової Юлії Віталіївни

на тему “ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ”

Актуальність

На сьогоднішній день у зв’язку з стрімким зростанням кількості і масштабів підприємств, зростають і об'єми інформації, котрі циркулюють в межах інфраструктури підприємства, тож має місце і його інформаційна безпека, якою потрібно управляти. Існує безліч інструментальних засобів і методик для управління інформаційною безпекою на підприємстві, деякі з них мають певні недоліки або застаріли і не відповідають актуальним потребам ведення бізнесу. З огляду на зазначене дослідження сучасних методів управління подіями інформаційної безпеки на підприємстві в умовах безперервного інформаційного протиборства є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено традиційні методи і новітні технологічні рішення управління подіями в інформаційній безпеці і проаналізовано стратегічні напрями впровадження систем управління подіями.

2. Визначено особливості застосування в управлінні подіями - сучасних методів, машинного навчання та штучного інтелекту; розглянуто планування і розгортання системи управління подіями; розроблено імітаційні та навчальні сценарії управління подіями в умовах загроз інформаційній безпеці підприємства; представлено схему управління подіями у мульти-хмарному середовищі

3.За результатами дослідження запропоновано рекомендації на прикладах щодо оптимізації процесів управління подіями для ефективного реагування на події в галузі інформаційної безпеки та забезпечення стійкості бізнес-процесів підприємства.

Недоліки

Доцільно було б приділити більше уваги вивченню і використанню результатів наукових досліджень з управління подіями інформаційної безпеки організацій в Україні. Однак, вищезгадане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувачка Мартинова Юлія Віталіївна заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньопрофесійною 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: 75 стор., 12 рис., 6 табл., 69 джерел.

Метою роботи є вивчення підходів до управління подіями в інформаційній безпеці на підприємстві.

Об'єктом дослідження є управлінські процеси подіями в інформаційній безпеці на підприємстві.

Предмет дослідження – сучасні методи управління подіями в інформаційній безпеці.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі були застосовано методи системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення.

Короткий зміст роботи. У роботі проведено аналіз управління подіями інформаційної безпеки в Україні, визначено основні поняття, принципи, закони та стандарти. Розглянуто актуальний стан, фактори та виклики для ефективного управління подіями ІБ. В заключному розділі висвітлені тенденції, проблеми та надані рекомендації для покращення управління подіями інформаційної безпеки через системи моніторингу та протидії інформаційній та кібербезпеці.

Галузь застосування. Розглянуті сучасні методи управління подіями в інформаційній безпеці, результати досліджденьь по їх застосуванню можуть бути використанні при створенні СУІБ в компаніях середнього та малого сегменту, або відповідно щодо їх покращення та оптимізації роботи підрозділів захисту безпеки.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СТАНДАРТИ.

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 75 pages, 12 figures, 6 tables, 69 sources.

The purpose of the work is to study methods for planning and implementing information security measures at an enterprise.

Object of research is the processes of planning and implementation of information security measures at the enterprise.

Subject of research is approaches to planning and implementation of information security measures at the enterprise.

Research methods To solve the scientific task, the method of system analysis, the theory of information security and the method of comparison and theoretical generalization, analysis and synthesis were used.

Brief content of research. The paper analyzes the management of information security events in Ukraine, defines the basic concepts, principles, laws and standards. The current state, factors and challenges for effective management of information security events are considered. The final section highlights trends, problems and provides recommendations for improving the management of information security events through monitoring and counteraction systems for information and cybersecurity.

Field of research. The considered standards and laws, the developed basic points and the method of building an information security event management system can be used at the initial stage of creating an ISMS in medium and small companies, or, accordingly, to improve the existing state in the context of protecting and optimizing the work of the security department.

KEYWORDS:. ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY THREAT, INFORMATION SECURITY EVENT MANAGEMENT, STANDARDS, LAWS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM	–	система управління інформаційною безпекою та подіями інформаційної безпеки
ISMS	–	систем управління інформаційною безпекою
SEM	–	Security event management (управління подіями безпеки)
CRM	–	системи управління відносинами з клієнтами
СВВ	–	системи виявлення вторгнень
IDS	–	Intrusion Detection System (система виявлення вторгнень)
IPS	–	Intrusion Prevention System (система запобігання вторгненням)
СУП	–	система управління подіями
МН	–	машинне навчання
ШІ	–	штучний інтелект
ІТ	–	інформаційні технології
IoT	–	Internet of Thingsабо (інтернет речей) – система фізичних об’єктів (речей), взаємопов’язаних між собою за допомогою технологій
AWS	–	Amazon Web Services, хмарна обчислювальна платформа та набір послуг, які надаються компанією Amazon

ВСТУП

В сучасному світі, де інформаційні технології набувають все більшого значення, питання забезпечення інформаційної безпеки на підприємствах стає актуальнішим і вимагає системного та комплексного підходу. В умовах постійного зростання обсягу та складності інформації, а також зростання кількості кіберзагроз, управління подіями інформаційної безпеки набуває важливого значення для забезпечення стійкості та надійності діяльності підприємства.

Актуальність теми полягає в тому, що підприємства щоденно стикаються з великим обсягом інформації, оскільки їхні розміри та масштаби стрімко зростають. Наразі існує багато інструментів та методик для забезпечення інформаційної безпеки на підприємстві, але деякі з них застарілі та не відповідають поточним вимогам бізнесу.

Метою роботи є: вивчення підходів до управління подіями в інформаційній безпеці на підприємстві - систематизація та аналіз сучасних методів управління подіями інформаційної безпеки, визначення їх переваг та недоліків, а також розробка рекомендацій щодо оптимізації процесів управління подіями для підвищення рівня захищеності підприємства в інформаційному просторі. Здійснення такого дослідження є актуальним завданням, оскільки дозволяє визначити оптимальні стратегії та інструменти для ефективного реагування на події в галузі інформаційної безпеки та забезпечення стійкості бізнес-процесів підприємства

Об'єкт дослідження – сучасні управлінські процеси подіями в інформаційній безпеці на підприємстві. В контексті швидкого розвитку технологій та сталих загроз кібербезпеки, вивчення та аналіз інноваційних підходів до управління подіями стає критичним завданням для забезпечення ефективності заходів із забезпечення безпеки інформації на підприємстві.

Предмет дослідження – сучасні методи управління подіями в інформаційній безпеці.

Наукова новизна результатів. Результати дослідження можуть бути використні для нового підходу управління подіями інформаційної безпеки та розробки практичних методів покращення роботи підприємств у цій галузі. Викладення результатів цього дослідження сприятиме підвищенню рівня управлінні подіями інформатичної безпеки, забезпечуючи більш ефективний та безпечний цифровий простір для сучасного підприємств.

Галузь застосування. Розглянуті сучасні методи управління подіями в інформаційній безпеці, результати досліджденьь по їх застосуванню можуть бути використанні при створенні СУІБ в компаніях середнього та малого сегменту, або відповідно щодо їх покращення та оптимізації роботи підрозділів захисту безпеки.

РОЗДІЛ 1
ОГЛЯД СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ПОДІЯМИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НА ПІДПРИЄМСТВІ

1.1. Традиційні методи управління подіями

Традиційні методи управління подіями в контексті інформаційної безпеки на підприємстві визначають стратегії та підходи до виявлення, аналізу та вирішення подій, що мають важливе значення для безпеки інформації. Ці методи часто базуються на добре відомих принципах та практиках, але враховують специфіку інформаційного середовища.

Традиційні методи управління подіями включають в себе етапи, які визначають, як події виявляються, обробляються та аналізуються на підприємстві. Ці етапи можуть включати: виявлення подій, збір та реєстрація подій, їх аналіз, відповідь на події, документування та звітність. [1]

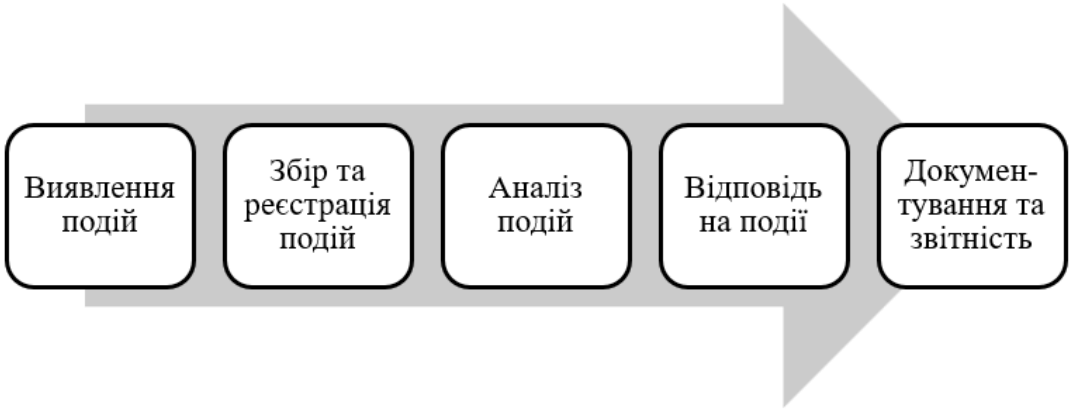

Рис. 1.1. Етапи традиційного управління подіями

У сфері інформаційної безпеки важливим елементом є систематичний підхід до виявлення подій, спрямований на розпізнавання та аналіз інцидентів, які можуть виникнути в інформаційних системах. Традиційні методи виявлення подій відображають накопичений досвід та практику в області забезпечення безпеки інформації. [2]

Процес збору подій відіграє ключову роль у створенні журналів подій, які можуть бути подальшим чином використані для аналізу, виявлення аномалій та реагування на можливі інциденти безпеки. Цей етап включає в себе автоматичне або напівавтоматичне збирання інформації про події, що відбуваються в системі. Він може охоплювати записи системних журналів, мережевий трафік, аудиторську інформацію, та інші дані, які можуть вказувати на діяльність користувачів та стан системи. [3]

На етапі аналізу подій відбувається ретельна обробка зібраних даних. Це динамічний та ітеративний процес, який дозволяє виявляти та реагувати на загрози в реальному часі, покращуючи при цьому загальний рівень безпеки системи. Для фільтрації, кореляції та аналізу величезної кількості даних використовуються передові інструменти, зокрема системи управління інформацією та подіями безпеки (SIEM). Такі методи, як розпізнавання образів, виявлення аномалій і статистичний аналіз, використовуються для виявлення ознак компрометації. [4]

Процес реагування на інциденти описує, як реагувати на конкретні подіїї, щоб забезпечити ефективне та результативне рішення проблеми. [5] Процес реагування на інциденти спрямований на якнайшвидше усунення інцидентів, а також на збір необхідної інформації для відновлення функцій підприємства, а також для покращення, виявлення та запобігання повторення інцидентів. [6]

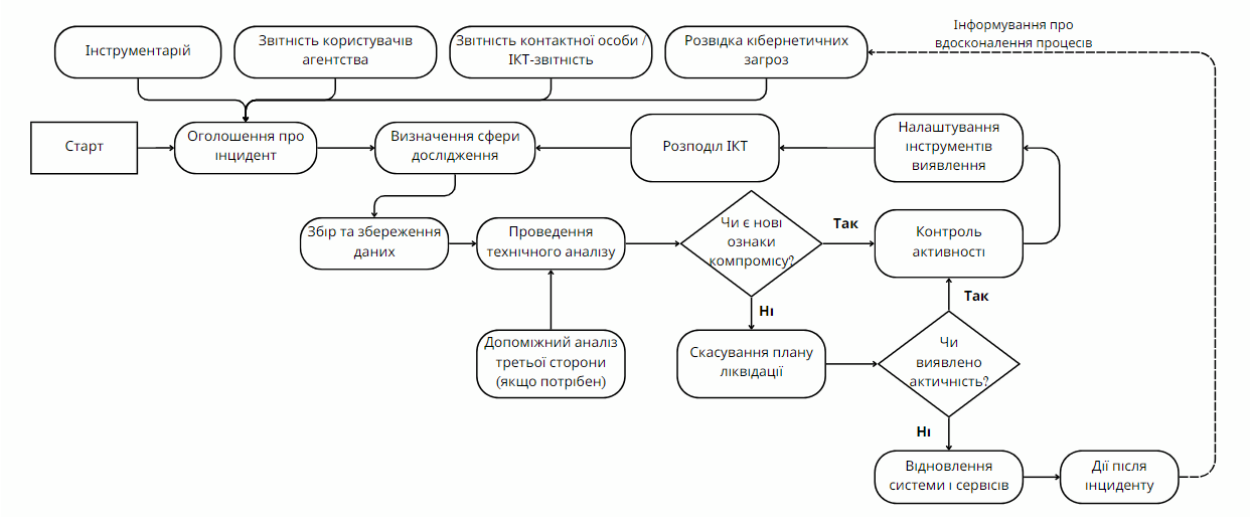

Рис. 1.2. Процес відповіді на події

Традиційні методи можуть стикатися з викликами, такими як обмеження у

швидкості реагування та адаптації до нових видів загроз. Проте, вони мають свої переваги, такі як стабільність та передбачуваність управління подіями. [7]

У світлі швидкозмінюваного середовища інформаційної безпеки, підприємства можуть також розглядати сучасні методи управління подіями, які використовують нові технології, такі як штучний інтелект, машинне навчання та автоматизовані системи аналізу подій для підвищення ефективності та точності управління безпекою інформації. [8]

Однією з важливих аспектів управління подіями є також врахування специфічних вимог та контексту сучасного цифрового середовища. До новітніх викликів входить поява розподілених систем, великого обсягу даних (Big Data), мобільних технологій та інших аспектів, які можуть впливати на управління подіями в інформаційній безпеці. [9]

1.2. Новітні технологічні рішення управління подіями

В сучасному цифровому середовищі постійно зростає кількість та складність кіберзагроз, тому для ефективного управління подіями в інформаційній безпеці на підприємстві необхідно використовувати новітні технологічні рішення. Вони спрямовані на забезпечення високого рівня безпеки в інформаційних системах організацій, швидке реагування на події і постійне оновлення даних для прийнятних результатів процесів управління подіями.

Важливим етапом у використанні рішень управління подіями є їх налаштування. Налаштування рішень варіюється в залежності від конкретних потреб та характеристик організації, але всі вони базуються на міжнародних стандартах. Серед них важливими є серія стандартів ISO/IEC 27000, NIST 800-61 та PCI DSS.

Серія стандартів ISO/IEC 27000, які стосуються систем управління інформаційною безпекою (ISMS), зазнали різних переглядів та оновлень протягом

років. Стандарт ISO/IEC 27000 надає огляд серії та містить терміни та визначення. Він періодично оновлювався, щоб узгодитися зі змінами в інших стандартах серії та змінами в ландшафті інформаційної безпеки. [10]

Стандарт ISO 27001 визнаний стандарт по всьому світу. Він є важливим для організацій, які прагнуть забезпечити високий рівень безпеки своїх інформаційних активів, і є ключовим інструментом у сучасному бізнесі та технологічному ландшафті. Стандарт був вперше опублікований у 2005 році, зосередившись на створенні, впровадженні, експлуатації, моніторингу, перегляді, підтримці та вдосконаленні ISMS. З першим переглядом у 2013 році була змінена структура стандарту, що значно полегшило його використання. Також було покладено більший акцент на вимірювання та оцінку ефективності ISMS організації. Найсвіжіше оновлення було зроблене у 2022 році для того, щоб стандарт відповідав сучасним загрозам безпеки. Воно переглянуло та оптимізувало деякі контролі та зробило стандарт більш адаптивним до різноманітних організацій та контекстів.[11]

Стандарт ISO 27001 широко використовується в багатьох сферах: урядові установи застосовують цей стандарт для захисту чутливої інформації, великі та малі компанії використовують його для забезпечення безпеки своїх інформаційних активів, а різні IT-компанії для захисту всього обсягу даних, з якими вони працюють. [12]

До задач стандарту ISO 27001 входять визначення політики безпеки, оцінка ризиків, заходи захисту та постійний моніторинг і перегляд. Компанії, що звертаються до цього стандарту, впевнені, що політики інформаційної безпеки будуть чітко сформовані, а заходи для управління ризиками будуть розроблені і впроваджені в найефективніший спосіб. [13]

NIST 800-61 є стандартом, розробленим Національним інститутом стандартів та технологій (NIST) Сполучених Штатів, який описує рекомендації та кращі практики для реагування на інциденти комп'ютерної безпеки. Цей документ надає детальні вказівки щодо формування політики реагування на інциденти, а також процесів виявлення, аналізу, пріоритетизації та відповіді на інциденти безпеки. [14]

Основними задачами NIST 800-61 є надання організаціям напрямів для підготовки до, реагування на та відновлення після інцидентів безпеки. Він забезпечує організації інформацією про те, як ідентифікувати та класифікувати інциденти безпеки, розробляти план дій для ефективного реагування та відновлення, а також як здійснювати післядійні дії для запобігання подібним інцидентам у майбутньому.

Цей стандарт широко використовується урядовими установами, корпораціями та іншими організаціями у Сполучених Штатах та по всьому світу, особливо тими, які шукають надійних напрямів у сфері кібербезпеки. Він є важливим ресурсом для фахівців із кібербезпеки та IT-менеджерів, які відповідають за управління інцидентами та забезпечення безпеки інформаційних систем в їх організаціях. [15]

PCI DSS (Payment Card Industry Data Security Standard) є набором стандартів безпеки, розробленим для захисту інформації про кредитні картки і транзакції. Цей стандарт встановлює вимоги до безпеки для всіх організацій, які зберігають, обробляють або передають дані кредитних карток. Ці вимоги включають забезпечення безпечної мережевої інфраструктури, захист даних власників карток, впровадження сильних контрольних механізмів доступу, регулярний моніторинг і тестування мереж, а також підтримку інформаційної політики безпеки. [16]

Головна задача PCI DSS - це зниження ризиків шахрайства з кредитними картками та захист інформації про платіжні картки від несанкціонованого доступу. Цей стандарт вимагає, щоб компанії вживали заходів для захисту даних платіжних карток на всіх етапах обробки транзакцій, від збору і передачі інформації до її зберігання.

PCI DSS використовується у всій індустрії платіжних карток і є обов'язковим для всіх організацій, які займаються обробкою, передачею або зберіганням даних платіжних карток. Це стосується різноманітних учасників ринку - від невеликих інтернет-магазинів до великих банків та фінансових установ. Дотримання PCI DSS допомагає не тільки у забезпеченні безпеки платіжних даних, але й у підвищенні довіри клієнтів та зменшенні ризиків для бізнесу. [17]

Сучасне середовище управління подіями в інформаційній безпеці на підприємстві включає в себе використання передових технологій для ефективного виявлення, аналізу та реагування на події. Новітні технологічні рішення спрямовані на автоматизацію та підвищення швидкості реакції на загрози, а також на підвищення точності в оцінці та відповіді на події. До новітніх технологій можна віднести Автоматизовані системи аналізу подій (SIEM), Виявлення кінцевої точки та відповідь (EDR) та Розширене виявлення та реагування (XDR), а також оркестрація, автоматизація й реагування (SOAR) системи безпеки.

Рис. 1.3. Новітні технології управління подіями безпеки

Автоматизовані системи аналізу подій (SIEM) — це комплексні рішення для збору, агрегації, аналізу та візуалізації подій, що виникають в інформаційних системах та мережах компаній чи організацій. Основна мета SIEM — це забезпечення централізованого моніторингу та управління інформаційною безпекою, а також виявлення та відповідь на інциденти забезпечення безпеки. [18]

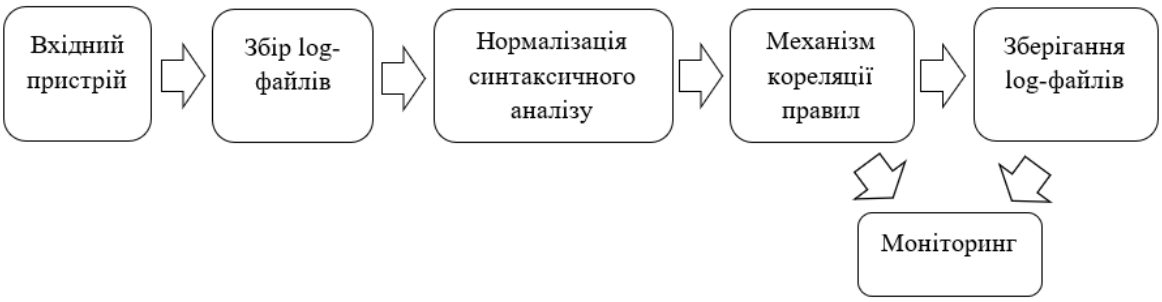

Рис. 1.4. Базові компоненти SIEM

SIEM-система повинна вирішувати комплекс задач, що зображено на рисунку 1.4.

Рис. 1.5. Комплекс задач SIEM-системи

Для вирішення даних задач, SIEM-система, на підставі зібраних з журналів (log-файлів) початкових даних, які накопичують інформацію про події, що відбуваються в системі, відбирає такі, що можуть бути ознаками кібератак або інших небажаних дій в системі. [19]

Головні переваги включають підвищення рівня безпеки, шляхом раннього виявлення та реагування на інциденти, зменшення часу відновлення після інцидентів, покращення виявлення аномалій та підозрілих активностей, а також спрощення управління безпековими подіями через централізовану платформу.

SIEM допомагає підняти ефективність кіберзахисту та забезпечити високий рівень безпеки інформаційних ресурсів організації. [20]

EDR (Endpoint Detection and Response) та XDR (eXtended Detection and Response) є технологіями кібербезпеки, призначеними для виявлення, розслідування та реагування на підозрілу активність та потенційні загрози в мережах комп'ютерів. EDR зосереджений на кінцевих точках, як-от комп'ютерах і мобільних пристроях, і дозволяє організаціям ефективно відстежувати та аналізувати загрози на цих пристроях, забезпечуючи можливість швидкого реагування на інциденти безпеки.[21]

XDR розширює цей підхід, інтегруючи дані з різних джерел, таких як мережі, хмарні сервіси, електронна пошта та інші технології безпеки, для створення більш цілісної картини загроз. Це дозволяє компаніям не лише виявляти та реагувати на інциденти в реальному часі, а й проводити більш глибокий аналіз та прогнозування загроз, що можуть вплинути на всю IT-інфраструктуру. [22]

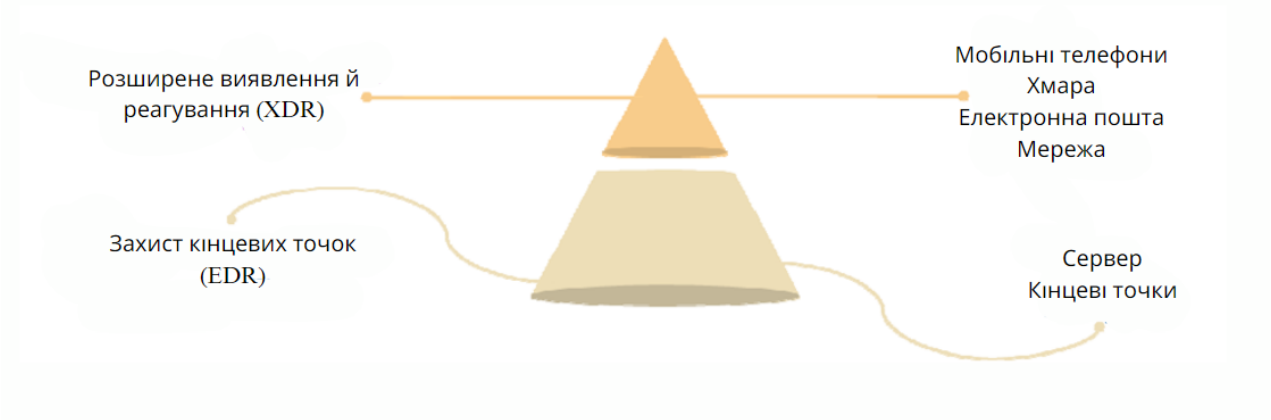

Рис. 1.6. Схема усунення обмежень XDR і EDR

Обидва ці підходи є ключовими для сучасних стратегій кібербезпеки, оскільки вони допомагають організаціям швидко виявляти, ізолювати та реагувати на складні кібератаки, зменшуючи час між компрометацією та виявленням загроз, а також мінімізуючи потенційні збитки. EDR та XDR стають все більш популярними в індустрії, оскільки вони забезпечують більш глибоке розуміння безпеки та ефективніші способи захисту від різноманітних та постійно еволюціонуючих кіберзагроз.

SOAR (Security Orchestration, Automation and Response) – це комплексний

підхід у сфері кібербезпеки, який об'єднує автоматизацію та оркестрацію безпеки з відповідними механізмами для реагування на інциденти. Цей підхід дозволяє компаніям ефективніше і швидше реагувати на інциденти безпеки, інтегруючи різні інструменти безпеки і автоматизуючи рутинні задачі, що допомагає знизити навантаження на команди безпеки. SOAR включає в себе функції, такі як збір даних про загрози з різних джерел, автоматизація процесів аналізу та реагування на загрози, а також координація різних інструментів і систем безпеки.

Завдяки SOAR організації можуть швидко виявляти, аналізувати та реагувати на загрози, мінімізуючи час від моменту виявлення до моменту відповіді. Це особливо важливо в сучасному світі кіберзагроз, де швидкість і ефективність реагування можуть значно зменшити потенційний збиток від інцидентів безпеки. SOAR також покращує співпрацю і комунікацію між командами безпеки, дозволяючи їм більш ефективно управляти інцидентами та забезпечувати більш високий рівень захисту для організації. [23]

Об'єднання SOAR, EDR та SIEM може значно покращити безпеку та можливості виявлення та реагування на загрози в інформаційних системах та мережах. В результаті поєдання цих засобів організація отримує ефективні наслідки, як, наприклад, підвищення ефективності виявлення загроз, зменшення часу реагування, зменшення навантаження на персонал, збільшення здатності до відстеження та аналізу інцидентів та забезпечення більшої гнучкості та адаптивності.

EDR у цій об’єднаній схемі буде забезпечувати детальний моніторинг та аналіз активності на кінцевих пристроях, дозволяючи вчасно виявляти аномальні або зловмисні дії, SOAR може автоматизувати багато задач, що раніше виконувались аналітиками безпеки, звільняючи їх від монотонних рутинних операці, а SIEM надати централізований репозиторій подій та логів, який можна використовувати для розслідування інцидентів та аналізу їхніх наслідків. [24]

Ця інтеграція допомагає підвищити ефективність боротьби зі загрозами та реагувати на нові загрози та вразливості швидше і ефективніше. Таким чином, об'єднання SOAR, EDR і SIEM є важливими інструментами для сучасних

організацій, що прагнуть забезпечити високий рівень кібербезпеки

1.3. Стратегічні аспекти впровадження систем управління подіями

Впровадження систем управління подіями є важливим етапом для підвищення ефективності та оперативності управління різними бізнес-процесами. Одним із ключових аспектів є адаптація до специфічних потреб та контексту організації. Важливо визначити, як SIEM-система взаємодіятиме з існуючими інформаційними технологіями та бізнес-процесами, враховуючи специфіку діяльності.

Стратегічний аспект також включає в себе визначення конкретних цілей впровадження SIEM. Це може включати підвищення рівня безпеки, зменшення часу реагування на інциденти, вдосконалення виявлення загроз та забезпечення відповідності регуляторним вимогам.

Здійснення стратегічного впровадження SIEM також передбачає розроблення чіткої комунікаційної стратегії. Комунікація з ключовими зацікавленими сторонами в організації, включаючи топ-менеджмент, технічний персонал та користувачів, є важливою для успішного прийняття та використання системи.

Крім того, ефективне впровадження SIEM вимагає навчання та підтримки персоналу, що взаємодіє з системою. Належна підготовка персоналу забезпечить оптимальне використання можливостей SIEM та ефективне управління подіями на всіх рівнях організації.

Загалом, стратегічне впровадження SIEM є комплексним завданням, яке включає адаптацію, визначення цілей, ефективну комунікацію та забезпечення готовності персоналу. Такий підхід допомагає максимально використовувати потенціал SIEM для забезпечення безпеки та ефективного управління інформаційними ресурсами організації. [25]

Аналіз бізнес-процесів - це систематичне вивчення та оцінка функцій, дій та взаємодій у межах організації з метою виявлення недоліків, визначення можливостей оптимізації та досягнення покращень в роботі. Цей процес дозволяє розкрити потенціал для підвищення ефективності, зменшення витрат та покращення якості продукції чи надання послуг. Аналіз бізнес-процесів включає в себе визначення ключових етапів та взаємодії між ними, моделювання, виявлення проблем, призначення пріоритетів для оптимізації та впровадження покращень, спрямованих на досягнення стратегічних цілей компанії.

Аналіз бізнес-процесів також включає в себе ретельне вивчення внутрішніх та зовнішніх факторів, які впливають на виконання організаційних завдань. Цей процес допомагає розкрити структурні, організаційні та технологічні аспекти бізнес-процесів, а також їхню взаємодію з клієнтами, постачальниками та іншими зацікавленими сторонами.[26]

При аналізі бізнес-процесів може також вивчатися відповідність організаційних стандартів, регуляторних вимог та законодавчих норм. Зокрема, у зв'язку зі зростанням важливості цифрової безпеки, аналіз бізнес-процесів може включати елементи визначення ризиків і заходів забезпечення безпеки для захисту конфіденційності та цілісності даних.

Крім того, важливо розглядати аналіз бізнес-процесів як інструмент для створення та підтримки корпоративної культури, спрямованої на постійне вдосконалення і тісну співпрацю всіх рівнів організації. Аналітики та дані, зібрані під час аналізу, можуть служити основою для прийняття обґрунтованих стратегічних рішень та розвитку інновацій у компанії. [27]

Процес аналізу бізнес-процесів складається з трьох етапів:

1. **Аналіз елементарних процесів**. Результатом цього етапу є перелік елементарних бізнес-процесів в організації, їх структура та взаємозв'язки. Основним методом, що використовується на цьому етапі, є аналіз подій і реакцій на них.

2. **Специфікація ключових процесів**. Результатом цього етапу є перелік ключових бізнес-процесів в організації, їх структура, взаємозв'язки та ключові

атрибути. Основною технікою, що використовується на цьому етапі, є об'єктний аналіз продуктів організації. Результат попереднього етапу - елементарні бізнес-процеси - використовуються тут як елементи ключових процесів.

3. **Специфікація підтримуючих процесів**. Результатом цього етапу є перелік підтримуючих бізнес-процесів організації, їх структура, взаємозв'язки та ключові атрибути. Основною технікою, що використовується на цьому етапі, є об'єктний аналіз організації. Аналіз підтримуючих бізнес-процесів базується на результатах попередніх етапів - детально описаних ключових бізнес-процесів організації. [28]

Визначення мети і обсягу системи у впровадженні систем управління подіями є ключовим етапом, спрямованим на чітке визначення цілей та меж, які організація прагне досягти за допомогою впровадження цієї системи. Це процес допомагає зорієнтувати увагу на стратегічні завдання та оптимальний спосіб використання ресурсів для досягнення визначених результатів. Визначення мети і обсягу створює фреймворк для ефективного планування, розробки та впровадження системи управління подіями, забезпечуючи спрямованість на конкретні вигоди та стратегічні переваги для організації.

Для досягнення визначеної мети і обсягу в системі управління подіями можемо виділити конкретні стратегії, які охоплюють аналіз бізнес-процесів, визначення ключових подій, вибір відповідної технології, розробку стратегії впровадження та постійне вдосконалення. Важливо акцентувати увагу на практичних перевагах для бізнесу, вирішенні конкретних викликів та забезпеченні адаптованості системи до стратегічних потреб організації. [29]

Вибір відповідної технології при впровадженні систем управління подіями є ключовим етапом, оскільки від цього рішення залежить ефективність та продуктивність управління подіями в організації. Вибір правильної технології дозволяє забезпечити високий рівень автоматизації, швидкість реакції на події, інтеграцію з іншими системами, а також забезпечити безпеку та стабільність функціонування. Правильно вибрана технологія сприяє ефективному вирішенню викликів та завдань, пов'язаних із збором, обробкою та аналізом подій, що

відбуваються в організації. В результаті, цей етап впливає на загальну ефективність та конкурентоспроможність організації в умовах швидко змінюючогося бізнес-середовища. [30]

Розробка стратегії впровадження системи управління подіями є ключовим етапом, оскільки це визначає напрямок і план дій для ефективного і успішного впровадження. Правильно розроблена стратегія враховує усі аспекти бізнес-процесів, визначає етапи впровадження, призначає відповідальних за реалізацію, а також передбачає механізми контролю та оцінки результатів. Це забезпечує системний та організований підхід до впровадження, дозволяючи уникнути потенційних проблем та максимізувати користь від використання системи управління подіями.

Ефективна стратегія допомагає підготувати персонал, забезпечити безперебійність діяльності та відповідність стратегічним цілям компанії. Такий підхід визначає успіх впровадження систем управління подіями та їхню здатність відповідати потребам та викликам сучасного бізнесу. [31]

Захист даних під час впровадження систем управління подіями є ключовим аспектом з точки зору конфіденційності, цілісності та доступності інформації. Забезпечення надійного захисту даних від несанкціонованого доступу, втрати чи порушення конфіденційності є критичним для забезпечення довіри користувачів, виконання вимог законодавства і запобігання можливим фінансовим та репутаційним втратам для організації. Персональна та конфіденційна інформація, що обробляється системою управління подіями, вимагає ефективних заходів з шифрування, автентифікації, контролю доступу та моніторингу безпеки. Підвищення кількості кіберзагроз та важливість дотримання стандартів безпеки підкреслює необхідність інвестування в захист даних для збереження довіри від клієнтів, партнерів та інших зацікавлених сторін. [32]

Відповідність стандартам та законодавству є ключовим етапом при впровадженні систем управління подіями (SIEM) з приводу кількох важливих причин.

По-перше, відповідність стандартам і законодавству забезпечує виконання

організацією всіх необхідних норм та вимог, які стосуються зберігання, обробки та передачі інформації. Це має важливе значення в контексті забезпечення конфіденційності, цілісності та доступності даних.

По-друге, відповідність є заходом для мінімізації ризиків щодо порушень законодавчих вимог, що може призвести до правових наслідків та фінансових санкцій. Законодавство, таке як Закон про захист персональних даних, може встановлювати строгі вимоги до обробки та зберігання особистої інформації, і невідповідність може мати серйозні наслідки для бізнесу.

По-третє, відповідність стандартам є важливою для забезпечення довіри інших зацікавлених сторін, таких як клієнти, партнери та регулятори. Компанії, які виявляють високий ступінь відповідності, можуть насолоджуватися підвищеним довір'ям і залученням клієнтів, а також мають менше шансів потрапити в правові складнощі. [33]

Отже, етап відповідності стандартам та законодавству є стратегічно важливим для забезпечення легальності, безпеки та довіри в контексті впровадження SIEM.

Моніторинг та аналіз результатів є важливим вже на етапі впровадження систем управління подіями з кількох причин:

По-перше, це дозволяє організації відстежувати ефективність системи та виявляти можливі недоліки чи обмеження. Моніторинг роботи SIEM дозволяє вчасно виявляти проблеми та реагувати на них, забезпечуючи неперервну та ефективну роботу системи.

По-друге, аналіз результатів дозволяє оцінювати досягнення стратегічних цілей, які були визначені на початку впровадження. Виявлення та аналіз ключових показників продуктивності допомагає визначити, наскільки SIEM відповідає потребам організації та які зміни можуть бути внесені для покращення.

По-третє, моніторинг та аналіз є необхідними для виявлення нових тенденцій та можливостей. Шляхом вивчення отриманих даних можна виявити нові можливості для оптимізації бізнес-процесів, підвищення ефективності та вдосконалення стратегій управління подіями.[34]

Отже, моніторинг та аналіз результатів впровадження SIEM не тільки забезпечують ефективність роботи системи, але і служать інструментом для постійного вдосконалення та адаптації до змін в бізнес-середовищі.

Постійне вдосконалення є важливим етапом при впровадженні систем управління подіями, оскільки він створює механізми для постійного удосконалення функціоналу та ефективності системи відповідно до змін в бізнес-середовищі. Цей етап дозволяє організації адаптувати SIEM до нових викликів, оптимізувати процеси та максимізувати вигоди від використання системи.

Постійне вдосконалення також сприяє виявленню можливостей для оптимізації бізнес-процесів, що виникають під впливом динамічних змін у сфері технологій, ринку та вимог клієнтів. Це забезпечує гнучкість та конкурентоспроможність організації, дозволяючи їй ефективно реагувати на непередбачені обставини та вдосконалювати свою стратегію відповідно до поточних потреб.[35]

У кінцевому результаті, постійне вдосконалення стає важливим елементом стратегічного управління та допомагає організації не тільки зберігати свою конкурентоспроможність, але й розвиватися, реагуючи на зміни у внутрішньому та зовнішньому середовищі.

Навчання з питань стратегічних аспектів впровадження систем управління подіями є важливою складовою для організацій та професіоналів, які бажають успішно впровадити та використовувати ці системи в своїй діяльності. Навчання в цій області може бути доступним у вигляді онлайн-курсів, вебінарів, тренінгів та навчальних матеріалів від провідних компаній та організацій, що спеціалізуються на управлінні подіями та інформаційної безпеці. Інвестування в навчання з цієї області допоможе організації максимізувати користь від впровадження SIEM та забезпечити успішну стратегію управління подіями. [36]

Висновки до розділу 1.

Управління подіями в інформаційній безпеці на підприємстві — це складний процес, який вимагає інтеграції традиційних та новітніх методів для ефективного виявлення, аналізу та реагування на події.

Традиційні методи управління подіями базуються на використанні журналів подій, систем виявлення вторгнень та ручного аналізу. Вони є важливою частиною безпекового ландшафту підприємства.

Новітні технологічні рішення в управлінні подіями використовують автоматизацію, машинне навчання, когнітивний аналіз та інші інноваційні підходи. Ці технології допомагають виявляти складні загрози та забезпечувати ефективну відповідь на інциденти.

Стратегічні аспекти впровадження систем управління подіями включають в себе ретельне визначення бізнес-мети, інтеграцію з бізнес-процесами, аналіз ризиків, залучення зацікавлених сторін, вибір технологічних рішень, навчання персоналу та інші аспекти. Ці стратегічні елементи допомагають забезпечити успішне впровадження та оптимальне функціонування систем управління подіями. Загалом, інтеграція традиційних та інноваційних методів, а також стратегічний підхід до впровадження систем управління подіями, стає важливою складовою для забезпечення інформаційної безпеки та реагування на сучасні кіберзагрози

РОЗДІЛ 2
АНАЛІЗ ЗАСТОСУВАННЯ СУЧАСНИХ МЕТОДІВ УПРАВЛІННЯ ПОДІЯМИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НА ПІДПРИЄМСТВІ

2.1. Технічні аспекти сучасних систем управління подіями

У сучасному інформаційному суспільстві, де обсяги даних неабияк зростають, а загрози для інформаційної безпеки стають більш складними, системи управління подіями відіграють критичну роль у забезпеченні цілісності та безпеки підприємств. Зараз сфокусуємось на технічних аспектах сучасних систем управління подіями, зокрема на системах виявлення вторгнень та їх внеску у процес управління подіями.

Технічні аспекти сучасних систем управління подіями включають ряд ключових компонентів і функцій, які відіграють важливу роль у ефективному управлінні подіями. Ці системи зазвичай орієнтовані на автоматизацію та оптимізацію процесів планування та управління різноманітними подіями, від невеликих зборів до великих корпоративних заходів.

Основні технічні аспекти цих систем включають інтеграцію з іншими системами, автоматизацію процесів, аналітику та звітність, мобільні додатки та інтерфейси, а також безпеку та конфіденційність. [37]

Сучасні системи управління подіями часто інтегруються з іншими корпоративними системами та платформами, такими як системи управління відносинами з клієнтами (CRM), фінансові системи, інструменти електронної пошти та соціальні медіа для забезпечення безшовного обміну даними і підвищення ефективності. Ці системи дозволяють автоматизувати багато аспектів управління подіями, включаючи реєстрацію учасників, трекінг відвідуваності, розсилку електронних листів і створення звітів. Системи надають інструменти для аналізу даних про події, дозволяючи організаторам оцінювати ефективність

заходів, розуміти поведінку учасників і вносити корективи для майбутніх подій. Багато сучасних систем включають мобільні додатки, які дозволяють учасникам доступати інформацію про події, реєструватися та взаємодіяти з іншими учасниками. Важливим аспектом є забезпечення безпеки даних та дотримання норм конфіденційності, особливо у світлі зростаючих вимог до захисту персональних даних. [38]

Завдання цих систем полягає в тому, щоб спростити процес управління подіями, знизити витрати часу та ресурсів, підвищити залученість учасників, та надати цінну інформацію для планування майбутніх подій. Вони є незамінними інструментами для компаній та організацій, які регулярно проводять різноманітні заходи.

2.1.1. Системи виявлення вторгнень та їхній внесок в управління подіями

Системи виявлення вторгнень (СВВ) є ключовим елементом в системах управління подіями, забезпечуючи надійне та вчасне виявлення неправомірних дій або потенційно небезпечних подій в інформаційних системах підприємства. Їхнє завдання полягає в моніторингу активності в мережі, аналізі трафіку та ідентифікації аномалій, що можуть бути пов'язані з атаками або порушенням безпеки.

До основних функцій систем виявлення вторгнень входять декілька етапів, а саме моніторинг мережевої активності, аналіз знаків вторгнення, попередження та реагування, збір та аналіз журналів подій.

СВВ постійно відслідковують мережевий трафік, системні журнали та інші дані для виявлення будь-яких непередбачуваних або аномальних подій та використовують алгоритми та правила для визначення ознак, що вказують на можливий вторгнення або інші загрози. Виявивши потенційний інцидент, СВВ

сповіщає відповідальних працівників і може навіть автоматично ініціювати процедури відновлення або ізоляції вражених систем, стсьема активно аналізує журнали подій з різних джерел, включаючи файли журналів, інформацію від агентів безпеки та інші джерела, щоб визначити загрози. [39]

Внесок систем виявлення вторгнень у управління подіями полягає у забезпеченні швидкого виявлення загроз, автоматизованої відповіді на інциденти, зменшення часу реакції, посилення безпеки мережі.

СВВ дозволяє виявляти небезпечні події практично в реальному часі, допомагаючи уникнути серйозних наслідків для інформаційної безпеки, а також автоматизувати реакцію на інциденти, включаючи відсіювання загроз та їх подальшу обробку. Швидке виявлення та реагування на події, які порушують безпеку, допомагає зменшити час реакції на інцидент та мінімізувати його вплив на бізнес-процеси. Система також забезпечує неперервний моніторинг та виявлення вторгнень, чим підвищує загальний рівень безпеки інформаційної інфраструктури. [40]

Використання сучасних технологій у системах виявлення вторгнень, таких як машинне навчання та штучний інтелект, робить ці системи ще більш ефективними в розпізнаванні нових та складних загроз, що допомагає удосконалити процес управління подіями.

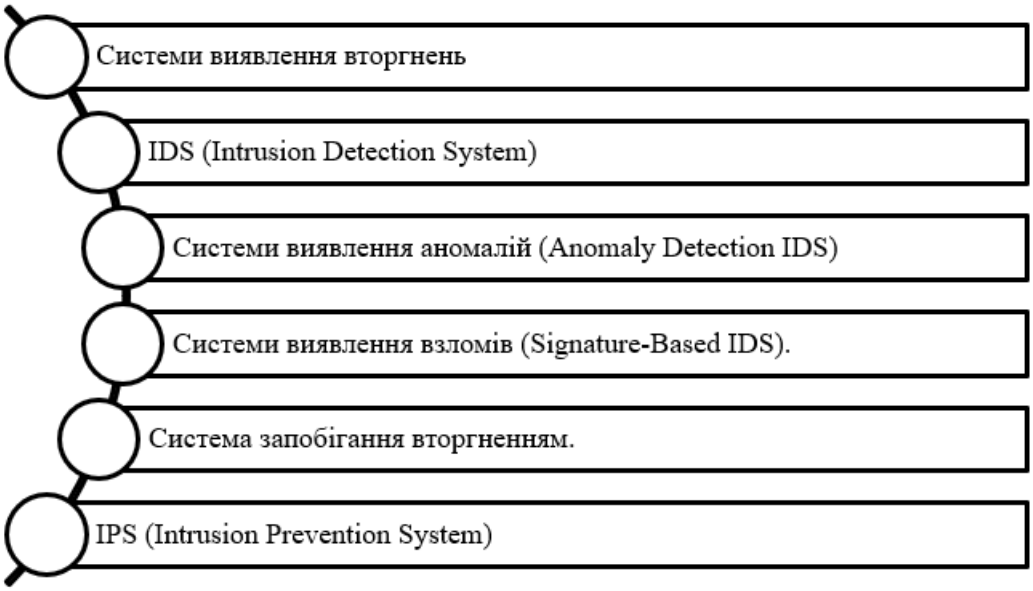

Рис. 2.1. Сучасні технічні системи управління подіями

Отже можна зробити висновок, що технічні аспекти сучасних систем управління подіями, зокрема систем виявлення вторгнень, відіграють важливу роль у забезпеченні безпеки інформації на підприємствах. Їхній внесок полягає в забезпеченні реагування на події шляхом виявлення потенційних загроз та забезпечення управління інцидентами на підприємстві. Використання новітніх технологій, таких як машинне навчання, дозволяє підвищити ефективність цих систем та покращити загальний рівень інформаційної безпеки.

IDS (Intrusion Detection System) – це система виявлення вторгнень. Вона призначена для виявлення незвичайної або агресивної активності в комп'ютерних мережах або системах, яка може свідчити про потенційні кібератаки або вторгнення.

Головною метою IDS є захист інформаційних ресурсів і комп'ютерних систем шляхом спостереження за мережевим трафіком або активністю в системі та виявлення незвичайних або підозрілих дій, таких як спроби несанкціонованого доступу, атаки зламу, віруси, черв'яки тощо. IDS може реагувати на ці події, сповіщаючи адміністратора або вживаючи інших заходів для запобігання або обмеження можливого вторгнення. [41]

Існують два основних типи IDS: Системи виявлення аномалій (Anomaly Detection IDS) та Системи виявлення взломів (Signature-Based IDS).

Системи виявлення аномалій виявляють вторгнення, порівнюючи поточну активність з попередніми шаблонами чи нормами. Якщо система виявляє незвичайну або аномальну активність, вона сповіщає про це. Системи виявлення взломів аналізують вхідні дані та порівнюють їх з відомими паттернами атак або відомими сигнатурами вірусів і черв'яків. Якщо вони виявляють сумісність, вони сповіщають про виявлену атаку.

IDS є важливим елементом захисту комп'ютерних систем і мереж, оскільки вони дозволяють вчасно реагувати на потенційні загрози та запобігати серйозним кібератакам. [42]

IPS (Intrusion Prevention System) – це система запобігання вторгненням. Вона виконує схожі функції, що і IDS (система виявлення вторгнень), але, в додаток до

виявлення підозрілої або зловмисної активності, IPS також має здатність приймати активні заходи для блокування цієї активності в реальному часі.

Основна мета IPS полягає в захисті комп'ютерних систем і мереж від потенційних загроз, не дозволяючи їм нанести шкоду. Ця система може вживати різні заходи для запобігання вторгненням, такі як блокування атак, відключення комп'ютерів або пристроїв, які представляють загрозу, або відправлення сповіщень про атаку адміністраторам для подальших заходів.

Основна відмінність між IDS і IPS полягає в тому, що IDS визначає потенційні атаки та надає інформацію про них адміністраторам для подальшої реакції, тоді як IPS активно втручається у процес і блокує шкідливу активність в реальному часі.

IPS допомагає забезпечити вищий рівень безпеки для мережі або системи, оскільки він дозволяє автоматично реагувати на загрози навіть без втручання людини, що може бути важливим у вразливих сценаріях. Порівняння IDS і IPS зображено в Таблиці 2.1 [43]

Таблиця 2.1

Порівняльна таблиця IDS і IPS

Параметр	**IDS**	**IPS**
Призначення	Виявлення потенційних атак	Виявлення та запобігання атак
Реакція на атаки	Сповіщення адміністратору	Активна блокування атак
Робочий принцип	Моніторинг трафіку і системи	Моніторинг та блокування трафіку
Типи виявлення	Аномалійне і сигнатурне	Аномалійне і сигнатурне
Реакція на загрози	Сповіщення адміністратору	Блокування, відключення, сповіщення
Застосування	Виявлення і діагностика атак	Запобігання та блокування атак
Швидкість реакції	Реакція після виявлення	Реакція в реальному часі
Типи помилок	Може бути помилкове виявлення	Може блокувати легітимний трафік
Налаштування	Менш складне налаштування	Складніше налаштування
Ресурси	Зазвичай менше вимог до ресурсів	Зазвичай більше вимог до ресурсів
Загальна ефективність	Залежить від реакції адміністратора	Автоматична реакція

Поєднуючи системи IDS і IPS у комплексну інтегровану систему, створюється рішення, яке має можливість виявлення потенційних атак і реагування на них в реальному часі. В результаті поєднання виникають певні переваги, але й наслідки, що потребують удосконаленого супроводу.

Найбільшою перевагою інтегрованої системи є те, що вона може автоматично реагувати на потенційні загрози, не лише виявлюючи їх, але і блокуючи атаки в реальному часі, що може зменшити шкоду від атак і прискорити реагування на них. Оскільки IDS і IPS працюють разом в єдиній системі, може бути менше шансів на помилкове виявлення атак або неправильні блокування легітимного трафіку. Інтегрована система може забезпечити більш ефективне використання ресурсів, оскільки не потребує окремих систем для виявлення та реакції на атаки. [44]

Але, на жаль, в кожній системі є свої недоліки, а в інтегрованій системі це призведення до блокування легітимного трафіку через неправильне виявлення або сприйнятливість до атак, які можуть використовувати такі системи

Загалом, об'єднання IDS і IPS може бути корисним для організацій з високими вимогами до безпеки, якщо це зроблено правильно і з урахуванням специфічних потреб і ризиків.

2.1.2. Можливості систем управління подіями

Системи управління подіями (СУП) відкривають широкі можливості для ефективного керування інформацією та ресурсами в організаціях. Вони дозволяють автоматизувати моніторинг подій, сповіщати про важливі зміни та реагувати на них в режимі реального часу. СУП використовуються для підтримки різноманітних процесів, включаючи керування ресурсами, безпеку, моніторинг систем та аналітику даних.

Ці системи можуть ефективно обробляти великі обсяги інформації,

фільтрувати події за певними критеріями та автоматично визначати пріоритетність. Вони підтримують взаємодію між різними компонентами системи, забезпечуючи єдність інформаційного середовища.

СУП також можуть використовуватися для прогнозування та аналізу подій, що дозволяє приймати обґрунтовані рішення на основі даних. Це допомагає підприємствам бути більш гнучкими та адаптивними до змін в оточенні. [45]

Однією з ключових можливостей є забезпечення високої доступності і надійності систем, зокрема у випадку виникнення непередбачуваних ситуацій чи аварій. СУП дозволяють швидко виявляти та вирішувати проблеми, зменшуючи час відновлення та мінімізуючи втрати.

Крім того, системи управління подіями можуть бути інтегровані з іншими системами підприємства, що розширює їхні можливості та полегшує обмін даними між різними платформами.

Загалом, використання систем управління подіями дозволяє підприємствам підвищити ефективність операцій, забезпечити швидку реакцію на зміни та покращити загальний рівень управління.

2.1.3. Машинне навчання та штучний інтелект в управлінні подіями

В сучасному інформаційному середовищі, де обсяги даних постійно зростають, важливим стає використання передових технологій, таких як машинне навчання (МН) та штучний інтелект (ШІ), для ефективного управління подіями та забезпечення інформаційної безпеки підприємств.

Машинне навчання в системах управління подіями розширює їхні можливості через автоматизацію процесів аналізу та взаємодії з подіями. За допомогою алгоритмів машинного навчання, система може вивчати патерни та тенденції зі збереженої інформації, щоб автоматично розпізнавати та класифікувати події.

Це дозволяє системам управління подіями не лише реагувати на визначені правила, але і навчатися з досвіду та адаптуватися до змін в оточенні. Машинне навчання допомагає покращити точність розпізнавання подій, спростити процес фільтрації та класифікації, а також забезпечити більш адаптивну та інтелектуальну систему управління подіями.

Ефективність використання машинного навчання полягає в здатності системи автоматично визначати важливість та пріоритетність подій, швидко адаптуватися до нових умов та оптимізувати процеси реагування. Це також дозволяє зменшити навантаження на людський фактор, оскільки система може самостійно приймати рішення на основі навченого досвіду.[46]

Машинне навчання в системах управління подіями сприяє створенню більш гнучких та реактивних платформ, що відповідають на сучасні вимоги динамічного бізнес-середовища. Такий підхід дозволяє підприємствам ефективніше використовувати дані, вдосконалювати процеси управління та забезпечувати високий рівень автоматизації в реальному часі.

Штучний інтелект в управлінні подіями розкриває перед підприємствами широкі можливості автоматизації та оптимізації процесів. Алгоритми машинного навчання та інші методи штучного інтелекту дозволяють системам в режимі реального часу аналізувати величезний потік даних, розпізнавати патерни та вчаться з попередніх подій.

Перевагою використання штучного інтелекту в управлінні подіями є можливість швидкого та точного реагування на зміни в оточенні. Системи можуть автоматично виявляти аномалії, передбачати можливі ризики та вживати відповідні заходи, зменшуючи вплив негативних подій на бізнес-процеси.

Штучний інтелект також дозволяє створювати персоналізовані стратегії управління подіями, враховуючи унікальні характеристики та потреби конкретного підприємства. Це призводить до ефективнішого використання ресурсів та збільшення адаптивності до змін в бізнес-середовищі.

Штучний інтелект сприяє автоматизації рутинних завдань управління подіями, що відпускає час та ресурси для стратегічного аналізу та прийняття

рішень. Це підвищує продуктивність та дозволяє фахівцям зосередитися на важливих аспектах управління та стратегії розвитку. [47]

Загалом, використання штучного інтелекту в управлінні подіями підвищує рівень автоматизації, забезпечує точність та прогностичні здібності, що сприяє створенню більш адаптивних та ефективних бізнес-процесів. Додатковий перелік речей, що можуть бути автоматизовані при використанні штучного інтелекту в управлінні подіями зображено на рисунку 2.2.

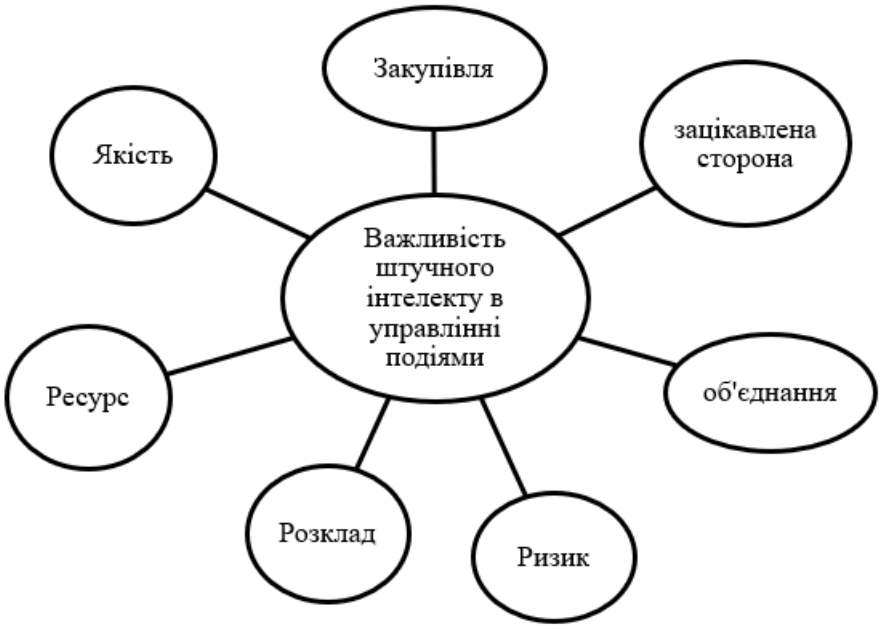

Рис. 2.2. Переваги штучного інтелекту в управлінні подіями

Інтеграція машинного навчання та штучного інтелекту у системи управління подіями дозволяє створювати розумні та самоадаптивні рішення. Це може включати автоматизоване вдосконалення моделей, реагування на нові загрози, створення прогнозів та стратегій відповіді. Внаслідок цього системи можуть автоматично адаптуватися до нових та загроз, що змінюються, за допомогою постійного навчання та оптимізації моделей. Машинне навчання та штучний інтелект дозволяють виявляти та аналізувати нові, раніше невідомі загрози, що робить системи більш адаптивними. Аналіз даних за допомогою МН та ШІ дозволяє створювати прогнози та ефективні стратегії відповіді на події, забезпечуючи більш прогностичний підхід до управління подіями. [48]

Інтеграція машинного навчання та штучного інтелекту в системи управління подіями допомагає не тільки підвищити ефективність виявлення та реагування на

події, але й зробити цей процес більш адаптивним та орієнтованим на майбутнє.

2.1.4. Забезпечення інтеграції систем управління подіями з існуючими IT-інфраструктурами

Забезпечення інтеграції систем управління подіями з існуючими IT-інфраструктурами полягає в створенні ефективного механізму взаємодії між системами та платформами, які вже існують в організації. Головним завданням цього процесу є забезпечення синхронізації обміну даними та інформацією між системами у режимі реального часу.

Інтеграція систем управління подіями з існуючою IT-інфраструктурою дозволяє здійснювати автоматизовану обробку подій та інформації з різних джерел. Це може включати в себе інтеграцію з базами даних, додатками, хмаровими сервісами, а також іншими системами управління, які вже використовуються в організації.

Завдання інтеграції включає в себе створення єдиної інформаційної екосистеми, де дані можуть ефективно обмінюватися та використовуватися між різними системами. Це дозволяє уникнути ізольованих "силосів" даних та забезпечує гладкий потік інформації в усьому підприємстві.

Інтеграція також вирішує завдання сумісності між різними технологічними стеками та стандартами, що забезпечує безпроблемну роботу систем управління подіями разом з існуючими інструментами та ресурсами. Такий підхід робить можливим використання потужностей систем управління подіями в контексті загальної IT-стратегії підприємства. [49]

Важливо використовувати стандартизовані протоколи та формати обміну даними для взаємодії між СУП та існуючою інфраструктурою. Наприклад, використання стандартів, таких як Common Event Format (CEF) або Syslog, дозволяє легше обробляти та передавати події між різними системами.

Наявність добре документованих API (інтерфейсів програмування застосунків) для СУП дозволяє легко забезпечити взаємодію з іншими системами. Інтеграційні модулі, які надають готові засоби для інтеграції з популярними платформами та додатками, спрощують процес підключення СУП до існуючої інфраструктури.[50]

Забезпечення безпеки інтеграції включає в себе використання захисту даних та шифрування для передачі інформації між системами. Важливо враховувати стандарти безпеки, такі як OAuth або OpenID, для забезпечення безпечної ідентифікації та автентифікації.[51]

Використання систем медіації або брокерів подій може спростити процес інтеграції, дозволяючи різним системам обмінюватися подіями через єдиний інтерфейс. Це дозволяє ефективно керувати потоками подій та їхнім розподілом між різними компонентами системи.[52]

Автоматизована конфігурація дозволяє швидко налаштовувати параметри інтеграції та забезпечує консистентність налаштувань між різними системами. Інструменти для автоматичного виведення конфігурацій можуть спростити і покращити процес інтеграції.[53]

Регулярне тестування та моніторинг інтеграції дозволяє вчасно виявляти та вирішувати проблеми, що можуть виникнути під час обміну даними між системами. Застосування засобів моніторингу дозволяє виявляти аномалії та оптимізувати продуктивність інтеграції.

Інтеграція систем управління подіями з існуючими IT-інфраструктурами допомагає покращити цілісність та ефективність управління подіями, забезпечуючи обширний огляд безпекових інцидентів та оперативну реакцію на них в межах усієї організації.

2.2. Методи управління подіями в інформаційній безпеці

Методи управління подіями в інформаційній безпеці включають в себе використання СУП, моніторинг та аналіз потоків даних для виявлення аномалій та потенційних загроз, реалізацію технологій машинного навчання для автоматичного визначення та класифікації подій. Також використовуються засоби автоматизованої реакції на виявлені події, щоб мінімізувати вплив потенційних загроз на інформаційну безпеку. Застосовують також інтеграцію з іншими системами безпеки та використання алгоритмів для аналізу та ідентифікації несподіваних сценаріїв.

Рис. 2.3. Методи управління подіями в інформаційній безпеці

2.2.1. Аналіз стійкості та надійності методів управління подіями

Аналіз стійкості та надійності методів управління подіями є важливим аспектом в інформаційних технологіях, бізнес-процесах та інших сферах діяльності, де використовується обробка подій. Визначення стійкості включає в себе оцінку відповідності системи до атак та здатність витримувати негативні

впливи. Надійність враховує здатність системи до ефективної роботи та відновлення в разі інциденту. Важливо враховувати динаміку кіберзагроз та забезпечити постійне оновлення та оптимізацію методів управління подіями для забезпечення максимальної стійкості та надійності в умовах швидко змінюючогося кіберпростору. [54]

Методи управління подіями повинні бути стійкими до помилок та здатними ефективно відновлювати роботу в разі виникнення непередбачених ситуацій. Система повинна вміти ефективно обробляти асинхронні події та уникати блокувань, які можуть виникнути при великому обсязі одночасних подій.

Система повинна забезпечувати гарантії доставки подій, щоб жодна подія не була втрачена або згублена. Надійні методи управління подіями повинні бути здатні ефективно працювати при великому обсязі подій і не приводити до відмов системи. Методи управління подіями повинні бути здатні масштабуватися для впорядкування зростаючого обсягу подій без втрати продуктивності.

Система повинна бути захищеною від різних видів атак, таких як впровадження шкідливого коду через події або атаки на канали комунікації. Забезпечення можливості моніторингу для виявлення проблем та покращення ефективності системи управління подіями. Зберігання журналів подій для подальшого аналізу та відстеження стану системи. [55]

Система повинна бути гнучкою та дозволяти налаштовувати правила обробки подій відповідно до конкретних вимог Методи управління подіями повинні бути легко інтегровані з іншими системами та сервісами.

Аналіз стійкості та надійності методів управління подіями варто проводити поетапно, враховуючи конкретні потреби та характеристики системи, в якій вони використовуються.

2.2.2. Моніторинг змін у загрозах та оцінка ефективності вдосконалення стратегій відповіді на них

Моніторинг змін у загрозах та оцінка ефективності вдосконалення стратегій відповіді на них відображають неперервний цикл аналізу та вдосконалення заходів інформаційної безпеки. Цей процес забезпечує постійне вдосконалення стратегій відповіді на загрози з урахуванням актуальної ситуації та розвитку нових загроз.

Моніторинг змін у загрозах передбачає систематичний аналіз оточення, виявлення нових загроз та оновлення існуючих. Це включає в себе використання інструментів моніторингу, аналізу журналів подій, а також спеціалізованих систем управління подіями для оперативного виявлення та класифікації подій.

Оцінка ефективності вдосконалення стратегій полягає в аналізі реакції на попередні загрози, визначенні слабких місць та розробці конкретних заходів для покращення безпеки. Вона включає в себе збір даних про впроваджені заходи, аналіз їхньої ефективності та внесення необхідних коректив. [56]

Цей неперервний цикл дозволяє підтримувати адаптивність та гнучкість в системі управління подіями, щоб вчасно реагувати на нові загрози та підвищувати ефективність стратегій відповіді на них. Для ефективного використання системи необхідно завжди розглядати аспекти процесу.

Процес моніторингу змін у загрозах та оцінка ефективності вдосконалення стратегій відповіді на них є критичним елементом у сфері кібербезпеки. Постійна оцінка загроз та вдосконалення стратегій відповіді вимагає систематичного аналізу та реагування на змінюючийся кіберландшафт. Моніторинг полягає у виявленні нових атак, аномалій та тенденцій, а також в оцінці їхнього потенційного впливу.

Оцінка ефективності стратегій відповіді на кіберзагрози визначається успішністю їхнього застосування та впливом на безпеку організації. Включає в себе аналіз результатів виявлених інцидентів, взаємодію з існуючими заходами та здатність адаптуватися до нових викликів у кіберпросторі. Необхідно проводити аудит безпеки для оцінки стану безпеки систем, виявлення слабких місць та розробки стратегій для їх усунення. Встановлення метрик, які можна використовувати для вимірювання ефективності стратегій відповіді, можуть включати в себе час виявлення інцидентів, час відновлення, кількість успішно

зупинених атак та інші ключові показники. Цей процес допомагає підтримувати та вдосконалювати стратегії відповіді для максимального забезпечення кібербезпеки організації.[57]

Для вдосконалення стратегій необхідно проводити ретельний аналіз інцидентів для виявлення недоліків у відповідях та вивчення прикладів кращої практики. Також підприємство забов'язане оновлювати політику

Навчання та свідомість персоналу передбачає систематичне інформування та тренування персоналу з питань кіберзахисту, щоб підвищити їхню готовність розпізнавати потенційні загрози та ефективно реагувати на них. Навчання також спрямоване на формування свідомої культури безпеки, де працівники розуміють важливість власної ролі у забезпеченні кібербезпеки та дотримання найкращих практик в цій області.

Цей цикл моніторингу, оцінки та вдосконалення є постійним ітеративним процесом, що дозволяє адаптувати стратегії відповіді до ландшафту кіберзагроз, що активно змінюється.

2.2.3. Планування та розгортання системи управління подіями

Для планування та розгортання системи управління подіями важливо мати чітке розуміння потреб організації, здатність визначити ключові завдання та цілі, які має вирішити система. Необхідно враховувати конкретні характеристики бізнес-процесів та особливості інфраструктури.

Під час планування важливо визначити, які дані та події є стратегічно важливими для організації, а також які процеси вимагають автоматизації чи підтримки системою управління подіями.

Розгортання системи передбачає правильний вибір технологій, інфраструктурних рішень та інтеграцію з існуючими системами. Важливо забезпечити надійність та швидкодіючість системи, а також забезпечити безпеку

обробки та зберігання інформації.

Планування та розгортання системи управління подіями допомагають підприємствам ефективно виявляти, аналізувати та реагувати на події в режимі реального часу, що може покращити управління ризиками, підвищити безпеку, оптимізувати бізнес-процеси та забезпечити ефективність у вирішенні завдань організації.[58]

Початковий етап полягає в визначенні стратегічних цілей та завдань, які SIEM повинен вирішити. Аналіз інфраструктури та визначення джерел подій визначають обсяг та характер інформації, яку система буде аналізувати.

Далі обирається підходяща SIEM-платформа, яка відповідає потребам організації. Розгортання включає встановлення та конфігурацію системи, налаштування збору та аналізу подій з різних джерел.

Розробка правил кореляції та стратегій реагування на інциденти є важливим етапом для ефективного виявлення та відповіді на аномальні або підозрілі активності. Також важливо налаштувати оповіщення для оперативного сповіщення про події, що вимагають уваги.

Паралельно із розгортанням технічної інфраструктури, слід приділяти увагу навчанню та підготовці персоналу, який буде використовувати SIEM. Їхня обізнаність і підготовка грають ключову роль у вдалому використанні системи.[59]

Завершальним етапом є впровадження системи в роботу та постійний моніторинг її ефективності. Регулярні аудити та оновлення дозволяють підтримувати високий рівень кіберзахисту в умовах постійних змін у кіберпросторі.

2.2.4. Розробка імітаційних та навчальних сценаріїв управління подіями

Розробка імітаційних та навчальних сценаріїв управління подіями є важливою складовою сфери інформаційної безпеки та бізнес-контингенту. Цей

процес передбачає створення віртуальних або симульованих сценаріїв, які моделюють різноманітні ситуації та події, що можуть виникнути в реальному бізнес-середовищі.

Метою розробки імітаційних та навчальних сценаріїв є тренування персоналу та вдосконалення стратегій управління подіями. Цей підхід дозволяє організаціям підвищити рівень готовності до вирішення різноманітних ситуацій, включаючи кібератаки, природні катастрофи, технічні збої та інші інциденти.

Розробка сценаріїв управління подіями дозволяє виробити ефективність комунікації, реакції та співпраці між різними відділами та членами команди у віртуальному середовищі. Також, цей процес сприяє виявленню слабких місць у системах управління подіями та формуванню кращих стратегій реагування на виклики. [60]

Використання імітаційних та навчальних сценаріїв управління подіями допомагає підвищити культуру безпеки в організації, зменшити час реакції на інциденти та забезпечити оптимальні умови для виявлення, аналізу та вирішення проблем в умовах, які моделюють реальне бізнес-середовище.

Розробка імітаційних та навчальних сценаріїв управління подіями — це процес, що вимагає систематичного та уважного підходу для підготовки персоналу до реальних кіберзагроз.

Рис. 2.4. Розробка сценаріїв управління подіями

Перший етап включає визначення конкретних цілей та сценаріїв, які будуть відтворюватися під час навчання. Далі необхідно створити детальний опис сценаріїв, включаючи в себе різноманітні кібератаки, інциденти та виклики для управління подіями. Це може охоплювати різні вектори атак, від витоку даних до виявлення та реагування на аномалії в системі.

Після цього важливим етапом є відтворення цих сценаріїв у симуляційному середовищі. Важливо забезпечити максимально реалістичні умови та враховувати різноманітність можливих ситуацій.[61]

Паралельно із симуляцією сценаріїв слід проводити тренінг персоналу, використовуючи отримані результати для вдосконалення їхніх навичок та підготовки до реальних ситуацій. Важливо забезпечити обговорення та аналіз кожного сценарію з метою винесення важливих вивчень та вдосконалення стратегій управління подіями.

Завершальний етап полягає у систематичному оновленні та розширенні сценаріїв, враховуючи нові кіберзагрози та тенденції, що дозволяє підтримувати високий рівень готовності персоналу до найновіших викликів у сфері кібербезпеки.

2.3. Використання аналітики великих даних у контексті управління подіями

Використання аналітики великих даних у контексті управління подіями є стратегічним підходом, спрямованим на ефективне виявлення, аналіз та реагування на події в реальному часі. Метою цього підходу є використання об'ємних та різноманітних даних для здійснення передбачуваності, ідентифікації патернів та забезпечення швидкого реагування на зміни в бізнес-середовищі.

Великі дані дозволяють аналізувати величезні масиви структурованих та неструктурованих даних, таких як логи подій, транзакції, дані від сенсорів,

соціальні мережі тощо. Застосування аналітики великих даних в управлінні подіями дозволяє підприємствам ефективно виявляти аномалії, передбачати ризики та автоматизовано реагувати на події в реальному часі.

Використання аналітики великих даних у управлінні подіями надає підприємствам деякі переваги. Аналітика великих даних дозволяє передбачати можливі події та ризики, базуючись на аналізі історичних даних та виявленні патернів. Здатність обробляти великі обсяги даних у режимі реального часу дозволяє швидко реагувати на події та миттєво виконувати необхідні заходи. Аналітика великих даних допомагає виявляти аномалії та непередбачені сценарії, що може свідчити про потенційні загрози або проблеми в бізнес-процесах. Аналіз великих даних дозволяє розробляти персоналізовані стратегії управління подіями, враховуючи специфіку та потреби конкретної організації. [62]

Цей підхід використовується в різноманітних галузях, включаючи кібербезпеку, фінансовий сектор, телекомунікації, виробництво та інші сфери бізнесу. Наприклад, в області кібербезпеки аналітика великих даних дозволяє виявляти та протидіяти кіберзагрозам, а в фінансовому секторі вона використовується для виявлення фінансових шахраїв та запобігання шахрайським операціям.

Використання аналітики великих даних у контексті управління подіями допомагає організаціям забезпечити прогностичність, ефективність та стратегічну гнучкість у вирішенні викликів та оптимізації бізнес-процесів.

2.3.1. Застосування резервування та відновлення даних

Застосування резервування та відновлення даних у контексті управління подіями є критичним елементом стратегій інформаційної безпеки та бізнес-контингенту. Цей процес передбачає створення копій даних та механізмів для їх швидкого відновлення в разі виникнення подій, що можуть призвести до втрат чи

пошкоджень інформації.

Ефективне використання цього процесу може зіграти значну роль у роботі підприємства. Без регулярного створення резервних копій даних підприємство не зможе запобігти можливим втратам важливої інформації внаслідок технічних невдач, кібератак, природних катастроф чи інших подій. Також наявність резервів дозволяє швидко відновлювати роботу систем та бізнес-процесів після інцидентів, забезпечуючи найменший час простою. Резервування та відновлення даних є важливою частиною загальної стратегії управління подіями, сприяючи забезпеченню неперервності бізнес-процесів та зменшенню впливу інцидентів на операційну діяльність. [63]

Важливість цього етапу виявляється у можливості швидкого відновлення операцій, мінімізації втрат та забезпеченні стійкості бізнес-систем у непередбачених обставинах. Процес резервування та відновлення даних включає створення регулярних резервних копій, перевірку їхньої цілісності, а також впровадження механізмів автоматичного відновлення під час інцидентів.

2.3.2. Управління логічною цілісністю та конфіденційністю даних

Управління логічною цілісністю та конфіденційністю даних у контексті управління подіями - це процес, спрямований на забезпечення цілісності та конфіденційності інформації під час виникнення різних подій та інцидентів. Цей підхід використовується для захисту важливих даних від несанкціонованого доступу, модифікацій чи витоку під час подій, що можуть вплинути на безпеку бізнес-процесів.

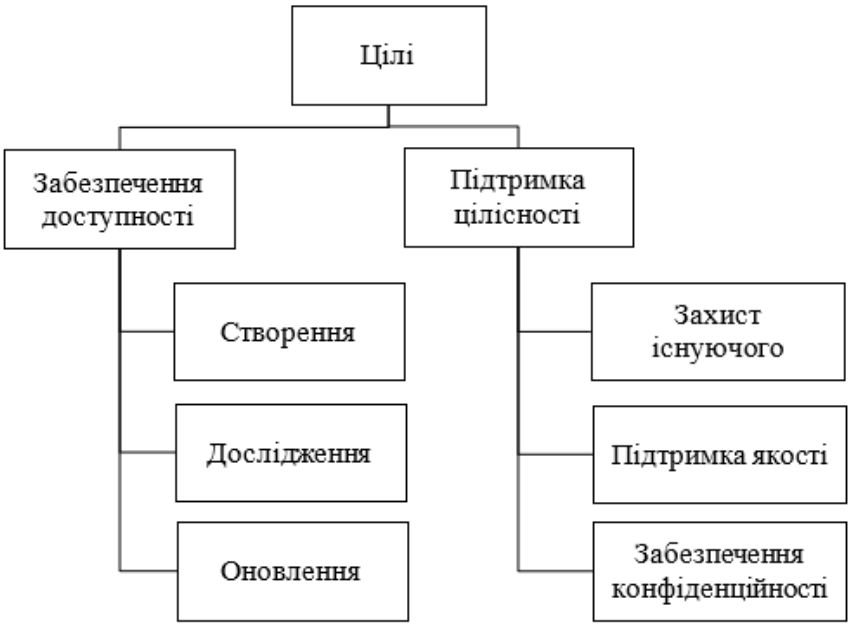

Рис. 2.5. Цілі управління логічною цілісністю та конфіденційністю даних

Управління логічною цілісністю та конфіденційністю даних важливе для забезпечення довіри до інформації та мінімізації можливості виникнення ризиків для бізнес-операцій. Це є важливим етапом у вирішенні завдань інформаційної безпеки та забезпеченні стійкості організації до різних інцидентів.

Процес забезпечення логічної цілісності передбачає виявлення та вирішення будь-яких аномалій чи незвичайних змін у данних, що можуть вказувати на можливі атаки або порушення. Заходи конфіденційності включають в себе обмеження доступу до чутливої інформації та застосування шифрування для захисту її від несанкціонованого перегляду.

Цей процес відбувається через впровадження заходів безпеки, таких як використання сучасних методів шифрування, регулярне оновлення політик безпеки, моніторинг доступу до даних та швидка реакція на будь-які порушення безпеки. В результаті, управління логічною цілісністю та конфіденційністю даних допомагає забезпечити надійний захист інформації, знижує ризики і зберігає довіру стейкхолдерів до організації. [64]

Управління логічною цілісністю та конфіденційністю даних використовується з метою забезпечення безпеки та надійності інформації. Ці

процеси мають на меті перешкоджати несанкціонованому доступу, змінам чи втратам даних, а також забезпечувати їхню конфіденційність, зберігаючи відомості від доступу осіб, які не мають на це прав.

Управління логічною цілісністю зосереджене на тому, щоб гарантувати, що дані залишаються недоторканими та невідомими для несанкціонованих змін, тоді як управління конфіденційністю ставить за мету обмежити доступ до інформації лише авторизованим користувачам, забезпечуючи таким чином захист від недозволених розголошень. [65]

Ці практики є ключовими у вирішенні проблем безпеки даних та використовуються в різних галузях, включаючи інформаційні технології, фінанси, медицину та інші сфери, де важлива конфіденційність та цілісність інформації.

2.3.3. Управління подіями у мультихмарному середовищі

Google Cloud провайдер – це компанія Google, яка надає хмарні обчислення та послуги для розробників та підприємств. Вони пропонують широкий спектр інфраструктурних, платформених та програмних послуг, які можна використовувати для різних цілей.

Google Cloud надає послуги, які дозволяють орендувати віртуальні сервери, зберігати дані в хмарних сховищах, налаштовувати мережеві ресурси та інше. Це дозволяє компаніям масштабувати свою інфраструктуру зручно та ефективно. Google Cloud також пропонує широкий спектр платформенних послуг, таких як бази даних, інструменти для розробки штучного інтелекту, аналітики даних, а також інші готові рішення, що спрощують розробку і впровадження програм.

Google Cloud надає розробникам доступ до різних інструментів і середовищ для розробки, тестування і впровадження програм, включаючи Kubernetes, Cloud Functions та інші. Провайдер пропонує різноманітні засоби для налаштування безпеки, моніторингу та управління мережами, що допомагають захищати дані та

забезпечувати надійність. Google Cloud надає доступ до потужних інструментів та середовищ для розробки та навчання моделей штучного інтелекту та машинного навчання. [66]

Цей провайдер використовується компаніями для різних цілей, таких як розробка веб-додатків, аналіз даних, створення інтелектуальних систем, забезпечення високої доступності та багато іншого. Використовуючи Google Cloud, підприємства можуть збільшити ефективність своїх IT-процесів і зменшити витрати на інфраструктуру та обслуговування.

Microsoft Azure – це хмарна обчислювальна платформа та набір послуг, які надаються компанією Microsoft. Вона призначена для створення, розгортання та керування різноманітними обчислювальними ресурсами та додатками в хмарному середовищі. Основна мета Microsoft Azure - це надати організаціям та розробникам доступ до потужностей хмарних технологій для розв'язання різних завдань та виконання бізнес-проектів. Azure надає широкий спектр послуг, включаючи обчислювальні ресурси, сховища даних, бази даних, інструменти для розробки додатків, аналітичні інструменти, штучний інтелект, Інтернет речей (IoT), блокчейн та багато інших.

Організації можуть використовувати Azure для створення, тестування та розгортання своїх додатків у хмарному середовищі. Це дозволяє їм легко масштабувати та керувати інфраструктурою. Azure надає можливість зберігати та обробляти великі обсяги даних, використовуючи сховища даних та аналітичні інструменти. Це корисно для ведення аналізу даних та прийняття інформованих рішень. Azure пропонує інструменти для розробки та навчання моделей штучного інтелекту та машинного навчання, що дозволяє створювати інтелектуальні додатки та сервіси. Azure допомагає підприємствам підключати, моніторити та управляти пристроями IoT, що дозволяє збирати та аналізувати дані з сенсорів та пристроїв. Azure надає різні інструменти для забезпечення безпеки даних, ідентифікації користувачів та захисту від загроз. [67]

Усі ці можливості дозволяють організаціям зосередитися на розвитку свого бізнесу, знижуючи витрати та складності управління інфраструктурою завдяки

хмарним рішенням Azure.

Amazon Web Services (AWS) – це хмарна обчислювальна платформа та набір послуг, які надаються компанією Amazon. Вона є однією з найпопулярніших та найрозширеніших хмарних платформ у світі. AWS дозволяє організаціям і розробникам отримувати доступ до різноманітних обчислювальних ресурсів та послуг, необхідних для створення, розгортання та управління різноманітними додатками та інфраструктурою.

AWS надає можливість легко масштабувати ресурси в залежності від потреб вашого бізнесу. Ви можете збільшувати або зменшувати потужність обчислювальних ресурсів за потребою, що дозволяє ефективно використовувати ресурси і знижувати витрати. AWS пропонує широкий спектр послуг, включаючи обчислювальні ресурси, сховища даних, бази даних, мережеві ресурси, інструменти розробки, аналітику, штучний інтелект та багато інших. Це дозволяє вам будувати різні типи додатків і розв'язувати різні завдання.

AWS має дата-центри та регіональні центри обробки даних по всьому світу, що дозволяє розгортати додатки та послуги біля ваших користувачів з урахуванням географічних особливостей. AWS надає інструменти для забезпечення безпеки даних та додатків, а також гарантує високу доступність та надійність ваших систем. Використання AWS може допомогти знизити витрати на інфраструктуру та обслуговування, оскільки ви платите лише за ті ресурси, які ви фактично використовуєте, і не потрібно вкладати гроші в капіталовкладення в обладнання. [68]

Загалом, AWS допомагає організаціям і розробникам прискорити розробку та розгортання додатків, підвищити продуктивність і знизити витрати завдяки хмарним можливостям та гнучкій інфраструктурі. Порівняння сервісів для управління подіями у мультихмарному середовищі наведено в Таблиці 2.2

Таблиця 2.2

Amazon Web Services, Microsoft Azure і Google Cloud Platform в контексті їх можливостей для управління подіями

Характеристика	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform (GCP)
Надавані сервіси	AWS Elastic Beanstalk, AWS Lambda, AWS Step Functions, Amazon EventBridge	Azure Functions, Azure Logic Apps, Azure Event Grid	Cloud Functions, Cloud Pub/Sub, Cloud Scheduler, Cloud Run
Інтеграція з іншими сервісами	AWS інтегрується з широким спектром інших AWS-послуг та інструментів.	Azure легко інтегрується з іншими Microsoft-продуктами, такими як Office 365, і багатьма сторонніми сервісами.	GCP також має великий вибір інтеграцій, включаючи інші хмарні сервіси та сторонні програми.
Моніторинг та аналітика	AWS CloudWatch, AWS X-Ray	Azure Monitor, Azure Application Insights	Google Cloud Monitoring, Google Cloud Logging
Управління (рівень складності)	AWS може бути більш складним для новачків, але надає більше гнучкості та контролю.	Azure надає інструменти для легкого управління, зокрема за допомогою Azure Portal.	GCP відомий своєю простотою в управлінні та інтуїтивним інтерфейсом.
Доступність сервісу	AWS має широкий розподілений обсяг дата-центрів по всьому світу.	Azure також має глобальну присутність, з дата-центрами в багатьох регіонах.	GCP також присутній у численних регіонах та зон хмарних обчислень.
Цінова політика	AWS пропонує широкий вибір цінових планів та моделей оплати.	Azure також надає різноманітні опції ціноутворення.	GCP може бути конкурентоспроможним за ціною, але ціни можуть відрізнятися в залежності від регіону.

Залежно від конкретних потреб та унікальних вимог вашого проекту для Управління подіями, ви можете вибрати один з хмарних провайдерів, який краще підходить вашій ситуації. Кожен з цих провайдерів має свої переваги та слабкі сторони, тому важливо враховувати ваші конкретні вимоги та бюджет при прийнятті рішення

Управління подіями (Event Management) у мультихмарному середовищі вимагає особливого підходу, оскільки дані та процеси можуть розташовуватися в різних хмарних платформах. Ефективне управління подіями дозволяє виявляти, аналізувати та реагувати на події в реальному часі, надаючи організації можливість

забезпечувати безпеку та ефективність своїх інфраструктур та послуг.

Однією з ключових особливостей управління подіями у мультихмарному середовищі є здатність інтеграції та синхронізації інформації з різних хмарних ресурсів. Це передбачає використання спеціалізованих інструментів та платформ, які забезпечують єдиний погляд на всі події та інциденти, що відбуваються в усіх хмарних середовищах.

Управління подіями включає в себе автоматизовані механізми для виявлення незвичайних або підозрілих активностей, аналізу журналів подій, ідентифікації загроз та вжиття відповідних заходів у реальному часі. Важливою частиною цього процесу є також впровадження механізмів відновлення, що дозволяють відновлювати нормальну роботу систем та бізнес-процесів після інцидентів. [69]

Мультихмарне середовище ставить перед управлінням подіями нові виклики, пов'язані з гетерогенністю та розподіленістю ресурсів. Ефективне управління подіями допомагає організаціям забезпечити безпеку даних, швидко реагувати на потенційні загрози та оптимізувати використання хмарних середовищ для досягнення стратегічних цілей.

Висновки до розділу 2

У контексті управління подіями в інформаційній безпеці та використання аналітики великих даних, ключовою метою є ефективний аналіз, виявлення та реагування на інциденти, що можуть впливати на безпеку підприємства. Розглядаючи різні аспекти управління подіями, можна визначити декілька важливих висновків.

Технічні аспекти сучасних систем управління подіями, такі як системи виявлення вторгнень, можливості систем управління подіями та застосування машинного навчання та штучного інтелекту, сприяють покращенню реакції на загрози та підвищенню ефективності заходів забезпечення безпеки. Забезпечення

інтеграції систем управління подіями з існуючими IT-інфраструктурами стає ключовим етапом для забезпечення цілісності та ефективності управління подіями на підприємстві.

Методи управління подіями в інформаційній безпеці, такі як аналіз стійкості та надійності, моніторинг загроз та планування стратегій відповіді, сприяють не лише виявленню інцидентів, але й вдосконаленню систем та стратегій для ефективного управління ними.

Використання аналітики великих даних у контексті управління подіями, зокрема застосування резервування та відновлення даних, управління логічною цілісністю та конфіденційністю даних, а також управління подіями у мультихмарному середовищі, сприяє покращенню аналізу та реакції на події в реальному часі.

У цілому, інтеграція технічних, організаційних та аналітичних підходів до управління подіями стає необхідністю в умовах зростання кількості та складності кіберзагроз, що дозволяє ефективно впоратися з викликами інформаційної безпеки та забезпечити стійкість підприємства у цифровому середовищі.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМ УПРАВЛІННЯ ПОДІЯМИ НА ПІДПРИЄМСТВІ

3.1. Приклади успішної реалізації управління подіями на підприємствах.

Дослідження щодо вдосконалення систем управління подіями проведено на прикладі віртуального підприємства - у вигляді IT компанії розміром до 250 осіб. Дана компанія нараховує до 250 співробітників, і виступає як надійний партнер у світі технологій для своїх клієнтів. Основна спеціалізація цієї компанії - це надання послуг з підтримки IT-систем, що включає широкий спектр завдань, необхідних для ефективної роботи та безпеки інформаційних систем замовників.

Ключовим аспектом її діяльності є впровадження IT-систем. Вона бере на себе відповідальність за встановлення та налаштування IT-рішень, що відповідають конкретним потребам кожного клієнта. Працює як зі стандартними рішеннями, так і з індивідуально розробленими, забезпечуючи гнучкість та ефективність у вирішенні бізнес-завдань.

Крім цього, важливою частиною послуг є супровід та адміністрування IT-систем. Це означає, що вона забезпечує постійне технічне обслуговування, оновлення та моніторинг стану систем, гарантуючи їх безперебійну та стабільну роботу. Допомога користувачам, усунення несправностей та технічна підтримка також входять у перелік цих послуг.

Одним з найважливіших аспектів роботи - забезпечення кібербезпеки. В умовах зростаючих кіберзагроз, вона надає послуги з захисту IT-інфраструктури замовників. Це включає в себе розробку та імплементацію заходів безпеки, моніторинг систем на предмет вразливостей, а також швидке реагування на інциденти безпеки.

Таким чином, ця ІТ компанія стає всебічним ІТ партнером для своїх клієнтів, забезпечуючи не тільки технічну підтримку та обслуговування, але й забезпечуючи високий рівень безпеки та надійності їх ІТ-систем.

Проблематика: Зі збільшенням кількості замовників та розширенням їх ІТ-інфраструктур, ця ІТ компанія стикнулася з серйозними викликами. Ростуча кількість різнотипних систем та випадків, пов'язаних із кібербезпекою, значно збільшила обсяг роботи для моніторингу та аналізу. Реакція компанії на це – збільшення штату – зіткнулася з декількома проблемами, які вплинули на загальну ефективність послуг.

Першою проблемою став різний рівень кваліфікації співробітників. Залучення нових працівників, які не завжди мали однаковий рівень навичок та досвіду, призвело до нерівномірності у виконанні роботи. Це особливо важливо в контексті ІТ-інфраструктур, де навіть маленькі помилки можуть мати серйозні наслідки.

Друга проблема полягала в різній складності інфраструктур та систем замовників. Компанія опинилася перед викликом адаптації своїх сервісів до широкого спектру ІТ-систем, що потребували індивідуального підходу. Це ускладнило процес надання послуг та потребувало значних ресурсів для належного управління.

Третя проблема – відсутність достатньої інформації про функціональні можливості різних систем. Це ускладнювало роботу співробітників, які часто мусили витрачати додатковий час на вивчення особливостей кожної системи.

Остання проблема – неструктурований підхід до обробки подій безпеки. Різні співробітники могли обробляти однотипні інциденти по-різному, що створювало додаткові ризики та знижувало ефективність реагування на кіберзагрози.

Усе це призвело до ситуації, коли подальше розширення бізнесу стало неможливим без ризику повної втрати контролю над подіями безпеки, як для нових, так і для існуючих замовників. Компанія опинилася перед складним вибором: знайти способи оптимізації та удосконалення своїх процесів або прийняти

обмеження на подальше зростання.

Для вирішення вищезгаданих проблем, IT компанія впровадила комплексну систему управління подіями інформаційної безпеки (ISMS), що означало значне переосмислення та реструктуризацію їх підходів до управління кібербезпекою та персоналом. При цьому на практиці був **використаний підхід щодо проведення тренінгу та підготовки персоналу до управління подіями** (розподіл цільової аудиторії за категоріями та рівнями підготовки у сфері інформаційної безпеки показано в табл.3.1), в основу якої покладено наступна послідовність дій, яка зображена на рис. 3.1.

Рис. 3.1. Підхід до проведення тренінгу та підготовки персоналу до управління подіями

1. **Впровадження SIEM системи на базі Splunk Cloud Platform**.

Ця система дозволила централізувати процеси збору, аналізу та класифікації подій безпеки. Це не тільки спростило процес моніторингу інцидентів, але й покращило кореляцію подій та ефективність роботи з інцидентами.

2. **Реструктуризація персоналу**.

Персонал був перерозподілений на різні рівні (L1, L2, L3, інженери безпеки, менеджери якості) відповідно до їхньої кваліфікації та спеціалізації. Це забезпечило більш ефективне реагування на інциденти, а також уможливило

глибше розслідування та реагування на складні випадки.

3. **Розробка та оновлення процедур SOC (Security Operations Center).**

Компанія розробила та регулярно оновлювала важливі процедури, такі як триаж, реагування на інциденти, кібер-розслідування, політики пошуку загроз та інші. Це забезпечило більш структурований підхід до обробки подій безпеки.

4. **Система планування чергування та обміну інформацією**.

Ця система допомогла забезпечити безперервність моніторингу та реагування на інциденти, а також покращила комунікацію між членами команди.

5. **Політика навчання та підвищення кваліфікації персоналу**.

Важливий акцент було зроблено на навчання та підвищення кваліфікації персоналу, щоб забезпечити високий рівень професійних знань та навичок усіх співробітників. Перелік необхідних знань для персоналу наведено в Таблицях 3.1-3.4.

Результати впровадження цих змін:

- **Підвищення якості роботи персоналу**: Завдяки кращому розподілу обов'язків та фокусу на навчанні, персонал став більш компетентним та ефективним у своїй роботі.
- **Покращення ключових показників:** Ключові показники продуктивності та реагування на інциденти покращилися, що свідчить про більш ефективне управління та реагування на інциденти.

Таблиця 3.1

Необхідні знання, навички та вміння для керівників відділу, заступника керівника відділу, провідного спеціаліста, спеціаліста

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
Знання: Знання протоколів шифрування трафіку; Знання налаштування контролеру домену; Знання технології контейнеризації;	Систем віртуалізації; Знання систем бекакування; Знання kubernetes. **Навички та вміння:** Вміння роботи з інфраструктурою віртуальних робочих столів;	**Знання:** Вміння аналізувати великі об’єми трафіку; Вміння протидіяти витоку інформації; Вміння аналізу контролю доступу до інфраструктури.

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
Навички та вміння: Навички налаштування VPN тунелів; Вміння розгортати контролер домену; Налаштовувати політики безпеки; Вміння налаштовування віддалених робочих столів; Навички роботи з контейнерами.	Вміння роботи з балансування навантаження на мережу; Вміння проводити на налаштовувати автоматичні backup даних та конфігурації основних систем; Навички роботи з технологією kubernetes.	**Навички та вміння:** Вміння роботи з класифікацією інформації; Знання систем протидії витоку інформації; Знання налаштування та розробки правил аналізу трафіку;

Таблиця 3.2

Необхідні знання, навички та вміння для техніка

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
Знання: Знання захисту кінцевих користувачів; Знання аналізу трафіку. **Навички та вміння:** Вміння розбору файлів які можуть містити шкідливе програмне забезпечення; Вміння проведення аналізу DNS запитів; вміння проведення аналізу трафіку HTTP та HTTPS без використання TLS.	**Знання:** Знання MITRE матриці; **Навички та вміння:** Вміння виявляти скомпрометовані системи; Вміння роботи з скрипковими мова програмування для проведення автоматиції конфігурації мережевого обладнання.	**Знання:** Знання технології контейнеризації; Знання технології CI/CD; **Навички та вміння:** Вміння налаштування та роботи з контейнерами; Навички роботи з Kubernetes;

Таблиця 3.3

Необхідні знання, навички та вміння для техніка адміністратора

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
Знання: загальні технічні знання з побудови та функціонування мереж; знання технічного обслуговування серверного обладнання. **Навички та вміння:** Вміння проведення технічного обслуговування серверного обладнання; Вміння проведення оновлення серверного програмного забезпечення; Вміння роботи з RAID контролерами; Вміння проведення монтажних робіт мережевого обладнання.	**Знання:** знання основ криптографічного захисту; знання систем віртуалізації; знання базового налаштування IP-телефонії в межах частини. **Навички та вміння:** Вміння роботи з сертифікатами безпеки; Вміння налаштування двохфакторної аунтифікації; Вміння розгортання віртуальних машин; Вміння роботи з віртуальними комутаторами та data storage; Вміння проведення проводити бекапування віртуальних машин силами системи віртуалізації.	**Знання:** Знання PKI інфрастуктури; Знання SSL шифрування; Знання процедури проведення бекапування конфігурації та даних. **Навички та вміння:** Вміння роботи з PKI інфраструктурою; Вміння проведення дворівневого бекапування даних; Вміння відновлювати інформацію з бекапів; Вміння роботи з аналізом трафіку; Мати навички роботи з інструментами аналізу події безпеки.

Таблиця 3.4

Необхідні знання, навички та вміння для оператора

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
Знання: загальні технічні знання з основ побудови та функціонування мереж. **Навички та вміння:** знання моделі OSI; знання стеку протоколів TCP/IP; знання протоколів IP, TCP, UDP, DHCP, ARP, NAT, ICMP та DNS; знання протоколів маршрутизації OSPF, ISIS; BGP, EIGRP;	**Знання:** знання (розуміння принципу роботи) DNS-протоколу та вміння проводити налаштування розподілених зон; знання базового налаштування міжмережевих екранів; розуміння системи віртуалізації. **Навички та вміння:** знання роботи з операційними системами	**Знання:** розширенні знання у сфері виявлення та аналізу події кібербезпеки; знання технології комутації та маршрутизації. **Навички та вміння:** вміння роботи з файловими системами; вміння проведення аналізу шляхом кореляції та аналізу журналів події; вміння проводити поетапне

Необхідні знання, навички та вміння		
Базові	Професійні	Спеціалізовані
вміння працювати з пошуком програмного забезпечення SIEM; вміння проводити аналіз події та проводити фільтрацію події за допомогою програмного забезпечення SIEM.	Windows server та Ubuntu server; знання основ кібербезпеки, а саме захисту периметру; вміння розробляти та налаштовувати правила кореляції.	розслідування інцидентів кібербезпеки; вміння розроблять рекомендації щодо недопущення повторення інцидентів кібербезпеки; вміння роботи з новітніми вразливостями проведення аналізу та розробка рекомендації по їх недопущенню;

- **Покращення задоволення замовників**: Замовники отримали вищу якість сервісів, що позитивно відбилося на їхньому загальному задоволенні.
- **Прогнозованість витрат на навчання та розширення штату**: Менеджмент тепер має краще розуміння майбутніх витрат, пов'язаних з розвитком та навчанням персоналу.
- **Зниження операційних витрат**: Оптимізація процесів та більш ефективне використання ресурсів призвело до зниження витрат на обслуговування.
- **Контрольованість та однозначність управління подіями безпеки**: Впровадження чітких процедур та політик забезпечило більшу прозорість та контроль над процесами управління інцидентами.

Загалом, ці зміни виявилися ефективними у вирішенні викликів, з якими стикалася компанія, та допомогли їй підвищити якість своїх послуг, зміцнивши довіру замовників і підтримуючи стабільне зростання в умовах складного та швидкозмінного IT-світу.

3.2. Формулювання рекомендацій щодо вдосконалення системи управління подіями

Організації повинні слідувати найкращим практикам реагування на інциденти, щоб бути готовими до дій у разі потреби. Наступні найкращі практики слід застосовувати на стратегічному (рамки), тактичному (плани/інструкції) та командному (люди) рівнях:

1. **Розробіть план реагування на інциденти**

Розробіть план реагування на інциденти, який окреслює кроки, які команда реагування на інциденти повинна виконувати у разі інциденту. План допомагає командам покращити часи реагування та відновлення, щоб швидко та ефективно відновити бізнес-операції.

2. **Використовуйте рамки реагування на інциденти**

Плани реагування на інциденти часто базуються на рамках реагування на інциденти, які окреслюють, як найкраще структурувати операції реагування на інциденти. Рамки доступні від міжнародних компаній NIST, ISO, ISACA, Інституту SANS та Альянсу безпеки хмар, серед інших. Ці рамки описують операції реагування та як операції групуються або сегментуються. Під час розробки програми реагування на інциденти перегляньте такі рамки, щоб визначити, які елементи найкраще підходять для потреб вашої організації.

3. **Дотримуйтесь шість фаз реагування на інциденти**

Етапи реагування на інциденти описують основні фази обробки інцидентів:

Підготовка. Ця фаза включає створення та періодичний огляд політик та інструкцій, оцінки ризиків, ідентифікацію команди реагування на інциденти та інші завдання для ефективного реагування на інциденти.

Виявлення. Ця фаза включає виявлення того, що інцидент відбувається, збір доказів та оцінку серйозності події.

Локалізація. Ця фаза включає завдання, спрямовані на обмеження впливу інциденту.

Видалення. Це передбачає видалення основної причини інциденту.

Відновлення. Ця фаза полягає у поверненні залучених систем та пристроїв до стандартної роботи.

Післяінцидентний огляд. Це включає документування інциденту, щоб зрозуміти, як він стався, та застосувати набуті уроки на майбутнє.

4. **Створіть інструкції для реагування на інциденти**.

Організації повинні мати бібліотеку інструкцій для реагування на інциденти - задокументовані поетапні процедури - які описують, як вирішувати поширені інциденти, такі як атаки з використанням викупного програмного забезпечення та фішинг, вторгнення в мережі та інфікування шкідливим програмним забезпеченням. Інструкції допомагають забезпечити швидке та послідовне реагування на інциденти в усій організації.

5. **Сформуйте команду реагування на інциденти**.

Команда реагування на інциденти є важливою для забезпечення належного виконання планів та інструкцій реагування на інциденти. Розмір, тип і назва команди реагування на інциденти залежить від потреб окремих організацій, але цілі є однаковими. При створенні команди реагування на інциденти врахуйте, кого включити в команду внутрішніх та зовнішніх членів та їхні ролі та обов'язки. Основна технічна команда , включаючи менеджера з реагування на інциденти, аналітиків безпеки та реагувальників на інциденти повинна мати підтримуючих членів, включаючи представників зв'язку, зовнішніх зацікавлених сторін і третіх сторін, таких як постачальники послуг та консультанти.

6. **Наявність комунікації**.

План зв'язку у відповідь на інциденти допомагає командам реагування на інциденти обмінюватися знаннями про події безпеки та надавати оновлення щодо прогресу реагування на інциденти. Зв'язок може бути необхідним як всередині організації, так і зовні, залежно від інциденту.

7. **Навчання персоналу реагування на інциденти**.

Члени команди реагування на інциденти повинні пройти навчання з процесів реагування на інциденти та своїх конкретних обов'язків. Проводьте періодичні

тренінги, щоб забезпечити, що члени команди знають, як реагувати, та проводьте навчальні вправи реагування на інциденти, щоб переконатися, що вони готові, коли станеться реальний інцидент.

8. **Періодичний аудит процесів**.

Процеси реагування на інциденти повинні постійно оцінюватися, переглядатися та оновлюватися залежно від змін в IT-інфраструктурі, бізнес-операціях, персоналі та постійно розширюваному спектрі загроз. Застарілі плани призводять до плутанини та підривають процедури реагування на інциденти.

9. **Проактивний пошук загроз**.

Використовуйте розвідувальні дані про загрози та полювання на загрози, щоб проактивно виявляти ознаки компрометації. Розгляньте можливість використання систем виявлення, які попереджають команди реагування на інциденти, коли спостерігається підозріла поведінка.

10. **Післяінцидентний аналіз**.

Після того, як інцидент опрацьований, команда реагування на інциденти повинна створити звіт про те, що сталося, як інцидент було вирішено та які уроки було отримано - наприклад, як краще реагувати на такі події в майбутньому. Відповідно коригуйте плани та інструкції.

11. **Підбір ефективних інструментів**.

Командам реагування на інциденти потрібні відповідні інструменти для виявлення, аналізу та управління загрозами, а також для створення звітів. Поширені інструменти реагування на інциденти повинні реалізувати наступні завдання:

- Оцінювання вразливостей.
- Обробка інцидентів
- Управління подіями.
- Виявлення та реагування на кінцевих точках.
- Оркестрація безпеки, автоматизація та реагування.
- Інструменти проведення розслідувань інцидентів безпеки.

12. **Можливість використання автоматизації**.

Автоматизація може допомогти командам реагування на інциденти, які не встигають або перевантажені. Автоматизовані інструменти реагування на інциденти використовують штучний інтелект та машинне навчання для допомоги аналітикам безпеки відфільтрувати велику кількість даних, щоб знайти та проаналізувати потенційні інциденти. Вони також можуть сортувати інциденти нижчого рівня та рутинні завдання, таким чином звільняючи аналітиків для зосередження на більш нагальних питаннях та аналізі.

13. **Консультації зовнішніх експертів**.

Організації, які не можуть впоратися з реагуванням на інциденти всередині компанії, можуть бути краще підготовлені до аутсорсингу деяких або всіх завдань реагування на інциденти. Постачальники послуг з управління безпекою можуть управляти виявленням загроз та реагуванням на них, допомагати з комунікаціями та управлінням PR, а також проводити управління кризами для організацій, які не мають достатньо персоналу або ресурсів, щоб робити це самостійно.

Висновки до розділу 3.

Аналізуючи вищезазначену інформацію, можна зробити висновок, що дана IT компанія успішно вирішила свої проблеми з управлінням подіями інформаційної безпеки (ISMS) та розробила ефективну методику тренінгу та підготовки свого персоналу.

Ключові аспекти успішної реалізації управління подіями (ISMS):

● **Впровадження централізованої SIEM системи**: Використання Splunk Cloud Platform дозволило компанії ефективно збирати, аналізувати та класифікувати події безпеки, значно покращивши кореляцію подій та ефективність роботи з інцидентами.

● **Структурований розподіл персоналу**: Розподіл персоналу за рівнями (L1, L2, L3 та інші) відповідно до їх кваліфікації забезпечив ефективне реагування

на інциденти та глибше розслідування складних випадків.

● **Розробка та оновлення процедур SOC**: Чітко визначені процедури допомогли структурувати обробку подій безпеки та підвищили загальну ефективність команди.

Методика проведення тренінгу та підготовки персоналу:

● **Категоризація навчальних потреб**: Компанія ефективно визначила різні рівні навичок та знань потрібні для різних ролей, забезпечуючи цільове навчання та розвиток співробітників.

● **Регулярне оновлення та підвищення кваліфікації**: Неперервне навчання та розвиток персоналу забезпечували, що команда залишалася в курсі останніх тенденцій та практик у сфері кібербезпеки.

● **Практичні вправи та тренінги**: Проведення регулярних навчальних вправ та симуляцій допомогло персоналу краще розуміти свої ролі та обов'язки в управлінні інцидентами.

Отже, успішне впровадження комплексної системи ISMS та ефективна методика тренінгу та підготовки персоналу дозволили IT компанії не тільки вирішити існуючі виклики, але й створити міцну основу для подальшого розвитку та адаптації до швидко змінюваного цифрового ландшафту. Це підкреслює важливість гнучкого підходу до управління інформаційною безпекою та інвестицій у розвиток персоналу для досягнення довгострокового успіху в сфері IT.

ВИСНОВКИ

В роботі розглянуто сучасні методи управління подіями інформаційної безпеки на підприємствах, а саме: традиційні та новітні методи управління, включаючи використання журналів подій, систем виявлення вторгнень, автоматизацію, машинне навчання та когнітивний аналіз. Проаналізовано основні стратегічні аспекти, які включають визначення бізнес-мети, інтеграцію з бізнес-процесами, аналіз ризиків, залучення зацікавлених сторін, вибір технологічних рішень та навчання персоналу.

Для вдосконалення галузі рекомендується зосередитись на розробці більш інтегрованих та гнучких систем управління, які забезпечують швидке адаптування до нових викликів та технологій. Це включає інвестиції у розвиток штучного інтелекту та машинного навчання для автоматизації реагування на інциденти, а також створення адаптивних рамок управління, які можуть оперативно реагувати на змінні бізнес-вимоги та загрози.

Розробка більш інтегрованих та гнучких систем управління подіями інформаційної безпеки вимагає декількох ключових елементів:

Автоматизація та штучний інтелект: Впровадження автоматизованих рішень, заснованих на штучному інтелекті та машинному навчанні, для швидкого виявлення та реагування на інциденти безпеки.

Інтеграція з бізнес-процесами: Створення систем, що тісно інтегровані з ключовими бізнес-процесами, забезпечуючи неперервний моніторинг та адаптацію до змін у бізнес-середовищі.

Гнучкість та масштабованість: Розробка систем, здатних адаптуватися до змінюваних вимог та масштабуватися відповідно до потреб організації.

Навчання персоналу: Освіта та розвиток навичок персоналу для роботи з новітніми технологіями та методами управління інцидентами.

Продумана стратегія реагування на інциденти: Розробка чітких, але

гнучких планів реагування, які можуть бути швидко адаптовані під конкретні сценарії інцидентів.

Вдосконалення цієї галузі також може включати розвиток співпраці з експертами у сфері кібербезпеки та використання передових аналітичних інструментів для глибшого аналізу даних та передбачення потенційних ризиків

ПЕРЕЛІК ПОСИЛАНЬ

1. Unit: 01 Introduction to event management. Malabon : De La Salle Araneta University, 2021. 98 p. URL : https://www.uou.ac.in/sites/default/files/slm/HM-402.pdf

2. Hitchens T., Goren N. International Cybersecurity Information Sharing Agreements. *JSTOR*. 2017. 140 p. URL : https://www.jstor.org/stable/resrep20426

3. Vielberth M., Pernul G. A Security Information and Event Management Pattern. *SugarLoaf-PLoP 2018* : 12th Latin American Conference on Pattern Languages of Programs ; 20th - 23th. November 2018. Valparaíso, 2018. URL : https://www.researchgate.net/publication/337946451_A_Security_Information_and_Event_Management_Pattern

4. What is Threat Hunting? *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/what-threat-hunting-trolleyesecurity-fwadc

5. : NYS-S13-005. Cyber Incident Response. NY, 2023. 22 p. URL : https://its.ny.gov/system/files/documents/2023/11/nys-s13-005-cyber-incident-response_0.pdf

6. Cybersecurity Incident & Vulnerability Response Playbooks. *Cybersecurity and Infrastructure Security Agency*. 2021. 43 p. URL : https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

7. Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey / Gan C. et al. *Mathematics*. 2023. Vol. 11, no. 14. P. 3115. URL: https://doi.org/10.3390/math11143115

8. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804

9. Chen H., Chiang R., Storey V. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*. 2012. Vol. 36, no. 4. P. 1165. URL: https://doi.org/10.2307/41703503

10. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018. URL : https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022. URL : https://www.iso.org/standard/27001

12. ISO 27001:2022. *DataGuard* : веб-сайт. URL : https://www.dataguard.co.uk/knowledge/iso-27001/

13. ISO 27001. *Techtarget* : веб-сайт. URL : https://www.techtarget.com/whatis/definition/ISO-27001

14. NIST SP 800-61. Computer Security Incident Handling Guide, 2012. URL : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

15. Cybersecurity Incident Response Plans. *Health Sector Cybersecurity Coordination Center*, 2023. URL : https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

16. PCI DSS (Payment Card Industry Data Security Standard). *Techtarget* : веб-сайт. URL : https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

17. What are the 12 requirements of PCI DSS Compliance? *ControlCase* : веб-сайт. URL : https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/

18. What is SIEM? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/siem

19. Субач І., Микитюк А., Кубрак В. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об’єктів критичної інфраструктури. *Information Technology and Security*. 2019. Vol. 7. Iss. 2 (13). С. 208-215. URL : https://ela.kpi.ua/bitstream/123456789/33889/1/ITS2019-7-2_09.pdf

20. Security Information and Event Management Tools for Cybersecurity Analyst. *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/security-

information-event-management-toolsfor-analyst-saheed-oyedele-ake1e?trk=article-ssr-frontend-pulse_more-articles_related-content-card

21. What is EDR (endpoint detection and response)? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/edr

22. A. George, S. Fernando, T. Baskar, H. George. Extending Detection and Response: How MXDR Evolves Cybersecurity. *Partners Universal International Innovation Journal (PUIIJ).* 2023. Vol. 01 Issue 04. URL : https://www.researchgate.net/publication/373391567_Extending_Detection_and_Response_How_MXDR_Evolves_Cybersecurity

23. Що таке SOAR? *Microsoft* : веб-сайт. URL : https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar

24. How Does SOAR Fit in an EDR-centric SOC? *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/how-does-soar-fit-edr-centric-soc-d3-security-management-systems?trk=article-ssr-frontend-pulse_more-articles_related-content-card

25. SIEM Implementation in 4 Steps. *Exabeam* : веб-сайт. URL : https://www.exabeam.com/explainers/siem/siem-implementation-in-4-steps/

26. What is Business Process Analysis? *IBM* : веб-сайт. URL : https://www.ibm.com/blog/business-process-analysis/

27. Managing Risk in Digital Transformation. *Deloitte* : веб-сайт. URL : https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-digital-transformation-1-noexp.pdf

28. Repa V. Methodology for Business Processes Analysis. *Evolution and Challenges in System Development*. 1999. URL : https://www.researchgate.net/publication/267916961_Methodology_for_Business_Processes_Analysis

29. Project scope. *Techtarget* : веб-сайт. URL : https://www.techtarget.com/searchcio/definition/project-scope

30. Finding the Right Venue and Event Management Solution. *Momentus technologies* : веб-сайт. URL : https://gomomentus.com/blog/finding-the-right-venue-and-event-management-solution

31. 9 Steps to Successful Functional Strategic Planning. *Gartner* : веб-сайт. URL : https://www.gartner.com/smarterwithgartner/9-steps-successful-functional-strategic-planning

32. What is data security? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/data-security

33. What is SIEM? *Exeon* : веб-сайт. URL : https://exeon.com/what-is-siem

34. What Is SIEM, Why Is It Important and How Does It Work? *Exabeam* : веб-сайт. URL : https://www.exabeam.com/explainers/siem/what-is-siem/

35. Security information and event management, SIEM. *IITD* : веб-сайт. URL : https://iitd.com.ua/en/upravlinnja-informaciieju-ta-podijami-bezpeki-siem/

36. Training for security information and event management. *RSI* : веб-сайт. URL : https://blog.rsisecurity.com/training-for-security-information-and-event-management/

37. Bronson R. The Role Of Technologies In Event Management. *StartUs Magazine*. 2018. URL : https://magazine.startus.cc/role-technologies-event-management/

38. CRM (customer relationship management). *Techtarget* : веб-сайт. URL : https://www.techtarget.com/searchcustomerexperience/definition/CRM-customer-relationship-management

39. Debar H., Dacier M., Wespi A. A revised taxonomy for intrusion-detection systems. *Annales Des Télécommunications*. 2000. Vol. 55, no. 7-8. P. 361–378. URL: https://doi.org/10.1007/bf02994844

40. Werlinger R., Hawkey K., Muldner K., Jaferian P. The challenges of using an intrusion detection system: Is it worth the effort? *Association for Computing Machinery* : Proceedings of the 4th symposium on Usable privacy and security. July 23 - 25, 2008. New York, 2008. URL : https://www.researchgate.net/publication/221166372_The_challenges_of_using_an_intrusion_detection_system_Is_it_worth_the_effort

41. What is an intrusion detection system (IDS)? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/intrusion-detection-system

42. Jabez J., Muthukumar B. Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach. *Procedia Computer Science*. 2015. Vol. 48. P. 338–346. URL: https://doi.org/10.1016/j.procs.2015.04.191

43. What is an intrusion prevention system (IPS)? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/intrusion-prevention-system

44. IDS/IDPS. *Vectra* : веб-сайт. URL : https://www.vectra.ai/topics/intrusion-detection-prevention-system

45. Shah D., Vasudavan H., Razali N. Event Management Systems (EMS). *Journal of Applied Research and Technology*. 2023. URL : https://www.researchgate.net/publication/371874293_Event_Management_Systems_EMS

46. Taye M. M. Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. *Computers*. 2023. Vol. 12, no. 5. P. 91. URL: https://doi.org/10.3390/computers12050091

47. Real-time artificial intelligence and event processing. *IBM* : веб-сайт. URL : https://www.ibm.com/blog/real-time-artificial-intelligence-and-event-processing/

48. Kamalov F., Santandreu Calonge D., Gurrib I. New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution. *Sustainability*. 2023. Vol. 15, no. 16. P. 12451. URL: https://doi.org/10.3390/su151612451

49. Security information and event management (SIEM). *Techtarget* : веб-сайт. URL : https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

50. What is an API? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/api

51. API Authentication Security Best Practices. *Impart* : веб-сайт. URL : https://www.impart.security/api-security-best-practices/api-authentication-security-best-practices

52. Domain events: Design and implementation. *Microsoft* : веб-сайт. URL : https://learn.microsoft.com/en-us/dotnet/architecture/microservices/microservice-ddd-cqrs-patterns/domain-events-design-implementation

53. What Is Configuration Management? *Cisco* : веб-сайт. URL : https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-configuration-management.html

54. Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams / T. A. Williams et al. *Academy of Management Annals*. 2017. Vol. 11, no. 2. P. 733–769. URL: https://doi.org/10.5465/annals.2015.0134

55. Chenaru O., Mocanu S., Dobrescu R. Nicolae M. Enhancing Antifragile Performance of Manufacturing Systems through Predictive Maintenance. *Applied sciences*. 2022. Vol. 12, no. 23. P. 11958. URL: https://doi.org/10.3390/app122311958

56. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review / U. Tariq et al. *Sensors*. 2023. Vol. 23, no. 8. P. 4117. URL: https://doi.org/10.3390/s23084117

57. What Is Security Control Effectiveness? *Picus* : веб-сайт. URL : https://www.picussecurity.com/resource/glossary/what-is-security-control-effectivess

58. System Integration: Types, Approaches, and Implementation Steps. *Altexsoft* : веб-сайт. URL : https://www.altexsoft.com/blog/system-integration/

59. González-Granadillo G., González-Zarzosa S., Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. 2021. Vol. 21, no. 14. P. 4759. URL: https://doi.org/10.3390/s21144759

60. Planning and Executing Scenario Based Simulation Exercises: Methodological Lessons / D. Van Niekerk et al. *Journal of Homeland Security and Emergency Management*. 2015. Vol. 12, no. 1. URL: https://doi.org/10.1515/jhsem-2013-0077

61. Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System / S. M. Khalil et al. *Computers & Security*. 2022. P. 102950. URL: https://doi.org/10.1016/j.cose.2022.102950

62. Big Data Fundamentals. Big Data Lifecycle & Big Data stack. Big Data's Complexity: Unveiling the 7 Key Challenges & Big Data Solutions. *Linkedin* : веб-сайт. URL : https://www.linkedin.com/pulse/big-data-fundamentals-lifecycle-stack-datas-

complexity-rajoo-jha-mbovc?trk=article-ssr-frontend-pulse_more-articles_related-content-card

63. What is backup and disaster recovery? *IBM* : веб-сайт. URL : https://www.ibm.com/topics/backup-disaster-recovery

64. Information security. *Softserve* : веб-сайт. URL : https://www.softserveinc.com/en-us/information-security

65. Consultation Paper on Draft Regulatory Technical Standards. *Joint committee of the European supervisory authorities*. 2023. URL : https://www.eiopa.europa.eu/system/files/2023-06/2.%20CP%20-%20Draft%20RTSs%20ICT%20risk%20management%20tools%20methods%20processes%20and%20policies.pdf

66. Google Cloud. *Google* : веб-сайт.URL : https://cloud.google.com

67. Azure. Limitless innovation. *Microsoft* : веб-сайт. URL : https://azure.microsoft.com/en-gb/

68. Amazon Web Services. *Amazon* : веб-сайт. URL : https://aws.amazon.com

69. The 4 Types Of Cloud Computing: Choosing The Best Model. *Cloudzero* : веб-сайт. URL : https://www.cloudzero.com/blog/types-of-cloud-computing/